United States Government Accountability Office

GAO

Report to Congressional Committees

May 2009

DOD BUSINESS SYSTEMS MODERNIZATION

Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed

GAO-09-586

May 2009

DOD BUSINESS SYSTEMS MODERNIZATION

Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-586, a report to congressional committees

Why GAO Did This Study

Since 1995, GAO has designated the Department of Defense's (DOD) business systems modernization program as high risk, and it continues to do so today. To assist in addressing DOD's business system modernization challenges, the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (the Act) contains provisions that require the department to take certain actions and to annually report to its congressional committees on these actions. The Act also directs GAO to review each annual report. In response, GAO performed its fifth annual review of DOD's actions to comply with key aspects in the Act and related federal guidance. To do so, GAO reviewed, for example, the latest version of DOD's business enterprise architecture (BEA) and transition plan, investment management policies and procedures, and information in the department's business system data repositories.

What GAO Recommends

Because GAO has existing recommendations that address most of the weaknesses discussed in this report, it reiterates these recommendations and further recommends that DOD resolve the issues surrounding key modernization management positions and the quality of investment-related information. DOD partially agreed with GAO's recommendations and described either commitments or actions being planned or under way to partially address them.

View GAO-09-586 or key components.
For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

The pace of DOD's progress in defining and implementing key institutional modernization management controls has slowed compared with progress made in each of the last 4 years, leaving much still to be accomplished to fully implement the Act's requirements and related guidance. In particular,

- The corporate BEA continues to evolve and address previously identified missing elements, inconsistencies, and usability issues, but gaps still remain. For example, while the BEA now identifies information assurance laws, regulations, and policies, it still does not include business rules for all business processes. Further, little progress has been made in the last year in extending (i.e., federating) the BEA to the entire family of business mission area architectures, including using an independent verification and validation agent to assess the components' subsidiary architectures and federation efforts.
- The updated enterprise transition plan continues to identify systems and initiatives, but important elements are still missing, as are individual component plans. For example, while the plan provides a range of information, such as budgets and performance measures, for key enterprisewide and component-specific investments, it is missing information on identified investments.
- The fiscal year 2009 budget submission included some, but omitted other, key information about business system investments, in part because of the lack of a reliable comprehensive inventory of all defense business systems.
- Investment approval and accountability structures have been established for DOD and the Air Force, and related policies and procedures that are consistent with relevant guidance have been partially defined. However, these structures and processes are still lacking for the Navy.
- Business system investments costing over $1 million continue to be certified and approved, but these decisions are not always based on complete information. For example, key Navy investments have not fully demonstrated compliance with the department's BEA, and their economic justifications were not based on reliable estimates of cost and benefits. In addition, the information in DOD's authoritative repository of system investments that is used to make these decisions is not always accurate.

Department officials attributed this slowdown in large part to pending decisions surrounding the roles, responsibilities, authorities, and relationships among key senior leadership positions, such as DOD's Deputy Chief Management Officer and the military departments' Chief Management Officers. Until DOD fully implements these long-standing institutional modernization management controls provided for under the Act, addressed in GAO recommendations, and otherwise embodied in relevant guidance, its business systems modernization will likely remain a high-risk program. As a result, it is important that the department act quickly to resolve pending decisions about key positions.

Contents

Abbreviations

ASD(NII)/DOD CIO	Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer
BEA	business enterprise architecture
BTA	Business Transformation Agency
CIO	Chief Information Officer
CMO	Chief Management Officer
DBSMC	Defense Business Systems Management Committee
DITPR	Defense Information Technology Portfolio Repository
DOD	Department of Defense
ETP	enterprise transition plan
IRB	Investment Review Board
IT	information technology
IV&V	independent verification and validation
ITIM	Information Technology Investment Management
NDAA	National Defense Authorization Act
OMB	Office of Management and Budget
SNAP-IT	Select and Native Programming Data Input System–Information Technology

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 18, 2009

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 and an effective institutional approach to managing information technology (IT) investments.[3]

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-09-271 (Washington, D.C.: Jan. 22, 2009).

[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 or "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 (the Act) that were consistent with our recommendations.[6] More specifically, the Act requires 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 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

[5]See for example, 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); *DOD Business Systems Modernization: Billions Being Invested without Adequate Oversight*, GAO-05-381 (Washington, D.C.: Apr. 29, 2005); *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); *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, GAO-03-1018 (Washington, D.C.: Sept. 19, 2003); *Business Systems Modernization: Summary of GAO's Assessment of the Department of Defense's Initial Business Enterprise Architecture*, GAO-03-877R (Washington, D.C.: July 7, 2003); *Information Technology: Observations on Department of Defense's Draft Enterprise Architecture*, GAO-03-571R (Washington, D.C.: Mar. 28, 2003); *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 as a baseline, analyzing whether the department had taken actions to comply with those requirements, related guidance, and our prior recommendations that we previously identified as not yet addressed.[7] In doing this, we also relied on the results of relevant reports that we have issued since our prior annual report.[8] We also reviewed the department's report to Congress, which was submitted on March 18, 2009, and evaluated the information used to satisfy the budget submission and investment review, certification, and approval aspects of the Act.

We conducted this performance audit at DOD offices in Arlington, Virginia, from January to May 2009, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Details on our objective, scope, and methodology are contained in appendix I.

