May 2008

# DOD BUSINESS SYSTEMS MODERNIZATION

## Progress in Establishing Corporate Management Controls Needs to Be Replicated Within Military Departments

**G A O**

Accountability ★ Integrity ★ Reliability

# GAO
**Accountability·Integrity·Reliability**

# Highlights

# DOD BUSINESS SYSTEMS MODERNIZATION

## Progress in Establishing Corporate Management Controls Needs to Be Replicated Within Military Departments

## Why GAO Did This Study

In 1995, GAO first designated the Department of Defense's (DOD) business systems modernization program as "high risk," and GAO continues to do so today. To assist in addressing this high-risk area, the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 contains provisions that are consistent with prior GAO investment management and enterprise architecture-related recommendations, and requires the department to submit annual reports to its congressional committees on its compliance with these provisions. The act also directs GAO to review each annual report. In response, GAO assessed the actions taken by DOD to comply with requirements of the act. To do so, GAO leveraged its recent reports on various aspects of the department's modernization management controls, and it reviewed, for example, the latest version of its business enterprise architecture and the associated transition plan and architecture federation strategy. GAO also interviewed key officials.

## What GAO Recommends

Because GAO has previously made recommendations to DOD aimed at putting in place the management controls needed to fully comply with the act and related federal guidance, it is not making additional recommendations. DOD provided technical comments that have been incorporated into the report.

## What GAO Found

As part of DOD's continuing efforts to strengthen management of its business systems modernization program, it has taken steps over the last year to build on past efforts and further comply with the National Defense Authorization Act's requirements and related federal guidance. Notwithstanding this progress, aspects of these requirements and relevant guidance have yet to be fully satisfied. In particular, the military departments, under DOD's "federated" and "tiered" approach to establishing institutional modernization management controls, have lagged well behind DOD's corporate efforts, and the corporate efforts are still not yet where they need to be. For example:

- The latest version of DOD's corporate business enterprise architecture continues to add content needed to improve its completeness, consistency, understandability, and usability. Moreover, its latest architecture federation strategy is more detailed and explicit than the prior version. However, the corporate architecture is still missing important content, such as business rules for, and information flows among, certain business activities. Moreover, the architecture has yet to be federated. Specifically, the military departments, which are the largest members of the federation, do not yet have mature enterprise architecture programs, and the federation strategy aimed at accomplishing this is still evolving. GAO has existing recommendations to address these and other architecture issues.

- The updated enterprise transition plan, which provides a temporal investment roadmap for transitioning from the current architectural environment to the target environment, continues to identify systems and initiatives that are to fill business capability gaps and address the DOD-wide and component business priorities that are contained in the business enterprise architecture. However, the plan still does not include investments for all components and does not reflect key factors associated with properly sequencing planned investments, such as dependencies among investments and the capability to execute the plan. Furthermore, the military departments, which are the largest members of the business federation, have yet to fully develop their own architecturally-based transition plans. GAO has existing recommendations to address these and other transition plan issues.

- DOD and the military departments have yet to fully establish key investment review structures and have yet to define related policies and procedures for effectively performing both project-level and portfolio-based investment management. GAO has existing recommendations to address these and other investment issues.

Until DOD fully implements GAO's existing recommendations relative to the act and related guidance, its business systems modernization will likely remain a high-risk program.

_____
**United States Government Accountability Office**

# Contents

**G A O**
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

May 15, 2008

Congressional Committees

For decades, the Department of Defense (DOD) has been challenged in modernizing its timeworn business systems.[1] In 1995, we designated DOD's business systems modernization program as high risk, and we continue to designate it as such today.[2] As our research on public and private sector organizations shows, two essential ingredients to a successful systems modernization program are having a well-defined enterprise architecture[3] and an effective institutional approach to managing information technology (IT) investments.

Accordingly, we made recommendations to the Secretary of Defense in May 2001 that included the means for effectively developing an enterprise architecture and establishing a corporate, architecture-centric approach to investment control and decision making.[4] Between 2001 and 2005, we reported that the department's business systems modernization program continued to lack both of these, concluding in 2005 that hundreds of millions of dollars had been spent on a business enterprise architecture

---

[1] Business systems support DOD's business operations, such as civilian personnel, finance, health, logistics, military personnel, procurement, and transportation.

[2] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[3] An 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 the enterprise's current "as is" operational and technological environment and its target or "to be" environment, and contains a capital investment road map for transitioning from the current to the target environment. These snapshots consist of "views," which are basically one or more architecture products that provide conceptual or logical representations of the enterprise.

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

(BEA) and investment management structures that had limited value.[5] Accordingly, we made more explicit architecture and investment management-related recommendations.

To further assist DOD in addressing these modernization management challenges, Congress included provisions in the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 [6] that were consistent with our recommendations. More specifically, the act required the department to, among other things, (1) develop a BEA, (2) develop a transition plan to implement the architecture, (3) identify systems information in its annual budget submission, (4) establish a system investment approval and accountability structure, (5) establish an investment review process, and (6) certify and approve any system modernizations costing in excess of $1 million. The act further requires that the Secretary of Defense submit an annual report to congressional defense committees on DOD's compliance with certain requirements of

---

[5]See, for example, GAO, *Defense Business Transformation: Sustaining Progress Requires Continuity of Leadership and an Integrated Approach*, GAO-08-462T (Washington D.C.: Feb.7, 2008); GAO, *DOD Business Systems Modernization: Progress Continues to Be Made in Establishing Corporate Management Controls, but Further Steps Are Needed*, GAO-07-733 (Washington D.C.: May 14, 2007); GAO, *Business Systems Modernization: Strategy for Evolving DOD's Business Enterprise Architecture Offers a Conceptual Approach, but Execution Details are Needed*, GAO-07-451 (Washington, D.C.: Apr.16, 2007); GAO, *Defense Business Transformation: A Comprehensive Plan, Integrated Efforts, and Sustained Leadership Are Needed to Assure Success*, GAO-07-229T (Washington, D.C.: Nov. 16, 2006); GAO, *Business Systems Modernization: DOD Continues to Improve Institutional Approach, but Further Steps Needed*, GAO-06-658 (Washington, D.C.: May 15, 2006); GAO, *DOD Business Systems Modernization: Long-standing Weaknesses in Enterprise Architecture Development Need to Be Addressed*, GAO-05-702 (Washington, D.C.: July 22, 2005); GAO, *DOD Business Systems Modernization: Billions Being Invested without Adequate Oversight*, GAO-05-381 (Washington, D.C.: Apr. 29, 2005); GAO, *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); GAO, *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); GAO, *Business Systems Modernization: Summary of GAO's Assessment of the Department of Defense's Initial Business Enterprise Architecture*, GAO-03-877R (Washington, D.C.: July 7, 2003); GAO, *Information Technology: Observations on Department of Defense's Draft Enterprise Architecture*, GAO-03-571R (Washington, D.C.: Mar. 28, 2003); GAO, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458 (Washington, D.C.: Feb. 28, 2003); and GAO-01-525.

[6]Ronald 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).

the act not later than March 15 of each year from 2005 through 2009. Additionally, the act directs us to submit to these congressional committees—within 60 days of DOD's report submission—an assessment of DOD's actions to comply with these requirements.

As agreed with your offices, the objective of our review was to assess the actions taken by DOD to comply with requirements of section 2222 of Title 10, U.S. Code. To accomplish this, we used our prior annual report under the act[7] as a baseline, analyzing whether the department had taken actions to comply with those provisions of the act, related guidance, and our prior recommendations that we had previously identified as not yet addressed. In doing this, we also relied on the results of relevant reports that we have issued since our prior annual report.[8] We conducted this performance audit at DOD headquarters in Arlington, Virginia, from March to May 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Details on our objectives, scope, and methodology are contained in appendix I.

# Results in Brief

DOD continues to take steps to comply with legislative requirements and related guidance pertaining to its business systems modernization high-risk area. In particular, on March 14, 2008, DOD released a new version of its BEA and issued its annual report to congressional defense committees describing steps taken and planned relative to the act's requirements, among other things. The steps address several of the missing elements that we previously identified relative to the legislative provisions and related best practices concerning the BEA, enterprise transition plan, and investment management, and continue to address the act's requirements relative to business system budgetary disclosure and certification and approval of systems costing in excess of $1 million. However, additional steps are needed to fully comply with the act and relevant guidance:

---

[7]GAO-07-733.

[8]GAO, *Business Systems Modernization: Air Force Needs to Fully Define Policies and Procedures for Institutionally Managing Investments*, GAO-08-52 (Washington, D.C.: Oct. 31, 2007); GAO, *Business Systems Modernization: Department of the Navy Needs to Establish Management Structure and Fully Define Policies and Procedures for Institutionally Managing Investments*, GAO-08-53 (Washington, D.C.: Oct. 31, 2007); GAO, *DOD Business Systems Modernization: Military Departments Need to Strengthen Management of Enterprise Architectures*, GAO-08-519 (Washington, D.C.: May 12, 2008); and GAO-08-462T.

- The latest version of the BEA resolves several of the architecture gaps associated with the prior version, such as adding business rules and data attributes. However, like the previous version, its focus is largely on DOD-wide corporate policies, capabilities, rules, and standards. While these are essential to meeting the act's requirements, this version has yet to be augmented by the DOD component organizations' subsidiary architectures that also are essential to meeting the act's requirements and the department's goal of having a federated family of architectures. DOD has taken some steps toward extending its architecture through its recently updated federation strategy, however the military departments' architecture programs remain immature, particularly those of the Army and the Navy. To address these challenges, we have existing recommendations that DOD has agreed to implement.[9] Once these challenges are addressed, the federated BEA should provide a more sufficient frame of reference to optimally guide and constrain DOD-wide system investments.

- The updated transition plan continues to identify more systems and initiatives that are to fill business capability gaps and address DOD-wide and component business priorities. Further, the plan continues to provide a range of information for each identified system and initiative (e.g., budget information, performance metrics, and milestones), and it identifies legacy systems that will not be part of DOD's target architectural environment. However, this latest transition plan still does not include system investment information for all organizational components (e.g., defense agencies). Moreover, the plan does not yet sequence the planned investments based on a range of relevant factors, such as technology opportunities, marketplace trends, institutional system development and acquisition capabilities, legacy and new system dependencies and life expectancies, and the projected value of competing investments. Finally, the plan is not augmented by military department enterprisewide transition plans that are based on analyses of the gaps between their respective current and target architectures. Thus, component-unique investments may not have been chosen based on an enterprisewide strategy, and thus may not represent the optimal investment mix and sequence. We have existing recommendations aimed at addressing these issues that DOD has agreed to implement.[10] Once they are addressed, the department will be better positioned to effectively and efficiently migrate to a more modernized systems environment.

---

[9]GAO-08-519.

[10]GAO-07-733.

- The department's fiscal year 2009 budget submission provides a range of information on its approximately 3,000 business systems, of which 273 are listed as development/modernization investments. Consistent with the act, the types of information provided include system name, designated approval authority, and funding development/modernization versus operations/maintenance activities.