Background

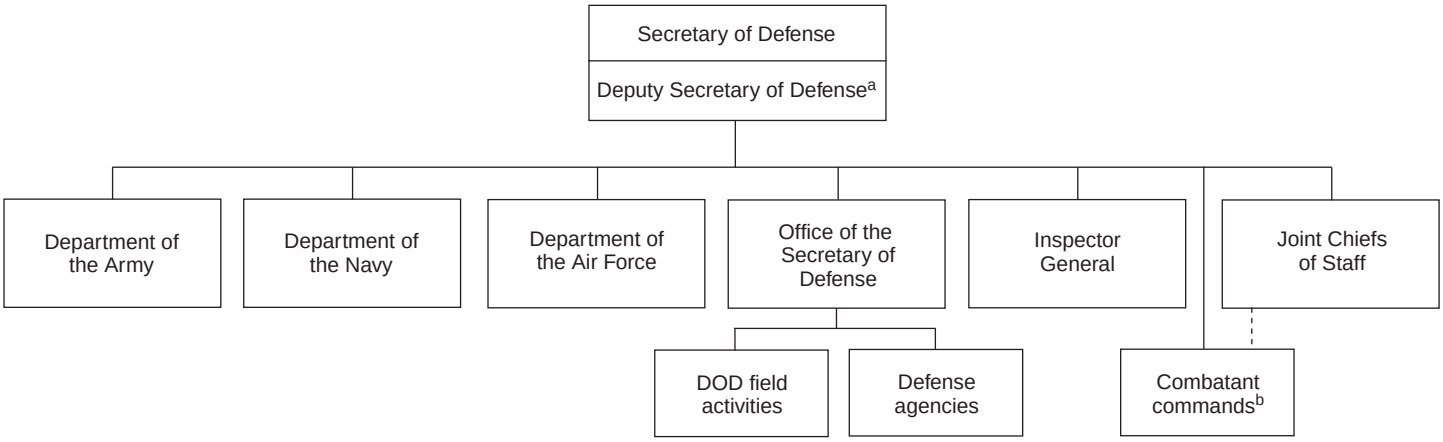
DOD is a massive and complex organization and is entrusted with more taxpayer dollars than any other federal department or agency. To illustrate, Congress provided DOD with about $512 billion in appropriations for fiscal year 2009. Additionally, Congress has provided about $808 billion in supplemental emergency funding for operations in support of the Global War on Terrorism since 2001. Moreover, the recent American Recovery and Reinvestment Act of 2009 contains nearly $12.6 billion in appropriations for DOD for military construction, environmental restoration, and other purposes. Organizationally, the department includes the Office of the Secretary of Defense, the Joint Chiefs of Staff, the military departments, numerous defense agencies and field activities, and

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

[8]See for example, GAO, *DOD Business Systems Modernization: Key Marine Corps System Acquisition Needs to Be Better Justified, Defined, and Managed*, GAO-08-822 (Washington, D.C.: July 28, 2008); *DOD Business Systems Modernization: Key Navy Programs' Compliance with DOD's Federated Business Enterprise Architecture Needs to Be Adequately Demonstrated*, GAO-08-972 (Washington, D.C.: Aug. 7, 2008); and *DOD Business Systems Modernization: Important Management Controls Being Implemented on Major Navy Program, but Improvements Needed in Key Areas*, GAO-08-896 (Washington, D.C.: Sept. 8, 2008).

various unified combatant commands that are responsible for either specific geographic regions or specific functions. (See fig. 1 for a simplified depiction of DOD's organizational structure.)

Figure 1: Simplified DOD Organization Structure



Source: GAO based on DOD documentation.

[a]The Deputy Secretary of Defense serves as the Chief Management Officer, who provides focused and sustained leadership over DOD's business transformation efforts.

[b]The 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, 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.[9] Moreover, the department recently reported that this systems environment is composed of approximately 2,480 separate business systems. For fiscal year 2009, DOD requested about $15.3 billion in funds to operate, maintain, and modernize these business systems and associated IT infrastructure.

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

As we have previously reported, the department's nonintegrated and duplicative systems impair its ability to combat fraud, waste, and abuse.[10] In fact, DOD currently bears responsibility, in whole or in part, for 15 of our 30 high-risk areas.[11] Eight of these areas are specific to the department,[12] while it shares responsibility for 7 other governmentwide high-risk areas.[13] Collectively, these high-risk areas relate to DOD's major business operations that are inextricably linked to the department's ability to perform its overall mission, directly affect the readiness and capabilities of U.S. military forces, and can affect the success of a mission. 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. Since the early 1990s, we have promoted the use of architectures to guide and constrain systems modernization, recognizing them as a crucial means to meeting this challenging goal: optimally defined operational and technological environments. Congress, the Office of Management and Budget (OMB), and the federal Chief Information Officers (CIO) Council have also recognized the importance of an architecture-centric approach to modernization. The Clinger-Cohen Act of 1996 mandates that an agency's CIO develop, maintain, and facilitate the implementation of an information

[10]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); *Military Pay: Army National Guard Personnel Mobilized to Active Duty Experienced Significant Pay Problems*, GAO-04-89 (Washington, D.C.: Nov. 13, 2003); and *Defense Inventory: Opportunities Exist to Improve Spare Parts Support Aboard Deployed Navy Ships*, GAO-03-887 (Washington, D.C.: Aug. 29, 2003).

[11]GAO-09-271.

[12]These 8 high-risk areas are 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.

[13]The 7 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.

technology architecture.[14] Further, the E-Government Act of 2002 requires OMB to oversee the development of enterprise architectures within and across agencies.[15] In addition, we, OMB, and the CIO Council have issued guidance that emphasizes the need for system investments to be consistent with these architectures.[16] For example, in April 2003, we issued a framework that emphasizes the importance of having an enterprise architecture as a critical frame of reference for organizations when they are making IT investment decisions.[17] Also, in December 2008, OMB issued guidance that addresses system investment compliance with agency architectures.[18]

A corporate approach to IT investment management is another important characteristic of successful public and private organizations. Recognizing this, Congress enacted the Clinger-Cohen Act of 1996,[19] 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.[20] 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.[21] We have also issued guidance in this area that defines institutional structures (such as

[14]40 U.S.C. § 11315(b)(2).

[15]44 U.S.C. § 3602(f)(14).

[16]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004); *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management*, *Version 1.1*, GAO-03-584G (Washington, D.C.: April 2003); *OMB Capital Programming Guide*, *Version 1.0* (July 1997); and CIO Council, *A Practical Guide to Federal Enterprise Architecture*, *Version 1.0* (February 2001).

[17]GAO-03-584G.

[18]OMB, *Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework v3.0)* (December 2008).

[19]40 U.S.C. § 11302(c)(1). The Clinger-Cohen Act of 1996 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).

[20]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).

[21]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.

investment boards), processes for developing information on investments (such as cost/benefit), and practices to inform management decisions (such as whether a given investment is aligned with an enterprise architecture).[22]

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). An architecture describes the enterprise in logical terms (such as interrelated business processes and business rules, information needs and flows, and work locations and users) as well as in technical terms (such as hardware, software, data, communications, security attributes, and performance standards). It provides these perspectives both for the enterprise's current, or "as is," environment, and for its target, or "to be," environment, and it provides a transition plan for moving from the "as is" to the "to be" environment. This transition 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"[23] and the DOD Architecture Framework.[24]

[22]See for example, GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009); GAO-04-394G; GAO-03-584G; and *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*, GAO/AIMD-10.1.13 (Washington, D.C.: February 1997).

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

[24]DOD, *Department of Defense Architecture Framework*, Version 1.5, Volumes I-III (April 2007).

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. The alternative, as our work has shown, is the perpetuation of the kinds of operational environments that burden many agencies today, where a lack of integration among business operations and the IT resources supporting them leads to systems that are duplicative, poorly integrated, and unnecessarily costly to maintain and interface.[25] Our framework provides federal agencies with a common benchmarking tool for planning and measuring their efforts to improve enterprise architecture management.[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 gives autonomy to an organization's components while ensuring enterprisewide linkages and alignment where appropriate. Where

[25]See, for example, GAO, *Federal Aviation Administration: Stronger Architecture Program Needed to Guide Systems Modernization Efforts*, GAO-05-266 (Washington, D.C.: Apr. 29, 2005); *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; *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; *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

[26]GAO-03-584G.

commonality among components exists, there are also opportunities for identifying and leveraging shared services.

A service-oriented architecture 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, 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.[27] A service-oriented architecture approach is thus intended not only 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.

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.

[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).

[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).

- 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 (ITIM) framework consists of five progressive stages of maturity for any given agency relative to selecting, controlling, and evaluating its investment management capabilities.[29] (See fig. 2 for the five ITIM stages of maturity.) The overriding purpose of the framework is to encourage investment selection and control and to 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, and a number of agencies have adopted it.[30]

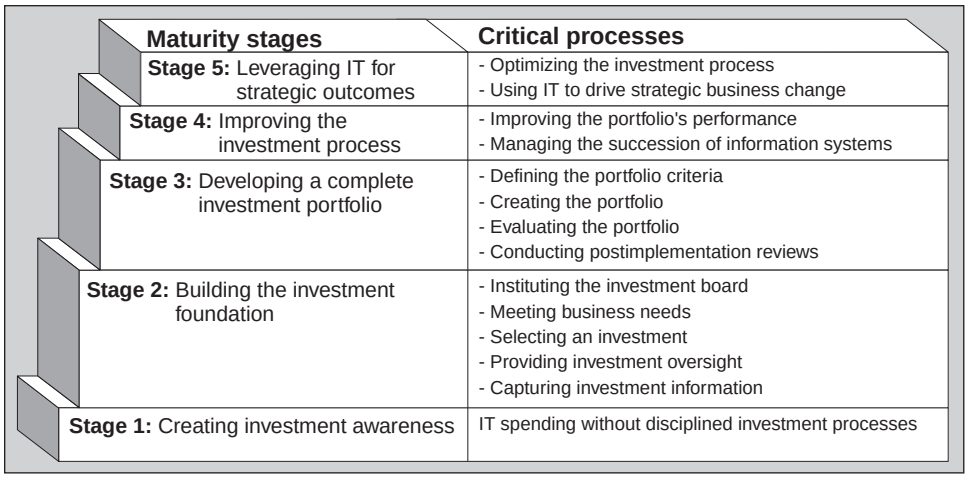
In our ITIM framework, with the exception of the first stage, each maturity stage is composed of "critical processes" that must be implemented and institutionalized in order for the organization to achieve that stage. Each ITIM critical process consists of "key practices"—to include organizational structures, policies, and procedures—that must be executed to implement the critical process. Our research shows that agency efforts to improve

[29]GAO-04-394G.