- The department has established and begun implementing most of the investment review structures and processes that are consistent with the act. However, it has yet to establish one of the five investment review boards that are required pursuant to the act, and has not defined related investment management policies and procedures in a manner that is consistent with relevant guidance. In particular, the Enterprise Information Environment Mission Area review board has not been chartered, although DOD officials told us that the department anticipates issuing a policy shortly that, among other things, will establish an information technology infrastructure guidance board that will meet the act's requirement. In addition, neither DOD nor the military departments have defined the full range of project-level and portfolio-based IT investment management policies and procedures that are necessary to meet the investment selection and control provisions of the Clinger-Cohen Act of 1996. To address these investment management limitations, we have previously made recommendations that DOD has agreed to implement.[11] In this regard, the department reports that it is defining missing policies and procedures in its new business capability lifecycle methodology. However, this methodology has not been approved and released. Moreover, based on a draft of the methodology, it may not address all the investment management policy and procedure gaps that our recommendations address. Until DOD and the military departments have well-defined investment management processes, its business systems and portfolios of systems will continue to risk being inconsistently and improperly selected and controlled.

- The department continues to certify and approve business systems as directed by the act. As of September 30, 2007, the department reported that its highest investment review and decision-making body, the Defense Business System Management Committee, had approved 314 systems that had been certified by DOD's Investment Review Boards. According to DOD, the 314 systems represent the total number of certified and approved systems since the act became effective and includes all

---

[11]GAO-07-538.

modernization investments that involved at least $1 million in obligations through fiscal year 2007. Since then, the department reports that it has certified and approved 39 additional investments during fiscal year 2008.

Notwithstanding the progress that DOD continues to make in meeting the business systems modernization provisions of the act and related federal guidance, more needs to be accomplished, particularly with respect to the institutionalization of modernization management controls by the department's largest component organizations—the military departments. In this regard, we have made a number of recommendations that provide an effective roadmap for progress. As a result, we are not making additional recommendations at this time, but would add that until DOD fully implements our existing modernization management-related recommendations, its business systems modernization will likely remain a high-risk program.

In comments on a draft of this report, signed by the Deputy Under Secretary of Defense (Business Transformation), the department stated that it appreciated our support in advancing its business transformation efforts. It also provided several technical comments that we have incorporated throughout the report, as appropriate.

## Background

DOD is a massive and complex organization. The department reported that its fiscal year 2007 operations involved approximately $1.5 trillion in assets and $2.1 trillion in liabilities; more than 2.9 million military and civilian personnel; and $544 billion in net cost of operations. For fiscal year 2008, the department has received discretionary budget authority for about $546 billion and reports total obligations of about $492 billion to support ongoing operations and activities related to the Global War on Terrorism. Organizationally, the department includes the Office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the military departments, numerous defense agencies and field activities, and various unified combatant commands that are either responsible for specific geographic regions or specific functions. (See fig. 1 for a simplified depiction of DOD's organizational structure.)

**Figure 1: Simplified DOD Organizational Structure**
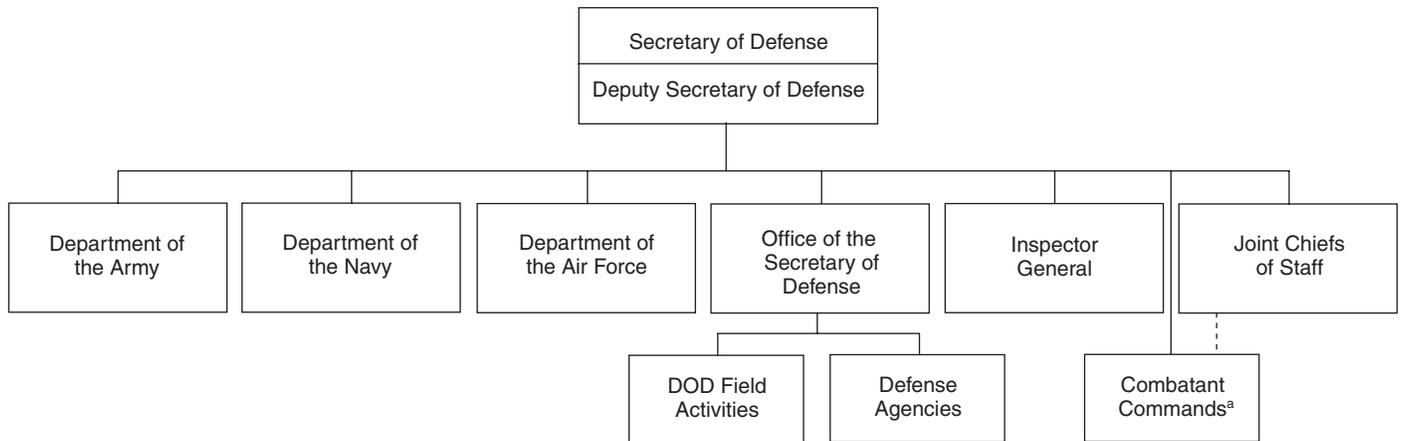


Source: GAO based on DOD documentation.

ªThe Chairman of the Joint Chiefs of Staff serves as the spokesman for the commanders of the combatant commands, especially on the administrative requirements of the commands.

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. As we have previously reported,[12] the DOD systems environment that supports these business functions 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 data to be entered manually into multiple systems. Moreover, the department recently reported that this systems environment is comprised of approximately 3,000 separate business systems. For fiscal year 2007, Congress appropriated approximately $15.7 billion to DOD, and for fiscal year 2008, the department has requested about $15.9 billion in appropriated funds to operate, maintain, and modernize these business systems and associated IT infrastructure.

---

[12]GAO-06-658.

As we have previously reported,[13] the department's nonintegrated and duplicative systems impair its ability to combat fraud, waste, and abuse. In fact, DOD currently bears responsibility, in whole or in part, for 15 of our 27 high-risk areas.[14] Eight of these areas are specific to the department,[15] while it shares responsibility for seven other governmentwide high-risk areas.[16] DOD's business systems modernization is one of the high-risk areas, and it is an essential enabler to addressing many of the department's other high-risk areas. For example, modernized business systems are integral to the department's efforts to address its financial, supply chain, and information security management high-risk areas.

## Enterprise Architecture and IT Investment Management Controls Are Critical to Achieving Successful Systems Modernization

Effective use of an enterprise architecture—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 this challenging goal: optimally defined operational and technological environments. Congress, the Office of Management and Budget (OMB), and the federal Chief Information Officer's (CIO) Council also have recognized the importance of an architecture-centric approach to modernization. The Clinger-Cohen Act of 1996[17] mandates that an agency's CIO develop, maintain, and facilitate the implementation of an information technology architecture. Further, the E-Government Act of 2002[18] requires OMB to oversee the development of enterprise architectures within and

---

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

[14]GAO-07-310.

[15]These eight high-risk areas include DOD's overall approach to business transformation, business systems modernization, financial management, the personnel security clearance program, supply chain management, support infrastructure management, weapon systems acquisition, and contract management.

[16]The seven governmentwide high-risk areas are disability programs, ensuring the effective protection of technologies critical to U.S. national security interests, interagency contracting, information systems and critical infrastructure, information-sharing for homeland security, human capital, and real property.

[17]40 U.S.C. § 11315(b)(2).

[18]44 U.S.C. § 3602(f)(14).

across agencies. In addition, we, OMB, and the CIO Council have issued guidance that emphasizes the need for system investments to be consistent with these architectures.[19]

A corporate approach to IT investment management is characteristic of successful public and private organizations. Recognizing this, Congress enacted the Clinger-Cohen Act of 1996,[20] which requires OMB to establish processes to analyze, track, and evaluate the risks and results of major capital investments in IT systems made by executive agencies.[21] In response to the Clinger-Cohen Act and other statutes, OMB has developed policy and issued guidance for planning, budgeting, acquisition, and management of federal capital assets.[22] We also have issued guidance in this area.[23]

## 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 ("As Is") environment and its target ("To Be") environment. These snapshots consist of "views," which are one or more interdependent and interrelated architecture products (e.g., models, diagrams, matrixes, and text) that provide logical or technical

---

[19]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004); *OMB Capital Programming Guide*, Version 1.0 (July 1997); and CIO Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001).

[20]The Clinger-Cohen Act of 1996, 40 U.S.C. § 11302(c)(1). This act expanded the responsibilities of OMB and the agencies that had been set under the Paperwork Reduction Act with regard to IT management. See 44 U.S.C. 3504(a)(1)(B)(vi) (OMB); 44 U.S.C. 3506(h)(5) (agencies).

[21]We 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).

[22]This 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.

[23]See for example, GAO-04-394G; GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO-03-584G (Washington, D.C.: April 2003); and 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).

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 road map for moving between the two environments and incorporates such considerations as technology opportunities, marketplace trends, fiscal and budgetary constraints, institutional system development and acquisition capabilities, legacy and new system dependencies and life expectancies, and the projected value of competing investments.

The suite of products produced for a given entity's enterprise architecture, including its structure and content, is largely governed by the framework used to develop the architecture. Since the 1980s, various architecture frameworks have been developed, such as John A. Zachman's "A Framework for Information Systems Architecture"[24] and the DOD Architecture Framework.[25]

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 optimize the interdependencies and relationships among an organization's business operations (and the underlying IT infrastructure and applications) that support these operations. Moreover, 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 mission performance. Our experience with federal agencies has shown that investing in IT without defining these investments in the context of an

---

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

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

architecture often results in systems that are duplicative, not well integrated, and unnecessarily costly to maintain and interface.[26]

One approach to structuring an enterprise architecture is referred to as a federated enterprise architecture. Such a structure treats the architecture as a family of coherent but distinct member architectures that conform to an overarching architectural view and rule set. This approach recognizes that each member of the federation has unique goals and needs as well as common roles and responsibilities with the levels above and below it. Under a federated approach, member architectures are substantially autonomous, although they also inherit certain rules, policies, procedures, and services from higher-level architectures. As such, a federated architecture enables component organization autonomy while ensuring enterprisewide linkages and alignment where appropriate. Where commonality among components exists, there also are opportunities for identifying and leveraging shared services.

A service-oriented architecture (SOA) is an approach for sharing business capabilities across the enterprise by designing functions and applications as discrete, reusable, and business-oriented services. As such, service orientation permits sharing capabilities that may be under the control of different component organizations. As we have previously reported,[27] such capabilities or services need to be, among other things, (1) self-contained, meaning that they do not depend on any other functions or applications to execute a discrete unit of work; (2) published and exposed as self-describing business capabilities that can be accessed and used; and (3) subscribed to via well-defined and standardized interfaces. A SOA approach is thus not only intended to reduce redundancy and increase integration, but also to provide the kind of flexibility needed to support a quicker response to changing and evolving business requirements and emerging conditions.

---

[26]See, 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); GAO-04-731R; GAO, *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, GAO-04-43 (Washington, D.C.: Nov. 21, 2003); GAO-03-1018; GAO-03-877R; GAO, *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001); and GAO, *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

[27]GAO, *Information Technology: FBI Has Largely Staffed Key Modernization Program, but Strategic Approach to Managing Program's Human Capital Is Needed*, GAO-07-19 (Washington, D.C.: Oct. 16, 2006).