[30]GAO, *Information Technology: SSA Has Taken Key Steps for Managing Its Investments, but Needs to Strengthen Oversight and Fully Define Policies and Procedures*, GAO-08-1020 (Washington, D.C.: Sept. 12, 2008); *Information Technology: Treasury Needs to Strengthen Its Investment Board Operations and Oversight*, GAO-07-865 (Washington, D.C.: July 23, 2007); *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments*, GAO-07-424 (Washington, D.C.: Apr. 27, 2007); *Information Technology: Centers for Medicare & Medicaid Services Needs to Establish Critical Investment Management Capabilities*, GAO-06-12 (Washington, D.C.: Oct. 28, 2005); *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); *Information Technology Management: Census Bureau Has Implemented Many Key Practices, but Additional Actions Are Needed*, GAO-05-661 (Washington, D.C.: June 16, 2005); *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); *Information Technology: Departmental Leadership Crucial to Success of Investment Reforms at Interior*, GAO-03-1028 (Washington, D.C.: Sept. 12, 2003); *Bureau of Land Management: Plan Needed to Sustain Progress in Establishing IT Investment Management Capabilities*, GAO-03-1025 (Washington, D.C.: Sept. 12, 2003); *United States Postal Service: Opportunities to Strengthen IT Investment Management Capabilities*, GAO-03-3 (Washington, D.C.: Oct. 15, 2002); and *Information Technology: DLA Needs to Strengthen Its Investment Management Capability*, GAO-02-314 (Washington, D.C.: Mar. 15, 2002).

investment management capabilities should focus on implementing all lower-stage practices before addressing higher-stage practices.

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



Source: GAO.

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 Stage 2 and 3 practices have in place selection, control, and evaluation processes that are consistent with the Clinger-Cohen Act.[31] Stages 4 and 5 require the use of evaluation techniques to continuously improve both investment processes and portfolios in order to better achieve strategic outcomes.

DOD's Institutional Approach to Business Systems Modernization

The National Defense Authorization Act (NDAA) for Fiscal Year 2008 designated the Deputy Secretary of Defense as the Chief Management Officer (CMO) for DOD and created a Deputy CMO position.[32] The CMO's responsibilities include developing and maintaining a departmentwide strategic plan for business reform and establishing performance goals and

[31]40 U.S.C. §§ 11311-11313.

[32]Pub. L. No. 110-181 § 904 (2008).

measures for improving and evaluating overall economy, efficiency, and effectiveness and monitoring and measuring the progress of the department. The Deputy CMO's responsibilities include recommending to the CMO methodologies and measurement criteria to better synchronize, integrate, and coordinate the business operations to ensure alignment in support of the warfighting mission. The Business Transformation Agency (BTA) supports the Deputy CMO in leading and coordinating business transformation efforts across the department.

The CMO and Deputy CMO are to interact with several entities to provide executive leadership for the direction, oversight, and execution of DOD's business transformation efforts, which include business systems modernization. These entities 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 and is chaired by the Deputy Secretary of Defense; 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 BTA, which is responsible for supporting the IRBs, and for leading and coordinating business transformation efforts across the department. 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 in coordination with the warfighting and enterprise information environment mission areas[a] Recommends policies and procedures required to integrate DOD business transformation and attain cross-department, end-to-end interoperability of business systems and processes Serves as approving authority for business system modernization Establishes policies and approves the business mission area strategic plan, the enterprise transition plan for implementation of business systems modernization, the transformation program baseline, and the BEA	Chaired by the Deputy Secretary of Defense/CMO; the Vice Chair is the Under Secretary of Defense for Acquisition, Technology, and Logistics. Includes senior leadership in the Office of the Secretary of Defense such as the Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer (ASD(NII)/DOD CIO), the military departments' Secretaries and defense agencies' heads, 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 Serve as the certification authorities accountable for the obligation of funds for respective business system modernizations within designated core business missions[b] Provide the DBSMC with recommendations for system investment approval	Under Secretaries of Defense for Acquisition, Technology, and Logistics; Comptroller; and Personnel and Readiness; ASD(NII)/DOD CIO; and the Deputy Secretary of Defense.
IRBs	Serve as the oversight and investment decision-making bodies for those business capabilities that support activities under their designated areas of responsibility 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)/DOD CIO, core business mission area representatives, military departments, defense agencies, and combatant commands.
Component Precertification Authority	Ensures component-level investment review processes integrate with the investment management system Identifies those component systems that require IRB certification and prepare, review, approve, validate, and transfer investment documentation as required Assesses and precertifies architecture compliance of component systems submitted for certification and annual review Acts as the component's principal point of contact for communication with the IRBs	Includes the CIO from the Air Force; the Principal Director of Governance, Acquisition, and Chief Knowledge Office from the Army; the CIO from the Navy; and comparable representatives from other defense agencies.

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

Source: GAO based on DOD documentation.

[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 systems modernization. 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 DOD-wide policies, capabilities, standards, and 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 tiers 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 corporate 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	Major Automated Information System[a] or Major Defense Acquisition Program[b]	IRB and DBSMC
Tier 2	Exceeding $10 million in total development/modernization costs, but not designated as a Major Automated Information System or Major Defense Acquisition Program	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 an interest program by the IRB chair).

Source: GAO based on DOD documentation.

[a]A Major Automated Information System is a program or initiative that is so designated by the ASD(NII)/DOD CIO or that is estimated to require program costs in any single year in excess of $32 million, total program costs in excess of $126 million, or total life cycle costs in excess of $378 million in fiscal year 2000 constant dollars.

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

Consistent with the tiered accountability approach, the NDAA for Fiscal Year 2008 required the Secretaries of the military departments to designate the department Under Secretaries as CMOs with primary responsibility for business operations.[33] Moreover, the Duncan Hunter NDAA for Fiscal Year 2009 requires the military departments to establish business transformation offices to assist their CMOs.[34]

Summary of Fiscal Year 2005 NDAA Requirements

Congress included six provisions in the fiscal year 2005 NDAA that are aimed at ensuring DOD's development of a well-defined BEA and associated ETP, as well as the establishment and implementation of

[33]Pub. L. No. 110-181 § 904 (2008).

[34]Pub. L. No. 110-417 § 908 (2008).

effective investment management structures and processes.[35] The requirements are as follows:

1. Develop a BEA that includes an information infrastructure that, at a minimum, would enable DOD to

- comply with all federal accounting, financial management, and reporting requirements;
- routinely produce timely, accurate, and reliable financial information for management purposes;
- integrate budget, accounting, and program information and systems; and
- provide for the systematic measurement of performance, including the ability to produce timely, relevant, and reliable cost information.