## 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 that focuses on selecting, controlling, and evaluating investments in a manner that minimizes risks while maximizing the return of investment.[28]

- 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, they continue to meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems arise, 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 this guidance, our IT Investment Management framework (ITIM)[29] consists of five progressive stages of maturity for any given agency relative to selecting, controlling, and evaluating its investment management capabilities. (See fig. 2 for the five ITIM stages of maturity.) Stage 2 critical processes lay the foundation by establishing successful, predictable, and repeatable investment control processes at the project level. Stage 3 is where the agency moves from project-centric processes to portfolio-based processes and evaluates potential investments according to how well they support the agency's missions, strategies, and goals. Organizations implementing these Stages 2 and 3 practices have in place selection, control, and evaluation processes that are consistent with the Clinger-Cohen Act.[30] Stages 4 and 5 require the use of evaluation

---

[28]GAO-04-394G; GAO/AIMD-10.1.13; GAO, *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1994); and OMB, *Evaluating Information Technology Investments, A Practical Guide* (Washington, D.C.: November 1995).

[29]GAO-04-394G.

[30]40 U.S.C. §§ 11311-11313.

techniques to continuously improve both investment processes and portfolios in order to better achieve strategic outcomes.

**Figure 2: The Five ITIM Stages of Maturity with Critical Processes**

| Maturity stages | Critical processes |
|---|---|
| **Stage 5:** Leveraging IT for strategic outcomes | - Optimizing the investment process<br>- Using IT to drive strategic business change |
| **Stage 4:** Improving the investment process | - Improving the portfolio's performance<br>- Managing the succession of information systems |
| **Stage 3:** Developing a complete investment portfolio | - Defining the portfolio criteria<br>- Creating the portfolio<br>- Evaluating the portfolio<br>- Conducting postimplementation reviews |
| **Stage 2:** Building the investment foundation | - Instituting the investment board<br>- Meeting business needs<br>- Selecting an investment<br>- Providing investment oversight<br>- Capturing investment information |
| **Stage 1:** Creating investment awareness | *IT spending without disciplined investment processes* |

Source: GAO.

The overriding purpose of the framework is to encourage investment selection, control, and evaluate processes that promote business value and mission performance, reduce risk, and increase accountability and transparency. We have used the framework in several of our evaluations,[31] and a number of agencies have adopted it. With the exception of the first stage, each maturity stage is composed of "critical processes" that must be implemented and institutionalized in order for the organization to achieve that stage. Each ITIM critical process consists of "key practices"—to include organizational structures, policies, and procedures—that must be

---

[31]GAO, *Information Technology: Centers for Medicare & Medicaid Services Needs to Establish Critical Investment Management Capabilities*, GAO-06-12 (Washington, D.C.: Oct. 28, 2005); GAO, *Information Technology: HHS Has Several Investment Management Capabilities in Place, but Needs to Address Key Weaknesses*, GAO-06-11 (Washington, D.C.: Oct. 28, 2005); GAO, *Information Technology: FAA Has Many Investment Management Capabilities in Place, but More Oversight of Operational Systems Is Needed*, GAO-04-822 (Washington, D.C.: Aug. 20, 2004); GAO, *Information Technology: Departmental Leadership Crucial to Success of Investment Reforms at Interior*, GAO-03-1028 (Washington, D.C.: Sept. 12, 2003); GAO, *Bureau of Land Management: Plan Needed to Sustain Progress in Establishing IT Investment Management Capabilities*, GAO-03-1025 (Washington, D.C.: Sept. 12, 2003); GAO, *United States Postal Service: Opportunities to Strengthen IT Investment Management Capabilities*, GAO-03-3 (Washington, D.C.: Oct. 15, 2002); and GAO, *Information Technology: DLA Needs to Strengthen Its Investment Management Capability*, GAO-02-314 (Washington, D.C.: Mar. 15, 2002).

executed to implement the critical process. Our research shows that agency efforts to improve investment management capabilities should focus on implementing all lower stage practices before addressing higher stage practices.

## DOD's Institutional Approach to Business Systems Modernization

In 2005, the department reassigned responsibility for providing executive leadership for the direction, oversight, and execution of its business systems modernization efforts to several entities. These entities and their responsibilities include the Defense Business Systems Management Committee (DBSMC), which serves as the highest ranking investment review and decision-making body for business systems modernization activities; the Principal Staff Assistants, who serve as the certification authorities for business system modernizations in their respective core business missions; the Investment Review Boards (IRB), which are chaired by the certifying authorities and form the review and decision-making bodies for business system investments in their respective areas of responsibility; and the Business Transformation Agency (BTA), which is responsible for supporting the DBSMC and the IRBs, and for leading and coordinating business transformation efforts across the department. DOD's component organizations, to varying degrees, have leveraged existing, and established new, business system governance bodies to support their respective investment precertification responsibilities.

Table 1 lists these entities and provides greater detail on their roles, responsibilities, and composition.

**Table 1: DOD Business Systems Modernization Governance Entities' Roles, Responsibilities, and Composition**

| Entity | Roles and responsibilities | Composition |
|---|---|---|
| DBSMC | • Provides strategic direction and plans for the business mission area[a] in coordination with the warfighting and enterprise information environment mission areas.<br><br>• Recommends policies and procedures required to integrate DOD business transformation and attain cross-department, end-to-end interoperability of business systems and processes.<br><br>• Serves as approving authority for business system modernization.<br><br>• Establishes policies and approves the business mission area[a] strategic plan, the enterprise transition plan for implementation for business systems modernization, the transformation program baseline, and the BEA. | Chaired by the Deputy Secretary of Defense; Vice Chair is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). Includes senior leadership in the Office of the Secretary of Defense, the military departments' 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. |
| Principal Staff Assistants/Certification Authorities | • Support the DBSMC's management of enterprise business IT investments.<br><br>• Serve as the certification authorities accountable for the obligation of funds for respective business system modernizations within designated core business missions.[b]<br><br>• Provide the DBSMC with recommendations for system investment approval. | Under Secretaries of Defense for Acquisition, Technology, and Logistics; Comptroller; and Personnel and Readiness. |
| IRBs | • Serve as the oversight and investment decision-making bodies for those business capabilities that support activities under their designated areas of responsibility.<br><br>• Recommend certification for all business systems investments costing more than $1 million that are integrated and compliant with the BEA. | Includes the Principal Staff Assistants; Joint Staff; ASD(NII)/CIO; core business mission area representatives; military departments; defense agencies; and combatant commands. |
| Component Pre-Certification Authority | • Ensures component-level investment review processes integrate with the Investment Management system.<br><br>• Identifies those component systems that require IRB certification and prepare, review, approve, validate and transfer investment documentation as required.<br><br>• Assesses and precertifies architecture compliance of component systems submitted for certification and annual review.<br><br>• Acts as the component's principal point of contact for communication with the IRBs. | Includes the Chief Information Officer from Air Force, the Principal Director of Governance, Acquisition, and Chief Knowledge Office from the Army; the Chief Information Officer from the Navy; and comparable representatives from other defense agencies. |

| Entity | Roles and responsibilities | Composition |
|---|---|---|
| BTA | • Operates under the authority of the USD(AT&L) under the direction of the Deputy Under Secretary of Defense for Business Transformation and the Deputy Under Secretary of Defense for Financial Management.<br><br>• Maintains and updates the department's BEA and enterprise transition plan.<br><br>• Ensures that functional priorities and requirements of various defense components, such as the Army and Defense Logistics Agency are reflected in the architecture.<br><br>• Ensures adoption of DOD-wide information and process standards as defined in the architecture.<br><br>• Serves as the day-to-day management entity of the business transformation effort at the DOD enterprise level.<br><br>• Provides support to the DBSMC and IRBs. | Comprised of eight directorates (Chief of Staff, Defense Business Systems Acquisition Executive, Enterprise Integration, Enterprise Planning and Investment, Priorities and Requirements Financial Management, Priorities and Requirements Human Resource Management, Priorities and Requirements Supply Chain Management, and Warfighter Support Office). |

Source: DOD.

[a]According to DOD, the business mission area is responsible for ensuring that capabilities, resources, and materiel are reliably delivered to the warfighter. Specifically, the business mission area addresses areas such as real property and human resources management.

[b]DOD has five core business missions: Human Resources Management, Weapon System Lifecycle Management, Materiel Supply and Service Management, Real Property and Installations Lifecycle Management, and Financial Management.

## Tiered Accountability

In 2005, DOD reported that it had adopted a "tiered accountability" approach to business transformation. Under this approach, responsibility and accountability for business architectures and systems investment management are assigned to different levels in the organization. For example, the BTA is responsible for developing the corporate BEA (i.e., the thin layer of corporate policies, capabilities, standards, rules), and the associated enterprise transition plan (ETP). The components are responsible for defining a component-level architecture and transition plans associated with their own tier of responsibility and for doing so in a manner that is aligned with (i.e., does not violate) the corporate BEA. Similarly, program managers are responsible for developing program-level architectures and plans and ensuring alignment with the architectures and transition plans above them. This concept is to allow for autonomy while also ensuring linkages and alignment from the program level through the component level to the enterprise level. Table 2 describes the four investment tiers and identifies the associated reviewing and approving entities.

**Table 2: DOD Investment Tiers**

|  | Tier description | Reviewing/Approving entities |
|---|---|---|
| Tier 1 | MDAP[a] or MAIS[b] | IRB and DBSMC |
| Tier 2 | Exceeding $10 million in total development/modernization costs, but not designated as a MAIS or MDAP | IRB and DBSMC |
| Tier 3 | Exceeding $1 million and up to $10 million in total development/modernization costs | IRB and DBSMC |
| Tier 4 | Investment funding required up to $1 million | Component-level review only (unless the system or line of business it supports is designated as special interest by the Certification Authority) |

Source: DOD.

[a]A MDAP is an acquisition program so designated by the Under Secretary of Defense for Acquisition, Technology, and Logistics or that is estimated to require an eventual total expenditure for research, development, and test and evaluation of more than $365 million (fiscal year 2000 constant dollars) or, for procurement, of more than $2.190 billion (fiscal year 2000 constant dollars).

[b]A MAIS 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).

## Summary of Fiscal Year 2005 National Defense Authorization Act Requirements

Congress included six provisions in the fiscal year 2005 National Defense Authorization Act[32] that are aimed at ensuring DOD's development of a well-defined BEA and associated ETP, as well as the establishment and implementation of effective investment management structures and processes. The requirements are as follows:

1.  Develop a BEA that includes an information infrastructure that, at a minimum, would:

*   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;
*   provide for the systematic measurement of performance, including the ability to produce timely, relevant, and reliable cost information;

---

[32]Ronald 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).

- include policies, procedures, data standards, and system interface requirements that are to be applied uniformly throughout the department; and
- be consistent with OMB policies and procedures.

2. Develop an ETP for implementing the architecture that includes:

- an acquisition strategy for new systems needed to complete the enterprise architecture;
- a list and schedule of legacy business systems to be terminated;
- a list and strategy of modifications to legacy business systems; and
- time-phased milestones, performance metrics, and a statement of financial and non-financial resource needs.

3. Identify each business system proposed for funding in DOD's fiscal year budget submissions and include:

- description of the certification made on each business system proposed for funding in that budget;
- funds, identified by appropriations, for current services and for business systems modernization; and
- the designated approval authority for each business system.

4. Delegate the responsibility for business systems to designated approval authorities within the Office of the Secretary of Defense.

5. Require each approval authority to establish investment review structures and processes, including a hierarchy of IRBs—each with appropriate representation from across the department. The review process must cover:

- review and approval of each business system by an IRB before funds are obligated;
- at least an annual review of every business system investment;
- use of threshold criteria to ensure an appropriate level of review and accountability;
- use of procedures for making architecture compliance certifications;
- use of procedures consistent with DOD guidance; and
- incorporation of common decision criteria.

6. Effective October 1, 2005, DOD may not obligate appropriated funds for a defense business system modernization with a total cost of more than $1 million unless the approval authority certifies that the business system modernization:

- complies with the BEA and
- is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or is necessary to prevent a significant adverse effect on an essential project in consideration of alternative solutions, and the certification is approved by the DBSMC.

## Summary of Recent GAO Reviews of DOD's Business Systems Modernization and Business Transformation Efforts

In November 2005,[33] May 2006,[34] and May 2007,[35] we reported that DOD had partially satisfied four of the six business system modernization requirements in the fiscal year 2005 National Defense Authorization Act[36] relative to architecture development, transition plan development, budgetary disclosure, and investment review. In addition, we reported that it had fully satisfied the requirement concerning designated approval authorities and it was in the process of satisfying the last requirement for certification and approval of modernizations costing in excess of $1 million. As a result, each report concluded that the department had made important progress in defining and beginning to implement institutional management controls (i.e., processes, structures, and tools). However, each report also concluded that much remained to be accomplished relative to the act's requirements and relevant guidance. Among other things, this included developing component architectures that are aligned with the corporate BEA and ensuring that investment review and approval processes are fully developed and institutionally implemented across all organizational levels.

Notwithstanding this progress on business systems modernization, we previously reported[37] and more recently testified in February 2008[38] that two items remained to be done before DOD's overall business transformation efforts, which include business systems modernization, would be on a sustainable path to success. First, DOD had yet to establish a strategic planning process that results in a comprehensive, integrated,

---

[33]GAO-06-219.

[34]GAO-06-658.

[35]GAO-07-733.

[36]Ronald 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).

[37]GAO-07-1072.

[38]GAO-08-462T.

and enterprisewide plan or set of plans that would guide transformation. Second, DOD had yet to designate a senior official who could provide full-time attention and oversight to the business transformation effort. Subsequently, the National Defense Authorization Act for Fiscal Year 2008 designated the Deputy Secretary of Defense as the department's Chief Management Officer (CMO), created a Deputy CMO position, and designated the undersecretaries of each military department as CMOs for their respective departments.[39] The act also required the Secretary of Defense, acting through the CMO, to develop a strategic management plan that, among other things, is to include a detailed description of performance goals and measures for improving and evaluating the overall efficiency and effectiveness of the business operations of the department. According to DOD, steps have been taken and are ongoing to address these provisions.

We also testified in February 2008 that DOD continues to take steps to comply with key business systems modernization legislative requirements, but that much remained to be accomplished before the full intent of this legislation would be achieved. In particular, we stated that DOD's BEA, while addressing several issues previously reported by us, was still not sufficiently complete to effectively and efficiently guide and constrain business system investments across all levels of the department. Most notably, the BEA did not yet include well-defined architectures for DOD's components, and DOD's strategy for "federating" or extending its architecture to the military departments and defense agencies was still evolving and had yet to be implemented. In addition, the scope and content of the department's ETP still did not address DOD's complete portfolio of IT investments. We also testified that while the department had established and begun to implement legislatively mandated corporate investment review structures and processes, neither DOD nor the military departments had done so in a manner that was fully consistent with relevant guidance.

# DOD Is Continuing to Improve Its Approach to Modernizing Business Systems

DOD continues to take steps to comply with the requirements of the act and to satisfy relevant systems modernization management guidance. In particular, on March 14, 2008, DOD released an update to its BEA (version 5.0) and ETP, and issued its annual report to Congress describing steps that have been taken and are planned relative to the act's requirements, among other things. Collectively, these steps address several legislative

---

[39]Pub. L. No. 100-181 § 904, 122 Stat. 3, 273-75 (Jan. 28, 2008).

provisions and best practices concerning the BEA, transition plan, budgetary disclosure, and investment review of systems costing in excess of $1 million. However, additional steps are needed to fully comply with the act and relevant guidance. Most notably, the department has yet to extend and evolve its corporate BEA to the department's component organizations' (military departments and defense agencies) architectures and fully define IT investment management policies and procedures at the corporate and component levels. BTA officials agree that additional steps are needed to fully implement the act's requirements and our related recommendations. According to these officials, DOD leadership is committed to fully addressing these areas and efforts are planned and under way to do so.

## DOD Continues to Improve Its Corporate BEA, but Component Architectures Remain a Challenge

Among other things, the act requires DOD to develop a BEA that would cover all defense business systems and the functions and activities supported by defense business systems and enable the entire department to (1) comply with all federal accounting, financial management, and reporting requirements, (2) routinely produce timely, accurate, and reliable financial information for management purposes, and (3) include policies, procedures, data standards, and system interface requirements that are to be applied throughout the department. As such, the act provides for an architecture that extends to all defense organizational components. In 2006, the department adopted an incremental and federated approach to developing such an architecture. Under this approach, the department committed to releasing new versions of its BEA every 6 months that would include a corporate BEA that was augmented by a coherent family of component architectures. As we have previously reported, such an approach is consistent with best practices and appropriate given the DOD's scope and size.

In 2007,[40] we reported that the then current version of the BEA (version 4.1) resolved several of the architecture gaps associated with the prior version and added content proposed by DOD stakeholders,[41] but that gaps

---

[40] GAO-07-733.

[41] According to DOD, stakeholders include representatives from the core business mission areas through the Business Enterprise Priorities (e.g, Personnel Visibility, Acquisition Visibility, Common Supplier Engagement, Materiel Visibility, Real Property Accountability, and Financial Visibility). They also will include representatives from the component organizations that must align their architectures to the corporate BEA, the program that must align to the corporate BEA and the component architectures, the IRBs that use the BEA to guide and constrain investments, and contractors that support programs in building and configuring architecturally compliant systems.

still remained. On March 14, 2008, DOD released BEA 5.0 which addresses some of these remaining gaps. For example, it improves the Financial Visibility business enterprise area by expanding the Standard Financial Information Structure data elements (i.e., types of data) associated with information exchanges among operational nodes (e.g., organizational units or system functions) to include data attributes (characteristics of data elements). In addition, the latest version introduces data standards for the Enterprise Funds Distribution initiative. Together, these additions bolster the department's efforts to standardize financial data across DOD so that information is available to inform corporate decision making.

Version 5.0 of the BEA also addresses, to varying degrees, missing elements, inconsistencies, and usability issues that we previously identified. Examples of these improvements and remaining issues are summarized below.

- The latest version includes performance metrics for the business capabilities within enterprise priority areas, including actual performance relative to performance targets that are to be met. For example, it states that 62 percent of DOD assets are now using the Department of the Treasury's United States Standard General Ledger[42] compliant formats, as compared to a target of 100 percent. Further, this version provides actual baseline performance for operational activities (e.g., "Manage Audit and Oversight of Contractor"). As we previously reported,[43] performance models are an essential part of any architecture because having defined performance baselines to measure actual performance against provides the means for knowing whether the intended mission value to be delivered by each business process is actually being realized.

- The latest version includes important "As Is" information (e.g., current capability problems and limitations that enterprise priorities are to address and their root causes) for all six business enterprise priorities. As we previously reported, such "As Is" content is essential for analyzing capability gaps that in turn inform the plan for transitioning from the "As Is" to the "To Be" environments.

- The latest version includes 1,201 new business rules. As we previously reported, business rules are important because they explicitly translate

---

[42]The United States Standard General Ledger provides a uniform chart of accounts and technical guidance used in standardizing federal agency accounting.

[43]GAO-04-777; GAO-03-584G.

business policies and procedures into specific, unambiguous rules that govern what can and cannot be done. As such, they facilitate consistent implementation of policies and procedures. Examples of new business rules are that (1) each request for commercial export of DOD technology must be processed within 30 days of request from the Department of State or the Department of Commerce and (2) DOD must first seek to acquire commercial items before developing military unique material. In addition to adding business rules, Version 5.0 reflects the deletion of 1,046 business rules that were no longer applicable and thus obsolete.

Notwithstanding these additions and deletions, BEA 5.0 still does not provide business rules for all business processes. For example, there are no business rules for the "Perform Acceptance Procedures for Other Goods and Services" business process under the Common Supplier Engagement enterprise priority area. Also, business rules are defined at inconsistent levels of detail. For example, the Travel Authorization business rule states that each travel authorization must be processed in accordance with the Allowance Law, however, it does not identify the specific conditions that must be met. In contrast, the Trial Balance Reporting business rule is more explicitly defined, specifically citing the conditions under which actions are to be taken. Without well-defined business rules, policies and procedures can be implemented inconsistently because they will be interpreted differently by different organizations.

- The latest version includes updates on the information that flows among operational nodes (i.e., organizations, business operations, and system elements). Information flows are important because they define what information is needed and where and how the information moves to and from operational entities. In particular, Version 5.0 adds 240 new information exchanges (e.g., Accounts Payable) among business operations and 28 data exchanges (e.g., Acknowledge Inter-governmental Order) among system elements. However, it still does not provide information flows for all organizational units. For example, it does not identify information exchanges among the organizations that support the Human Resources Management enterprise priority area, and continues to lack information flows among DOD corporate and components organizations. Without such information exchanges, a common understanding of the semantic meaning of the information moving among these organizations does not exist. Moreover, Version 5.0 contains information exchanges (e.g., Accounts Payable Account) that are not attached or linked to any operational nodes. Further, this version's information-related architecture products contain inconsistencies. For example, "Acceptance Results" is identified as a new information

exchange in the integrated dictionary, but it is not in the operational information exchange product.

- The latest version expands on the operational activities that are or will be performed at each location and by each organization. For example, it now identifies the Defense Logistics Agency as one of the organizations involved in the "Authorize Return or Disposal" activity. However, as was the case with BEA Version 4.1, not all operational activities are assigned to an organization. For example, the "Manage Capabilities Based Acquisition" activity is not assigned. In addition, BEA 5.0 still does not include the roles and responsibilities of organizations performing the same operational activity, which is important because not doing so can result in either duplicative organizational efforts or gaps in activity coverage. Moreover, BEA 5.0 still does not include the Foreign Military Sales operational activity, which affects multiple DOD business missions and organizations.