In addition, the BEA must

- 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 nonfinancial resource needs.

[35]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).

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

- a 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 include

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

The fiscal year 2005 NDAA also requires that the Secretary of Defense submit to the congressional defense committees a report on the department's compliance with the above provisions.

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

Since 2005, we have reported that DOD has each year taken increasing steps to comply with the requirements of the fiscal year 2005 NDAA and to satisfy relevant systems modernization management guidance.[36] Moreover, we concluded that DOD had made important progress each year relative to architecture development, transition plan development, budgetary disclosure, and investment review; however, aspects of these requirements and relevant guidance had yet to be fully satisfied. We also reported that DOD had fully satisfied the requirement concerning designated approval authorities and continued to certify and approve modernizations costing more than $1 million. However, each report also concluded that much remained to be accomplished relative to the Act's requirements and relevant guidance, as these examples illustrate:

- The BEA lacked important content, such as business rules for, and information flows among, certain business activities, and it had yet to be extended (i.e., federated) throughout the DOD component organizations.
- The ETP did not include investments for all components and did not reflect key factors associated with properly sequencing planned investments, such as dependencies among investments and the capability to execute the plan.
- DOD and the military departments had yet to fully establish key investment review structures and define related policies and procedures for effectively performing both project-level and portfolio-based investment management.

Accordingly, we either provided new or reiterated existing recommendations to address each of these areas. DOD largely agreed with our recommendations. In August 2008, we also reported on issues with the

[36] GAO-06-219, GAO-06-658, GAO-07-733, and GAO-08-705.

process used to certify investments as compliant with DOD's BEA.[37] Specifically, we reported that key DOD business systems modernization programs did not adequately demonstrate compliance with the department's federated BEA, even though each program had largely followed DOD's existing compliance guidance, used its compliance assessment tool, and was certified and approved as being compliant by department investment oversight and decision-making entities. In addition, we reported that even though the department's investment oversight and decision-making authorities had certified and approved these business system programs as compliant with the BEA, these certification and approval entities did not validate each program's compliance assessment and assertions. Accordingly, we made recommendations to address each of those shortcomings, which DOD agreed with.

With respect to departmentwide business transformation, we recently reported that implementation of DOD's overall management framework for business transformation is not yet complete because key aspects had not been defined.[38] For example, we reported that the authority, roles, and relationships for some positions and entities had not been clearly defined, including a clearly defined decision-making authority for the Deputy CMO, a clearly defined relationship between DOD's Deputy CMO and the CMOs of the military departments, and clearly defined unique and shared responsibilities of various governance entities, such as the Deputy's Advisory Working Group and the DBSMC. We concluded that the current administration needed to move quickly to nominate and fill key leadership positions, including the Deputy Secretary of Defense (now statutorily designated as the CMO), the Deputy CMO, the Under Secretaries of Defense, and the military department CMOs. We also concluded that, in light of the transition, it will be important for senior leaders in the current administration to further define and clarify the roles, responsibilities, and relationships among the various positions and governance entities within DOD's management framework for business transformation in order to sustain and further DOD's progress.

In addition, we reported that DOD's first strategic management plan, issued in 2008, lacked key information and elements necessary for assisting in successfully achieving business management transformation.[39]

[37]GAO-08-972.

[38]GAO-09-272R.

[39]GAO-09-272R.

For example, it did not identify any strategic goals, objectives, and performance measures, and while it stated a purpose, the plan did not provide detailed information about business operations. Without strategic goals and objectives, we concluded that the strategic management plan could not be linked to other existing plans and tools for individual business areas, such as the ETP.

DOD Continues to Take Steps to Strengthen Management of Its Business Systems Modernization, but Long-standing Challenges Remain

DOD continues to take steps to comply with the requirements of the Act and to satisfy relevant systems modernization management guidance. In particular, DOD released an update to its corporate BEA (version 6.0) 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 statutory provisions and best practices concerning the BEA, transition plan, budgetary disclosure, and investment review of systems costing in excess of $1 million. However, the pace of DOD's progress in defining and implementing these key modernization management controls has slowed compared with the progress the department had made, and we have reported, each of the last 4 years. As a result, challenges that we identified last year largely remain to be addressed to fully implement the Act and relevant guidance. Most notably, the department has yet to extend and evolve its BEA and to provide the total federated family of DOD parent and subsidiary architectures for the business mission area, which are needed to comply with the Act. It also has yet to fully define IT investment management policies and procedures at the corporate and component levels, and the business system information used to support the development of the transition plan and DOD's budget requests, as well as certification and annual reviews, is of questionable reliability. DOD officials agree that additional steps are needed to fully implement the Act's requirements and related system modernization management best practices. Further, they stated that progress over the last year has been slowed by yet-to-be-resolved issues surrounding the Deputy CMO and military department CMO positions.

DOD Continues to Evolve Its Corporate BEA, but a Well-Defined Plan for Federating It Has Yet to Be Developed and Progress on Component Architectures Has Been Slow

Among other things, the fiscal year 2005 NDAA requires DOD to develop a BEA that would cover all defense business systems and their related functions and activities and that would enable the entire department to (1) comply with all federal accounting, financial management, and reporting requirements and (2) routinely produce timely, accurate, and reliable financial information for management purposes. The BEA should also include policies, procedures, data standards, and system interface requirements that are to be applied throughout the department. As such, the Act requires 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 releases new architecture versions every year that include a corporate BEA that is to be augmented by a coherent family of component architectures. As we have previously reported, such an approach is consistent with best practices and appropriate given DOD's scope and size.