- The latest version continues to lack important security architecture content. For example, while DOD officials told us that the Enterprise Information Environment Mission Area will provide infrastructure information assurance services (e.g., secure, reliable messaging) for business systems and applications, this information is not reflected in the latest version. Also, this version still does not describe relevant information assurance requirements contained in laws, regulations, and policies, or provide a reference to where these requirements are described. Such information is essential to adequately reflect security in the BEA, and thereby ensure that designs for business systems, applications, and services comply with applicable information assurance requirements.

Beyond the above discussed limitations, Version 5.0 also continues to represent only the thin layer of corporate architectural policies, capabilities, rules, and standards that apply DOD-wide (i.e., to all DOD federation members). This means that Version 5.0 appropriately focuses on addressing a limited set of enterprise-level (DOD-wide) priorities, and providing the overarching and common architectural context that the distinct and substantially autonomous member (i.e., component) architectures inherit. However, this also means that Version 5.0 does not provide the total federated family of DOD parent and subsidiary architectures for the business mission area that are needed to comply with the act.

To produce the federated BEA, the BTA released an update to its federation strategy in January 2008. (See fig. 3 for a simplified diagram of DOD's federated BEA.) In April 2007,[44] we reported on the prior version of this strategy, concluding that while it provided a foundation on which to build and align DOD's parent BEA with its subsidiary architectures, it lacked sufficient details to permit effective and efficient execution. Accordingly, we made recommendations to improve the strategy.
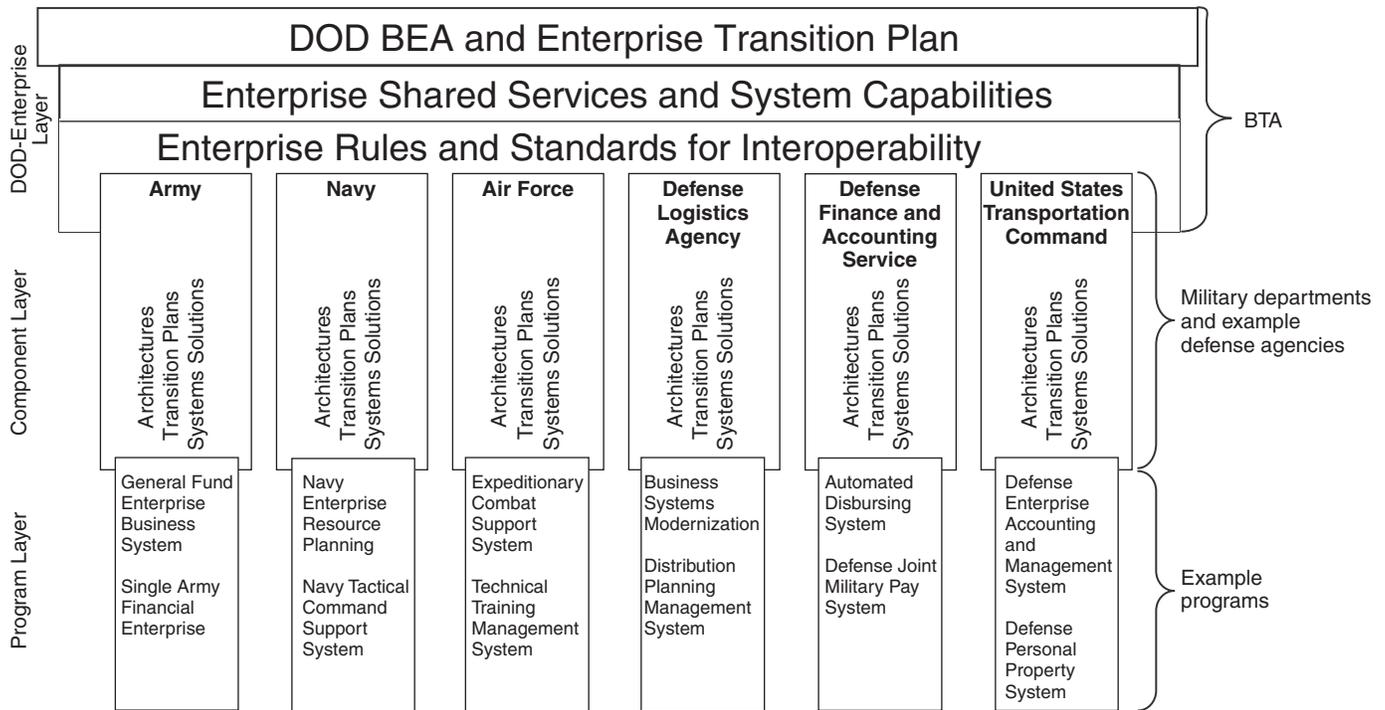
The updated strategy, along with the associated global information grid[45] (GIG) strategy,[46] partially addresses our recommendations. For example, the strategies now provide high-level roles and responsibilities for federating the architecture and additional definition around the tasks needed to achieve alignment among DOD and component architectures. In particular, the strategy for the business mission area provides for conducting pilot programs across the components to demonstrate the technical feasibility of architecture federation. BTA and CIO officials described the strategy for federating DOD's architectures as still evolving. They added that lessons learned from the pilots will be used to improve and update the strategies. They also noted that subsequent releases of the corporate BEA will reflect the evolving federation strategy by, for example, defining enforceable interfaces to ensure interoperability and information sharing.

---

[44]GAO-07-451.

[45]According to DOD, the GlG consists of a 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, policymakers, and support personnel, and as such represents the department's IT architecture.

[46]The GIG strategy provides for federating the many and varied architectures across the department's four mission areas—Warfighting, Business, DOD Intelligence, and Enterprise Information Environment. It was issued in August 2007 by the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer (ASD(NII)/CIO).

**Figure 3: Simplified Diagram of DOD's Business Mission Area Federated Architecture**



| | DOD BEA and Enterprise Transition Plan | |
|---|---|---|
| **DOD-Enterprise Layer** | Enterprise Shared Services and System Capabilities | BTA |
| | Enterprise Rules and Standards for Interoperability | |

| Army | Navy | Air Force | Defense Logistics Agency | Defense Finance and Accounting Service | United States Transportation Command | |
|---|---|---|---|---|---|---|
| Architectures / Transition Plans / Systems Solutions | Architectures / Transition Plans / Systems Solutions | Architectures / Transition Plans / Systems Solutions | Architectures / Transition Plans / Systems Solutions | Architectures / Transition Plans / Systems Solutions | Architectures / Transition Plans / Systems Solutions | Military departments and example defense agencies |
| General Fund Enterprise Business System / Single Army Financial Enterprise | Navy Enterprise Resource Planning / Navy Tactical Command Support System | Expeditionary Combat Support System / Technical Training Management System | Business Systems Modernization / Distribution Planning Management System | Automated Disbursing System / Defense Joint Military Pay System | Defense Enterprise Accounting and Management System / Defense Personal Property System | Example programs |

*Component Layer* / *Program Layer*

Source: GAO analysis of DOD data.

To help assist the department in its BEA federation efforts, we have made a number of recommendations. While DOD agreed with these recommendations, it did not implement one related to its latest annual report. Specifically, we previously recommended that DOD include in its annual report, required under the National Defense Authorization Act for Fiscal Year 2005, the results of its BEA independent verification and validation (IV&V) contractor's assessment of the completeness, consistency, understandability, and usability of the federated family of architectures. However, its latest annual report does not include this information. According to BTA officials, this is because the contractor's report was not finalized in time to include the results. While we have yet to receive either the contractor's statement of work or the results of the contractor's assessments, BTA officials provided us with a report dated April 11, 2008, that summarizes selected IV&V contractor observations and recommendations relative to the Version 5.0's ability to provide a foundation for BEA federation. Overall, the summary confirms our findings by stating that while the BEA provides a foundation for

**GAO-08-705 DOD Business System Modernization**

federation, much remains to be done before the department will have a complete family of architectures. In this regard, it provides several recommendations, such as having BTA track, measure, and report on the adoption of shared vocabularies and standards within the component architectures. However, the summary does not demonstrate that the IV&V contractor is being used to address the full scope of our recommendation. For example, the summary does not address the extent to which the department's federated family of architectures, including the related transition plan(s), are complete, consistent, understandable, and useable.

The challenges that the department faces in federating its BEA, and the importance of disclosing to congressional defense committees the state of its federation efforts, are amplified by our recent report on the current state of the military departments' enterprise architecture programs. Specifically, we reported in May 2008,[47] that none of the three military departments could demonstrate through verifiable documentation that it had established all of the core foundational commitments and capabilities needed to effectively manage the development, maintenance, and implementation of an architecture, although in relative terms the state of the Air Force's architecture efforts was well ahead of those of the Navy and Army. Examples of their architecture limitations are discussed below.

- None of the military departments had fully defined its "As Is" and "To Be" architecture environments and associated transition plans. This is important because without a full understanding of architecture-based capability gaps, the departments would not have an adequate basis for defining and sequencing its ongoing and planned business system investments.

- None of the military departments had fully addressed security as part of its respective "As Is" and "To Be" environments. This is important because security is relevant and essential to every aspect of an organization's operations, and therefore the nature and substance of institutionalized security requirements, controls, and standards should be embedded throughout the architecture, and reflected in each system investment.

- None of the military departments was using an IV&V agent to help ensure the quality of its architecture products. IV&V is a proven means for obtaining unbiased insight into such essential architecture qualities as completeness, understandability, usability, and consistency.

---

[47]GAO-08-519.

- None of the military departments had established a committee or group with representation from across the enterprise to direct, oversee, and approve its architecture. This is significant because the architecture is a corporate asset that needs to be enterprisewide in scope and endorsed by senior leadership if it is to be leveraged for optimizing operational and technology change.

- None of the military departments could demonstrate that its IT investments were actually in compliance with its architectures. This is relevant because the benefits from using an architecture, such as improved information sharing, increased consolidation, enhanced productivity, and lower costs, cannot be fully realized unless individual investments are actually in compliance with, among other things, architectural rules and standards.

   To address these limitations, we have made recommendations aimed at improving the management and content of these architectures. DOD agreed with our recommendations. Until DOD has a well-defined family of architectures for its business mission area, it will not fully satisfy the requirements of the act and it will remain challenged in its ability to effectively manage its business system modernization efforts.

## DOD Continues to Expand and Update Its Enterprise Transition Plan, but Important Elements and Component Plans Are Still Missing

Among other things, the act requires DOD to develop an ETP for implementing its BEA that includes listings of the legacy systems that will and will not be part of the target business systems environment and specific time-phased milestones and performance metrics for each business system investment.

In 2007,[48] we reported that the then version of the ETP addressed several of the missing elements that we previously identified relative to the act's requirements and relevant guidance. However, we also reported that the ETP was limited in several ways. On March 15, 2008, DOD released the latest version of its ETP, which provides required information on 102 programs (systems and initiatives) that are linked to key transformational objectives. For example, it includes specific time-phased milestones[49] for about 90 business system programs and performance metrics for about 75 of these. Further, the latest version of the ETP discusses progress made on

---

[48]GAO-07-733.

[49]The time-phased milestones refer to milestones, such as initial operating capability, full operating capability, technology development phase, and system development and demonstration phase.

business system investments over the last 6 months, as well as descriptions of planned near-term activities (i.e., next 6 months).

- The Defense Integrated Military Human Resources System program completed all interface designs required for system deployment to the Army and to defense agencies, and over half of the interface designs required for deployment to the Air Force. It also states that system interface testing and operational testing for the Army deployment will be completed in the next 6 months.[50]

- The Contractor Performance Assessment Reporting System was fully implemented following replacement of a proprietary software product with an open source product and rehosting of this product to a new facility. As a result, improvements in system performance, reliability, and security were attained.

  This version also partially addresses issues that we identified in our prior report.[51] Examples of improvements and remaining issues are summarized here.

- The latest version contains the results of analyses of gaps between its "As Is" and "To Be" architectural environments, in which capability and performance shortfalls are described and investments (such as transformation initiatives and systems) that are to address these shortfalls are identified. It also discusses planned and ongoing gap analyses. For example, it relates the DOD Electronic Mall investment to the Common Supplier Engagement business enterprise priority area and describes how it will address business capability gaps by providing access to off-the-shelf finished goods and services from both commercial and government sources. It also describes how related performance shortfalls will be addressed through shorter logistics response time, improved visibility of sources of supplies, one-stop tracking of order status, and improved ability to shop for best price. As we stated, determining how business capability gaps between the baseline and target architecture are to be addressed for all priority areas is key to the department's transition plan's ability to support informed investment selection and control decisions.

---

[50]We did not independently verify the reliability of this reported progress because we have an ongoing review of this program.

[51]GAO-07-733.

- The latest version provides a range of information for the 102 systems and initiatives identified, such as 3 years of budget information for 67 of these systems and initiatives. However, as we reported last year,[52] the plan has yet to address our prior finding for including system and budget information for investments by 13 of DOD's 15 agencies[53] and for eight of its nine combatant commands.[54] At that time, BTA officials stated that information for these defense agencies and combatant commands was excluded because the ETP focused on those business-related organizations having the majority of the tier 1 and 2 business investments, and the majority of the defense agencies and combatant commands do not have investments that meet this threshold criteria. However, not all DOD components have developed subordinate transition plans. For example, we recently reported that only one military department, the Air Force, had developed a transition plan and that this plan was limited because it did not include an analysis of the gap in capabilities between the military departments' "As Is" and "To Be" environments. This means that, similar to DOD's federated BEA, a complete family of DOD and component transition plans does not yet exist.

- The latest version provides performance measures for both enterprise and component investments (i.e., programs), including key milestones (e.g., initial operating capability). However, it does not include other important information needed to understand the sequencing of these investments. In particular, the planned investments are not sequenced based on a range of important factors cited in federal guidance, such 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

---

[52]GAO-07-733.

[53]DOD included system and budget information for the Defense Financial and Accounting Service and Defense Logistics Agency in the transition plan. DOD did not include this information for the following defense agencies: (1) Missile Defense Agency, (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 Geospatial-Intelligence Agency, and (13) National Security Agency.

[54]DOD 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.

of competing investments.[55] While the ETP has begun to incorporate some top-down analysis based on gaps in the business enterprise priorities, the plan continues to be largely based on a bottom-up planning process in which ongoing programs were examined and categorized in the plan around business enterprise priorities. For example, many of these investments are dependent on Net-Centric Enterprise Services (NCES)[56] for its core services, and as such the plans and milestones for each should reflect the incremental capability deployment of NCES. According to the BTA official responsible for the ETP, the investments were sequenced based on only fiscal year budgetary constraints. However, BTA officials said that they intend to depict investment dependencies in future versions of the ETP, especially program-to-program dependencies associated with adoption of a service-oriented architecture approach.

- The latest version of the ETP also includes discussion of how the department plans to use enterprise application integration,[57] including plans, methods, and tools for reusing applications that already exist while also adding new applications and databases. However, as we reported last year,[58] this discussion lacks specifics on which investments will reuse which applications.

According to BTA officials, a number of actions are envisioned to address the above cited areas and further improve the ETP, such as adding the results of capability gap analyses for all business priority areas, including tier 1 and 2 programs for all components, and recognizing dependencies among investments. Until the ETP, or a federated family of such plans, either directly or by reference includes relevant information on the full inventory of investments across the department (and does so in a manner that reflects consideration of the range of variables associated with a well-defined transition plan, such as timing dependencies among investments

---

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

[56]NCES is intended to provide capabilities that are key to enabling ubiquitous access to reliable decision-quality information. NCES capabilities can be packaged into four product lines: service-oriented architecture foundation (e.g., security and information assurance), collaboration (e.g., application sharing), content discovery and delivery (e.g., delivering information across the enterprise), and portal (e.g., user-defined Web-based presentation).

[57]Enterprise application integration software is a commercial software product, commonly referred to as middleware, to permit two or more incompatible systems to exchange data from different databases.

[58]GAO-07-733.

and the department's capability to manage them), it will not have a sufficient basis for informed investment decision making regarding disposition of the department's existing inventory of systems or for sequencing the introduction of modernized systems. To help DOD in addressing its transition planning challenges, we have previously made recommendations that the department is in the process of addressing.

## DOD's Fiscal Year 2009 Budget Submission Includes Key Information on Business Systems

Among other things, the act requires DOD's annual IT budget submission to include key information on each business system for which funding is being requested, such as the system's designated approval authority and the appropriation type and amount of funds associated with development/modernization and current services (i.e., operation and maintenance).

The department's fiscal year 2009 budget submission includes a range of information for the approximately 3,000 business system investments for which DOD is requesting funding. Of these, 273 involve modernization/development activities. For each of the 273, the information provided includes the system's (1) name, (2) approval authority, and (3) appropriation type. The submission also identifies the amount of the fiscal year 2009 request that is for development/modernization versus operations/maintenance. For example, the Army's General Fund Enterprise Business System, the amount of modernization funds related to "Other Procurement, Army" and "Research, Development, Testing and Evaluation, Army" are identified. For systems in excess of $1 million in modernization funding, the submission also cites its certification status (e.g., approved, approved with conditions, not applicable, and withdrawing) and the DBSMC approval date, where applicable.

## DOD and Military Departments Have Partially Established Key Investment Management Structures, but Have Yet to Fully Define Related Policies and Procedures

The National Defense Authorization Act for Fiscal Year 2005 requires DOD to establish business system investment review structures, such as the previously mentioned DBSMC and five IRBs, and processes that are consistent with the investment management provisions of the Clinger-Cohen Act.[59] As we have previously reported, organizations that have satisfied stages 2 and 3 of our ITIM framework have established the investment selection, control, and evaluation structures, and the related policies, procedures, and practices that are consistent with the investment management provisions of the Clinger-Cohen Act.

---

[59]40 U.S.C. § 11312.

DOD and the Air Force have established the kind of investment management structures provided for in the act and our ITIM framework.[60] However, the Navy has not. Moreover, neither DOD, the Air Force, nor the Navy have defined the full range of related investment management policies and procedures that our framework identifies as necessary to effectively manage investments as individual business system projects (stage 2) and as portfolios of projects (stage 3). Accordingly, we made recommendations to address the limitations that the department is addressing. Until all of DOD has in place these requisite investment management structures and supporting policies and procedures, the billions of dollars that the department and its components invest annually in business systems will remain at risk.

**Investment Management Structures Have Been Partially Established**

DOD has partially established the organizational structures that are associated with Stages 2 and 3 of our framework. Specifically, we reported in May 2007[61] that the department had established an enterprisewide investment board and four subordinate boards, and assigned them responsibility for business systems investment governance, including conducting investment certification and approval reviews and annual reviews as provided for in the act. The enterprisewide board—the DBSMC—is composed of senior executives, such as the Deputy Secretary of Defense and the ASD(NII)/CIO, as provided for in the act. Among other things, the DBSMC is responsible for establishing and implementing policies governing the organization's investment process and approving lower-level investment board processes and procedures. The subordinate boards include four IRBs[62] that are composed of senior officials representing their respective business areas, including representatives from the combatant commands, defense agencies, military departments, and Joint Chiefs of Staff. Among other things, the IRBs are responsible and accountable for overseeing and controlling certain business system investments, including ensuring compliance and consistency with the BEA. The department has also assigned responsibility to the USD(AT&L) for managing business system portfolio selection criteria.

However, as we reported last year, the department has yet to establish the fifth review board required pursuant to the act, the Enterprise Information

---

[60]GAO-04-394G.

[61]GAO-07-733.

[62]The four IRBs are for (1) Financial Management, (2) Weapon Systems Lifecycle Management and Materiel Supply and Services Management, (3) Real Property and Installations Lifecycle Management, and (4) Human Resources Management.

Environment Mission Area[63] IRB. According to ASD(NII)/CIO officials, this board has been operating under a draft concept of operations for about 2 years, but has not been chartered because of issues surrounding its authority across IT infrastructure-related investments. However, they stated that a policy is expected to be approved and issued by the end of May 2008 that will, among other things, establish a CIO Enterprise Guidance Board that will meet the act's requirements for Enterprise Information Environment Mission Area IRB. Specifically, the policy is to provide the Enterprise Guidance Board with DOD-wide oversight of IT investments.

With respect to the military departments' investment management structures, we reported in October 2007[64] that the Air Force had established the organizational structures associated with stages 2 and 3 of our framework. Specifically, it has instituted a business systems IRB, called the Senior Working Group, consisting of senior executives from the functional business units, including the Office of the Air Force CIO. This group has been assigned responsibility for business system investment governance, including conducting investment precertification and approval reviews and annual reviews, as required by the act. However, we also reported in October 2007[65] that the Navy had not established such investment management structures. Specifically, it did not have an enterprisewide IRB, composed of senior executives from its IT and business units, to define and implement a Navy-wide business system governance process. Without such structures, we concluded that the Navy's ability to ensure that business system investment decisions are made consistently and reflect the needs of the organization is limited. Accordingly we made a recommendation to the Navy for establishing these management structures.

**Investment Management Policies and Procedures Are Lacking at Both Corporate and Component Levels**

Neither DOD nor the departments of the Air Force and the Navy have defined the full range of policies and procedures needed to effectively support project-level (stage 2) and portfolio-based (stage 3) investment management practices. While the department is in the process of

---

[63]The Enterprise Information Environment Mission Area enables the functions of the other mission areas (e.g., Warfighting Mission Area, Business Mission Area, and Defense Intelligence Mission Area) and encompasses communications, computing, and core enterprise service systems, equipment, or software that provides a common information capability or service for enterprise use.

[64]GAO-08-52.

[65]GAO-08-53.

developing a new methodology for managing its business system investments throughout their life cycles that it reports will address this lack of policies and procedures, this new methodology is still in draft, has not been approved, and we have yet to be provided a copy. Until these missing policies and procedures are defined, it is unlikely that the thousands of DOD business system investments will be managed in a consistent, repeatable, and effective manner.