In 2008, we reported that the then-current version of the BEA (version 5.0) addressed, to varying degrees, missing elements, inconsistencies, and usability issues that we previously identified, but that gaps still remained.[40] On March 13, 2009, DOD released BEA 6.0, which addresses some of these gaps. For example, it begins to address information assurance by identifying related laws, regulations, and policies.[41] This is important because the nature and substance of institutionalized security requirements, controls, and standards should be captured in the architecture products, since information assurance permeates every aspect of an organization's operations. In addition, the latest version of the BEA begins to address the technical standards (e.g., W3C XML-Encryption[42]) needed to allow business systems to work in an

[40]GAO-08-705.

[41]Information assurance refers to measures that defend and protect information and information systems by ensuring their confidentiality, integrity, authenticity, availability, and utility.

[42]The W3C XML-Encryption Syntax and Processing standard provides end-to-end security for applications that require secure exchange of XML data. Agile Web services applications in need of secure and reliable data can use this standard to prevent interception, alteration, and unauthorized decryption of information.

expeditionary environment, which would, among other things, allow warfighters operating in these environments to access business systems.[43]

Version 6.0 of the BEA also addresses, to varying degrees, missing elements, inconsistencies, and usability issues that we previously identified, but continues to be missing important content. Examples of these improvements and remaining issues are summarized below.

- The latest version includes 35 new business rules. As we previously reported, business rules are important because they translate business policies and procedures into specific, unambiguous rules that govern what can and cannot be done. As such, they facilitate consistent implementation of laws, policies, and procedures. Examples of new business rules in the Common Supplier Engagement business priority area[44] are (1) an accepting or inspecting organization must be provided on all contracts for goods or services and (2) both a minimum and a maximum ordering limit must be provided when the contract is an indefinite delivery/indefinite quantity contract.[45] In addition to adding business rules, Version 6.0 reflects the deletion of 22 business rules that, according to DOD, were no longer applicable and were thus obsolete. Notwithstanding these additions and deletions, BEA 6.0 still does not provide business rules for all business processes. For example, there are no business rules for the File Discrepancy Report for Other Goods and Services business process in the Common Supplier Engagement and Materiel Visibility business priority areas.[46] Such limitations in DOD's business rules limit the department's

[43]An expeditionary environment is one in which warfighters are deployed away from their home base and where network access, bandwidth, and reliable infrastructure are constrained in comparison with the normal DOD business environment in the continental United States.

[44]The BEA is organized around six business enterprise priority areas. The Common Supplier Engagement priority area seeks to standardize the methods that DOD uses to interact with commercial and government suppliers in the acquisition of catalog, stock, as well as made-to-order and engineer-to-order goods and services. It also provides the associated visibility of supplier-related information to the warfighting and business mission areas. The other business enterprise priority areas are Personnel Visibility, Acquisition Visibility, Materiel Visibility, Real Property Accountability, and Financial Visibility.

[45]An indefinite delivery/indefinite quantity contract is a type of contract that provides, within stated limits, for an indefinite quantity of supplies or services during a fixed period of time.

[46]The File Discrepancy Report for Other Goods and Services business process includes listing goods or services that were not accepted, the reasons for rejection, and processing discrepancy dispute updates.

ability to ensure that business operations and supporting systems are properly implemented.

- The latest version includes additional information on important security architecture content. For example, it now identifies information assurance laws, regulations, and policies and describes information assurance characteristics of key information exchanges (e.g., Awarded Contract is designated as a sensitive information exchange[47]). However, not all financial information exchanges (e.g., Receipt Account Trial Balance and Ledgers[48]) include such key information assurance characteristics as confidentiality, integrity, and nonrepudiation. Without specifying such information assurance characteristics for all relevant exchanges, DOD will be limited in its ability to implement adequate security controls into the systems that support these exchanges.

- The latest version continues to add new operational activities, which describe actions performed in conducting DOD business operations (e.g., Deliver Property and Forces[49]). These operational activities are important because they are DOD's primary basis for determining if a system is being defined in a way that is compliant with the BEA. However, key operational activities are not yet included in the BEA. For example, Version 6.0 still does not include the Foreign Military Sales operational activity, which affects multiple DOD business missions and organizations. Without including such important operational activities, programs do not have all the information necessary for determining if they are compliant with applicable constraints (e.g., data definitions and business rules).

- 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. While Version 6.0 adds approximately 50 new information exchanges (e.g., Approved Payment Request[50]) among

[47]The Awarded Contract information exchange represents a contract that has been awarded to an external supplier.

[48]The Receipt Account Trial Balance and Ledgers information exchange contains detailed receipt transactions and balances reported by DOD during the month.

[49]Deliver Property and Forces describes activities for issuing, transporting, and delivering property, materiel, and forces.

[50]The Approved Payment Request information exchange is a request for payment from a vendor or other party owed by the government that has been approved and confirmed to comply with the terms and conditions of the contract.

business functions and approximately 15 data exchanges (e.g., Payment Request for Goods[51]) among system functions, it still contains information exchanges (e.g., Accounts Payable Account[52]) that are not attached or linked to any operational nodes (or organizations). Further, this version's information-related architecture products contain inconsistencies. For example, information exchanges such as Final Contract or Order Costs and Estimate at Completion[53] are listed in the information exchange integrated dictionary, but are not listed in the operational information exchange product.[54] As a result, DOD's ability to understand how information is shared among operational entities, and subsequently develop or modernize systems that can effectively share such information, will be constrained.