To DOD's credit, it has defined corporate policies and procedures relative to several key practices in our ITIM framework that are associated with project-level investment management (stage 2). However, it does not have the full range of project-level policies and procedures needed for effective investment management. Specifically, we reported in May 2007[66] that DOD had satisfied several policy- and procedure-related stage 2 practices, such as requiring that systems support ongoing and future business needs through alignment with the BEA, having procedures for identifying and collecting information about these systems to support DBSMC and IRB investment decision making, and assigning responsibility for ensuring that the information collected about projects meets the needs of DOD's investment review structures and processes. However, we also reported that it had not, for example, developed policies and procedures outlining how the DBSMC/IRB investment review processes are to be coordinated with other decision-support processes used at DOD, such as the Joint Capabilities Integration and Development System; the Planning, Programming, Budgeting, and Execution process; and the Defense Acquisition System.[67] Without clear linkage among these processes, inconsistent and uninformed decision making may result. Furthermore, without considering component and corporate budget constraints and opportunities, the IRBs risk making investment decisions that do not effectively consider the relative merits of various projects and systems when funding limitations exists.

Other important project-level, as well as portfolio-based, investment management policies and procedures that we reported as lacking include

---

[66]GAO-07-733.

[67]The Joint Capabilities Integration and Development System is a need-driven management system used to identify future capabilities for DOD; the Planning, Programming, Budgeting, and Execution process is a calendar-driven management system for allocating resources and comprises four phases--planning, programming, budgeting, and executing--that define how budgets for each DOD component and the department as a whole are created, vetted, and executed; and the Defense Acquisition System is an event-driven system for managing product development and procurement and guides the acquisition process for DOD.

ones that (1) specify how the full range of cost, schedule, and benefit data accessible by the IRBs is to be used in making selection decisions; (2) ensure sufficient oversight and visibility into component-level (e.g., Air Force and Navy) investment management activities, including component reviews of systems in operations and maintenance; (3) define the criteria to be used for making portfolio selection decisions; (4) create the portfolio of business systems investments; and (5) provide for conducting postimplementation reviews of these investments. DOD agreed with our findings and described actions that it planned to take to address our recommendations, including developing a new life cycle management methodology for business systems. In addition, it stated that while its actions would improve the department's corporate policies and procedures for business system investments, each component is responsible for developing and executing investment management policies and procedures needed to manage its business systems.

In this regard, the military departments also have not developed the full range of related investment management policies and procedures needed to execute the project and portfolio-level practices reflected in our ITIM framework. Specifically, we reported in October 2007[68] that the state of the Air Force and the Navy's investment management policies and procedures were similar to that of DOD in that while several of our ITIM framework stage 2 practices were satisfied, others were not, and none of the stage 3 practices were satisfied. For example, both the Air Force and the Navy, to their credit, had developed procedures for identifying and collecting information about their business systems to support investment selection and control, and assigned responsibility for ensuring that the information collected during project identification meets the needs of the investment management process. However, neither the Air Force nor the Navy had fully documented policies and procedures for overseeing the management of business system investments and for developing and managing complete business systems investment portfolio(s). Among other things, they did not have policies and procedures that specify decision-making processes for program oversight and describe how corrective actions should be taken when projects deviate from their project management plans. Without such policies and procedures, we concluded that both are at risk of investing in systems that are duplicative, stovepiped, nonintegrated, and unnecessarily costly to manage, maintain, and operate. To address these areas, we made recommendations aimed at

---

[68]GAO-08-52; GAO-08-53.

implementing our framework's stage 2 and 3 practices, and DOD partially agreed with these recommendations.

DOD reports that it has begun to address our investment management findings and recommendations. Specifically,[69] it has drafted and is piloting aspects of (e.g., an Enterprise Risk Assessment Methodology) a new lifecycle management methodology, called the Business Capability Lifecycle (BCL). The annual report states that these pilots have validated the BCL and that interim guidance for major business systems[70] has been developed. However, the new methodology has yet to be approved. Further, BTA officials stated that plans for its finalization and full implementation have been placed on hold until the department has implemented the Chief Management Officer (CMO) provisions of the National Defense Authorization Act for Fiscal Year 2008.[71]

Based on a draft of the BCL and descriptions of it contained in the annual report and briefed to us by BTA officials, this new lifecycle methodology could address some, but not all, of the policy and procedure gaps that we have recently reported. For example, the BCL is to consolidate DOD's currently distinct and separate system requirements, acquisition, and architectural/investment oversight processes into a single governance process. However, while lack of integration among these separate processes is a limitation that reported with DOD's business system investment management policies and procedures, this limitation also included lack of integration with DOD's budgeting process. Unless this new lifecycle methodology incorporates DOD's funding process, the risk of the respective processes producing inconsistent investment decisions remains.

The following are other examples of investment management policy and procedure limitations cited in our recent reports that the draft of the BCL methodology does not fully address.

- The BCL does not apply to programs after they have completed development/modernization activities and are in an operations and

---

[69]GAO-07-538.

[70]DOD refers to these systems as Major Automated Information Systems.

[71]The National Defense Authorization Act for Fiscal Year 2008 designates the Deputy Secretary of Defense as its CMO, creates a Deputy CMO position within the department, and designates the undersecretaries of each military department as CMOs for their respective departments.

maintenance mode, except for certain programs designated as "special interest." As we recently reported,[72] our ITIM framework provides for including both new system development/acquisition investments and operations and maintenance of existing system investments in the investment management process. According to the department, it plans to examine the applicability of the BCL methodology to systems in operations and maintenance.

- The BCL does not address how the full range of cost, schedule, and benefit data is to be used by the IRBs when making their program certification decisions. Without documenting how such boards are to consider cost, schedule, and benefits factors when making these decisions, the department cannot ensure that the boards consistently and objectively select proposals that best meet the department's needs and priorities.

- The BCL does not provide for DOD-level oversight and visibility into component-level investment management activities, including component reviews of systems in operations and maintenance and smaller investments, commonly referred to as tier 4 investments.[73] This is particularly important because, as DOD reports, only 353 of about 3,000 total business systems have completed the IRB certification process and have been approved by the DBSMC. This means that the vast majority of business systems have not come before the IRBs and DBSMC, and thus are reviewed and approved only within the component organizations. Without policies and procedures defining how the DBSMC and IRBs have visibility into and oversight of all business system investments, DOD risks components continuing to invest in systems that will fall short of expectations.

- The BCL does not provide for portfolio-based business system investment management. Without defining how projects are to be managed as part of portfolios of related investments, the department will not be able to take advantage of the synergistic benefits to be found among the entire collection of investments, rather than just from the sum of individual investments. Further, adequately documenting both the policies and procedures that provide predictable, repeatable, and reliable investment selection and control and govern how an organization reduces investment risk of failure and provides the basis for having rigor, discipline, and respectability in how investments are selected and controlled across the

---

[72]GAO-07-538.

[73]GAO-07-733.

entire organization. According to the department, as it implements both the CMO provisions of the National Defense Authorization Act for Fiscal Year 2008, and capability portfolio management, the IRB/DBSMC investment management approach is expected to become more portfolio oriented.

In finalizing the BCL, it will be important for DOD to address these gaps in its draft methodology. If it does not, the department will continue to risk selecting and controlling its business system investments in an inconsistent, incomplete, and ad hoc manner, which in turn will reduce the chances that these investments will optimally support mission needs in the most cost-effective manner.

## DOD Continues to Certify and Approve Business Systems Cited in the Act

The act specifies two basic requirements that took effect October 1, 2005, relative to DOD's use of funds for business system modernizations that involve more than $1 million in obligations in any given fiscal year. First, it requires that these modernizations be certified by a designated approval authority[74] as meeting specific criteria.[75] Second, it requires that the DBSMC approve each of these certifications. The act also states that failure to do so before the obligation of funds for any such modernization constitutes a violation of the Anti-deficiency Act.[76]

As we have previously reported,[77] the department has established an approach to meeting the act's requirements that reflects its philosophy of "tiered accountability." Under its approach, investment review begins within the military departments and defense agencies and advances through a hierarchy of review and decision-making authorities, depending

---

[74]The approval authorities, as discussed earlier in this report, are the heads of the IRBs. They are the USD(AT&L); the Under Secretary of Defense (Comptroller); the Under Secretary of Defense for Personnel and Readiness; and the ASD(NII)/CIO. They are responsible for the review, approval, and oversight of business systems and must establish investment review processes for systems under their cognizance.

[75]A 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.

[76]10 U.S.C.§2222(b); 31 U.S.C.§1341(a) (1) (A).

[77]GAO-07-733.

on the size, nature, and significance of the investment. For those investments that meet the act's dollar thresholds, this sequence of review and decision making includes component precertification, IRB certification, and DBMSC approval. For those investments that do not, investment decision-making authority remains with the component. This review and decision-making approach has two types of reviews for business systems: certification/approval reviews and annual reviews.

- **Certification/approval reviews.** Certification/approval reviews apply to new modernization projects with total costs over $1 million. These reviews focus on program alignment with the BEA and must be completed before components obligate funds for programs. Tiers 1, 2, and 3 investments in development and modernization are certified at three levels—components precertify, the IRBs certify, and the DBSMC approves. At the component level, program managers prepare, enter, maintain, and update information about their investments in their respective data repositories. Examples of information are regulatory compliance reporting, architectural profile, and requirements for investment certification and annual reviews. According to the process, the component precertification authority is to validate that the system information is complete and accessible on the repository, review system compliance with the BEA, and verify the economic viability analysis. This information is then transferred to DOD's IT Portfolio Repository.[78] The precertification authority asserts the status and validity of the investment information by submitting a component precertification letter to the appropriate IRB for its review.

  At the corporate level, the IRB reviews the pre-certification letter and related material, and if certification is decided, prepares a certification memorandum for the designated certification authority's signature that documents the IRB's decisions and any related conditions. The memorandum is forwarded to the DBSMC, which either approves or disapproves the IRB's decisions and issues a memorandum containing its decisions. If the DBSMC disapproves a system investment, it is up to the component precertification authority to decide whether to resubmit the investment after it has resolved the relevant issues.

- **Annual reviews.** The annual reviews apply to all business system investments and are intended to determine whether the investment is

---

[78]DOD's IT Portfolio Repository is the authoritative repository for certain information about DOD's business systems, such as system names and the responsible DOD components that are required for the certification, approval, and annual reviews of these business system investments.

meeting its milestones and addressing its IRB certification conditions. Tiers 1, 2, 3, and 4 business system investments are annually reviewed at two levels—the component and the IRBs. At the component level, program managers update information on all tiers of system investments that are identified in their component's data repository. For tiers 1 through 3 systems that are in development or being modernized, information is updated on cost, milestones, and risk variances and actions or issues related to certification conditions. The component precertification authority then verifies and submits the information for these business system investments for the IRB in an annual letter. The letter addresses system compliance with the BEA and ETP and includes investment cost, schedule, and performance information.[79]

IRBs annually review tiers 1, 2, and 3 business system development or modernization investments. These reviews focus on program compliance with the BEA, program cost and performance milestones, and progress in meeting certification conditions. IRBs can advise the DBSMC to revoke a certification when the investment has significantly failed to achieve performance commitments (i.e., capabilities and costs). When this occurs, the component must address the IRB's concerns and resubmit the investment for certification.

Since October 1, 2005 (the effective date of the relevant provision of the act), DOD has continued to certify and approve investments with annual obligations in excess of $1 million. For example, as of March 2007, DOD reported that the DBSMC had approved 285 system investments that had been previously certified by the IRBs. By September 30, 2007, DOD reported that the DBSMC had approved an additional 29 IRB-certified system investments, for a total of 314 approved systems. According to DOD:

- All 314 systems were certified and approved as meeting the first condition in the act—being in compliance with the BEA—and the 314 systems represent all of the modernization programs meeting the act's threshold through fiscal year 2007. Collectively, these 314 involved $7.9 billion in modernization funding.

[79]In addition, each component precertification authority submits a list of system names to the IRBs on a semiannual basis, to include Tier 4 systems and systems in operations and maintenance that have been reviewed at the component level.

- About 60 percent (187) of the 314 were reviewed and precertified within the military departments. More specifically, 69 were pre-certified within the Army, 58 within the Navy, and 60 within the Air Force. The remaining 127 were reviewed and precertified within 1 of 15 defense agencies, including 26 in the Military Health Service, 24 within the Defense Logistics Agency, and 20 in the BTA.

Since September 30, 2007, the IRBs have certified and the DBSMC has approved 39 additional system modernization investments. Moreover, available information from the military departments shows that 35 additional investments have been precertified. Specifically, the Air Force, Navy, and Army, report that 14, 19, and 2 investments, respectively, have been precertified. In addition, both the Air Force and Navy reported that they have reviewed and approved investments that are below the act's thresholds, and thus do not require IRB certification or DBSMC approval. Specifically, the Air Force reports 46 of these systems have been reviewed and approved, while the Navy reports 4 additional systems reviewed and approved. We have yet to receive comparable information from the Army.

The basis for DOD's continuing efforts to certify and approve business systems modernization investments as being compliant with the BEA are essentially each individual program's assertion of compliance. These assertions in turn are largely based on DOD BEA compliance assessment guidance. At the request of the Senate Armed Services Committee, we have ongoing reviews of several major business systems investments that include determining the extent to which these investments have demonstrated compliance with the BEA.

## Conclusions

Over the last year, DOD has continued to make important progress in defining and implementing key institutional modernization management controls, but much remains to be accomplished. In particular, the corporate BEA, while continuing to improve, is still missing important content, and it has yet to be federated through development of aligned subordinate architectures for each of the department's component organizations. Further, while the department has developed a strategy for federating the BEA in this manner, this strategy is still evolving and has yet to be implemented. Compounding this situation are recurring limitations in the ETP, as well as the immaturity of the military service architecture programs, to include their own transition plans. In addition, neither the corporate nor the military departments' approaches to business systems investment management have all the requisite structures and defined policies and procedures in place to be considered effective investment selection, control, and evaluation mechanisms. These architecture and

investment management limitations continue to put billions of dollars spent each year on thousands of business system investments at risk.

Development of a well-defined federated architecture and accompanying transition plans for the business mission area, along with institutionalization of effective business system investment management policies and procedures across all levels of the department, are critically important to addressing the business system modernization high-risk area. Equally, if not more important is for the department to actually implement the architecture and investment management controls on each and every business system investment. While not a guarantee, having an architecture-centric approach to investment management, combined with following the other key system acquisition disciplines that are reflected in our existing recommendations to the department, can be viewed as a recipe for the business systems modernization program's removal from our high-risk list.

Related to implementing our existing recommendations is the department's need to keep congressional defense committees fully informed about its progress in federating the DOD corporate BEA, to include the maturity of component organization architecture efforts and the related transition plan(s). In its most recent annual report to congressional defense committees pursuant to the National Defense Authorization Act for Fiscal Year 2005, the department missed an opportunity to do this by not including the results of its IV&V contractor's assessments of the completeness, consistency, understandability, and usability of the federated family of business mission area architectures, including associated transition plans, as we previously recommended.

## Recommendations for Executive Action

Because we have existing recommendations to the Secretary of Defense that address the issues raised in this report and that the department has yet to fully implement, we are not making additional recommendations at this time.

## Agency Comments

In comments on a draft of this report, signed by the Deputy Under Secretary of Defense (Business Transformation), the department stated that it appreciated our support in advancing its business transformation efforts. It also provided several technical comments that we have incorporated throughout the report, as appropriate.

We are sending copies of this report to interested congressional committees; the Director, Office of Management and Budget and the Secretary of Defense. Copies of this report will be made available to other interested parties upon request. This report will also be available at no charge on our Web site at http://www.gao.gov.

If you or your staffs have any questions on matters discussed in this report, please contact me at (202) 512-3439 or hiter@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 II.

Randolph C. Hite
Director
Information Technology Architecture and Systems Issues

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

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

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

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

# Appendix I: Objectives, Scope, and Methodology

As agreed with defense congressional committees, our objective was to assess the actions by the Department of Defense (DOD) to comply with the requirements of section 2222 of Title 10, U.S. Code.[1] To address this, we focused on five of the six requirements in section 2222, and related best practices contained in federal guidance, that we identified in our last annual report under the act as not being fully satisfied.[2] Generally, these five requirements are (1) development of a business enterprise architecture (BEA), (2) development of a transition plan for implementing the BEA, (3) inclusion of business systems information in DOD's budget submission, (4) establishment of business systems investment review processes and structures, and (5) approval of defense business systems investments with obligations in excess of $1 million. (See the background section of this report for additional information on the act's requirements.) We did not include the sixth requirement because our 2006 annual report under the act shows that it had been satisfied. Our methodology relative to each of the five requirements is as follows:

- To determine whether the BEA addressed the requirements specified in the act, and related guidance, we analyzed version 5.0 of the BEA, which was released on March 14, 2008, relative to the act's specific architectural requirements and related guidance that our last annual report under the act identified as not being met. We also reviewed version 5.0 to confirm whether statements made in DOD's March 15, 2008, annual report about the BEA's content were accurate. In addition, we reviewed DOD's Business Mission Area Federation Strategy and Road Map Version 2.0 released in January 2008, comparing the strategy and any associated implementation plans with prior findings and recommendations relative to the content of the strategy. Further, we reviewed the Business Transformation Agency's report of selected independent verification and validation (IV&V) contractor observations and recommendations relative to the Version 5.0's ability to provide a foundation for BEA federation, and compared this to our prior finding and recommendation relative to the content of an IV&V review of the BEA. Finally, we reviewed and leveraged the applicable results contained in our recent reports on the military departments' enterprise architecture programs, on the Air Force and

---

[1] Ronald 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).

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

Navy's investment management processes, and our recent testimony on
DOD's Business Transformation.[3]

- To determine whether the enterprise transition plan (ETP) addressed the
  requirements specified in the act, we reviewed the updated version of the
  ETP, which was released on March 15, 2008, relative to the act's specific
  transition plan requirements and related guidance that our last annual
  report under the act identified as not being met. We also reviewed the ETP
  to confirm that statements in DOD's March 15, 2008, annual report about
  the content of the ETP were accurate.

- To determine whether DOD's fiscal year 2009 information technology
  budget submission was prepared in accordance with the criteria set forth
  in the act, we reviewed and analyzed the department report entitled
  "Report on Defense Business System Modernization FY 2005 National
  Defense Authorization Act, Section 332," dated February 2008 and
  compared it to the specific requirements in the act.

- To determine whether DOD has established investment review structures
  and processes, we focused on the act's requirements that our last annual
  report under the act identified as not being met, obtaining documentation
  and interviewing cognizant DOD officials about efforts to establish the one
  IRB specified in the act that we previously reported had yet to be
  established. We also reviewed and leveraged our recent reports that
  assessed the department's,[4] Air Force's,[5] and Navy's[6] approaches to
  managing business system investments.

---

[3]GAO, *Business Systems Modernization: Air Force Needs to Fully Define Policies and
Procedures for Institutionally Managing Investments*, GAO-08-52 (Washington D.C.: Oct.
31, 2007); GAO, *Business Systems Modernization: Department of the Navy Needs to
Establish Management Structure and Fully Define Policies and Procedures for
Institutionally Managing Investments*, GAO-08-53 (Washington D.C.: Oct. 31, 2007); GAO,
*DOD Business Systems Modernization: Military Departments Need to Strengthen
Management of Enterprise Architectures*, GAO-08-519 (Washington D.C.: May 12, 2008);
and GAO, *Defense Business Transformation: Sustaining Progress Requires Continuity
of Leadership and an Integrated Approach*, GAO-08-462T (Washington D.C.: Feb. 7, 2008).

[4]GAO, *Business Systems Modernization: DOD Needs to Fully Define Policies and
Procedures for Institutionally Managing Investments*, GAO-07-538 (Washington, D.C.:
May 11, 2007).

[5]GAO-08-52.

[6]GAO-08-53.

- To determine whether the department was reviewing and approving
  business system investments exceeding $1 million, we reviewed DOD's list
  of business system investments certified by the Investment Review Boards
  (IRB) and approved by the Defense Business Systems Management
  Committee (DBSMC). We then compared the detailed information
  provided with the summary information contained in the department's
  March 15, 2008, report to the congressional defense committees to identify
  any anomalies. We also obtained documentation from the Air Force and
  the Navy to ascertain the specific actions that were taken (or planned to
  be taken) in order to perform the annual systems reviews as required
  pursuant to the act. We requested similar information from representatives
  of the Army, but did not receive it in time to include in this report.

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 this performance audit at DOD
headquarters in Arlington, Virginia, from March 2008 to May 2008, in
accordance with generally accepted government auditing standards. Those
standards require that we plan and perform the audit to obtain sufficient,
appropriate evidence to provide a reasonable basis for our findings and
conclusions based on our audit objectives.

# Appendix II: GAO Contact and Staff Acknowledgments

## GAO Contact

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

## Acknowledgments

In addition to the contact person named above, key contributors to this report were Elena Epps, Michael Holland, Tonia Johnson (Assistant Director), Neelaxi Lakhmani, Rebecca LaPaze, Anh Le, and Freda Paintsil.

| | |
|---|---|
| **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 "E-mail 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: <br><br> U.S. Government Accountability Office <br> 441 G Street NW, Room LM <br> Washington, DC 20548 <br><br> To order by Phone: Voice: (202) 512-6000 <br> TDD: (202) 512-2537 <br> Fax: (202) 512-6061 |
| **To Report Fraud, Waste, and Abuse in Federal Programs** | Contact: <br><br> Web site: www.gao.gov/fraudnet/fraudnet.htm <br> E-mail: fraudnet@gao.gov <br> Automated answering system: (800) 424-5454 or (202) 512-7470 |
| **Congressional Relations** | Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 <br> U.S. Government Accountability Office, 441 G Street NW, Room 7125 <br> Washington, DC 20548 |
| **Public Affairs** | Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 <br> U.S. Government Accountability Office, 441 G Street NW, Room 7149 <br> Washington, DC 20548 |