- The latest version also depicts end-to-end business flows (e.g., Budget to Report[55]) with linkages to BEA business processes (e.g., Execute Apportionment and Allocate Funds[56]). However, BEA 6.0 does not include, for each end-to-end business flow, a create, read, update, and delete matrix[57] that shows how the business processes and their associated applications manage specific data objects (e.g., Approved

[51]The Payment Request for Goods data exchange is a request for payment for goods from a vendor or other party owed by the government.

[52]The Accounts Payable Account information exchange is a summary of general ledger accounts used for financial reporting.

[53]The Final Contract or Order Costs information exchange is a determination of the final cost of a contract or intragovernmental order that is not firm-fixed price and must be reconciled prior to contract or order closeout; the Estimate at Completion information exchange is the estimated total cost for all authorized work.

[54]The operational information exchange product describes the information exchanges associated with operational activities.

[55]Budget to Report encompasses all business functions necessary to plan, formulate, create, execute against, and report on the budget and business activities of the entity, including updates to the general ledger.

[56]The Execute Apportionment and Allocate Funds business process involves recording an agency's budgetary resources and supporting the establishment of legal budgetary limitations within the agency. It also involves supporting the establishment of funding to agencies that are not subject to apportionment.

[57]A create, read, update, and delete matrix shows the specific business functions and applications that create, read, update, and/or delete specific data elements, which enables the organization to develop applications.

Apportionment[58]). These matrices are important because they reveal natural groupings of business activities and data objects, and thus are used to identify business activities to be automated. Without this information, DOD will be limited in its ability to develop a target architecture that effectively integrates information and systems that support its business activities.

BTA officials recognize many of these issues and state that they will be addressed as the BEA continues to evolve. In this regard, the Chief Architect stated that the process for evolving the BEA is described in the architecture's Concept of Operations. Specifically, it describes a process that calls for business cases to justify proposed improvements that are then prioritized and used to create a BEA plan for DBSMC approval. However, the Concept of Operations has yet to be approved, and available documentation does not demonstrate that this process is being followed. Further, we have yet to receive an architecture plan or evidence of DBSMC approval of such a plan. As we have previously reported and recommended, BTA needs an enterprise architecture program management plan that defines what the department's incremental improvements to the architecture (and transition plan) will be, and how and when they will be accomplished, including what (and when) architecture and transition plan scope and content and architecture compliance criteria will be added into which versions.[59] BTA has not yet developed such a plan. According to BTA officials, the department's next steps are contingent upon ongoing discussions about how architecture planning will be affected by the Deputy CMO's efforts to align the department's various planning activities in its strategic management plan, which is to be issued no later than July 1, 2009. These discussions will be further complicated by the lack of clarity surrounding the Deputy CMO's roles, responsibilities, and authorities and how the deputy will work with other senior leaders across the department who have responsibility for business operations.

Beyond the above-discussed limitations, Version 6.0 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 6.0 appropriately focuses

[58]Approved Apportionment is the notification from OMB that DOD's apportionment request has been approved and is available for distribution to the components and/or services.

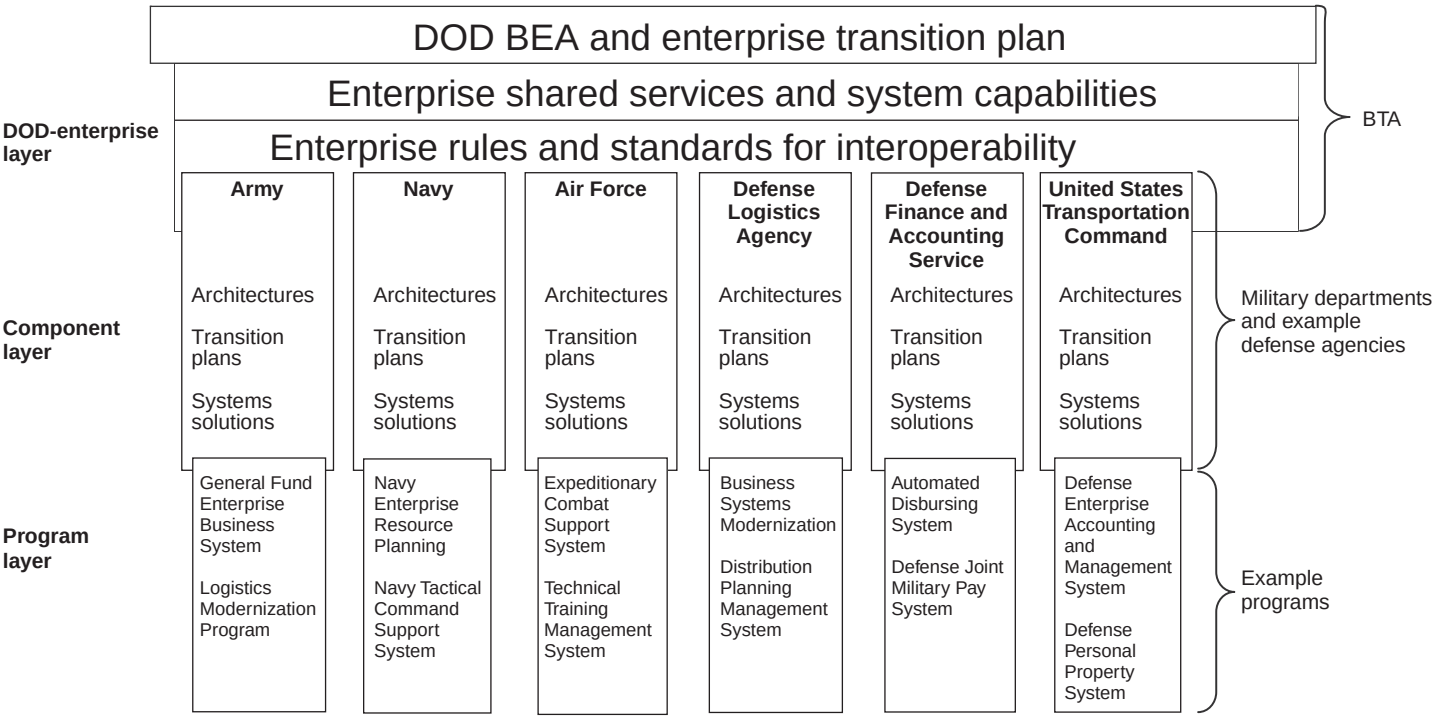
[59]GAO-08-705, GAO-07-733, and GAO-06-658.

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 6.0 does not provide the total federated family of DOD parent and subsidiary architectures for the business mission area.

DOD's Progress in Federating Its BEA Has Been Slow

Recognizing the need to address its component architecture challenges, BTA released an update to its initial business mission area federation strategy and road map in January 2008. Among other things, this strategy was to address how the corporate BEA would be extended to the military departments and defense agencies and how business services will be identified and delivered across the business mission area. (See fig. 3 for a conceptual representation of DOD's federated BEA.)

Figure 3: Conceptual Representation of DOD's Business Mission Area Federated Architecture



Source: GAO analysis of DOD data.

In September 2006, DOD issued its initial business mission area federated strategy and road map, which we reported lacked adequately defined tasks needed to achieve the strategy's goals, such as addressing how strategy

execution will be governed, component architectures will be aligned with the latest version of the BEA, and common applications and systems across the department will be identified and reused. Accordingly, we reiterated our prior recommendation for a BEA management plan, and recommended that DOD ensure that this plan describes, at a minimum, how the business mission area architecture federation would be governed; how the business mission area federation strategy alignment with the DOD architecture federation strategy would be achieved; how component business architectures' alignment with incremental versions of the BEA would be achieved; how shared services would be identified, exposed, and subscribed to; and what milestones would be used to measure progress and results.[60]

In January 2008, DOD issued an updated strategy, and in May 2008, we reported that the update, along with the associated global information grid strategy,[61] partially addressed our recommendations.[62] Specifically, we reported that the strategies provided high-level roles and responsibilities for federating the architecture and additional definition around the tasks needed to achieve alignment among DOD and component architectures. We also noted that the strategy for the business mission area provided for conducting pilot programs across the components to demonstrate the technical feasibility of architecture federation, and for using the lessons learned from the pilots to improve and update the strategies.

To their credit, BTA and other DOD entities, such as ASD(NII)/DOD CIO and the Department of the Army, are collaboratively taking steps to establish the foundation for implementing the strategy. For example, they have

[60]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).

[61]According to DOD, the global information grid 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. The global information grid 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 ASD(NII)/DOD CIO.

[62]GAO-08-705.

- selected the Department of the Army's Defense Knowledge Online to be BTA's federated enterprise portal, which is to be the point of access to information about all DOD and component architectures, and is to allow users to search and navigate through this information;

- established and are using the DOD Architecture Registry System, which is maintained by ASD(NII)/DOD CIO, as the repository to contain architecture content;

- conducted five pilots at three military departments and two defense agencies to evaluate various aspects of architecture federation and develop lessons learned about, for example, approaches for capturing and managing architecture metadata[63] (Air Force pilot), and enterprise search and discovery methods[64] (Navy pilot); and

- developed guidance on identifying and registering business services and, as of November 2008, identified and registered 25 business services, such as a service that provides detailed information on each aircraft at the base (e.g., an aircraft's mission capability and maintenance status), and a service that allows aircraft maintenance data to be retrieved, created, updated, and removed.

According to officials from ASD(NII)/DOD CIO, which is responsible for overall DOD architecture federation, the results of the pilots are being used to determine future federation steps for all DOD mission areas. In addition, BTA officials said that both BTA and ASD(NII)/DOD CIO are defining a basic set of standard architecture models,[65] including a common vocabulary for using architecture information across DOD, to allow for uniform representation of architecture content. Establishing such a common framework is important because DOD's current lack of uniform representation for enterprise architecture content, according to BTA and ASD(NII)/DOD CIO officials, will limit the understanding and utility of the federated architecture.

[63]Metadata is information (attributes) about artifacts (e.g., a description of the artifact or author of the artifact).

[64]Search and discovery capabilities are intended to enable discovery of architecture metadata and services stored in repositories.

[65]An architecture model is a template for creating an architecture view. It is intended to allow understandability by users and interoperability between architectures.

Notwithstanding the above steps, BTA's strategy for federating the BEA still does not contain sufficient detail to permit effective and efficient execution and adequately address our recommendations. For example, the business mission area's federation implementation road map only outlines high-level, near-term milestones, such as milestones for developing a governance charter for the DOD CIO Enterprise Guidance Board, which is DOD's senior forum for guiding the development and approval of enterprise-level guidance (including IT policy, architecture, and standards) on enterprise architecture, and conducting a pilot with Defense Knowledge Online to test an access control mechanism.[66] It does not, for example, specify tasks to be performed to achieve those milestones, identify milestones or tasks beyond fiscal year 2010, or identify resources needed to perform tasks (e.g., funding, staffing, tools, and training). Further, the strategy does not describe how the various architecture federation activities taking place across DOD come together over time to achieve a federated BEA, including measurement of progress, results, and the component architectures' alignment with the latest version of the BEA. BTA and ASD(NII)/DOD CIO officials stated that these details have yet to be described because of unresolved issues surrounding the Deputy CMO and military department CMO positions.

Moreover, DOD's federation efforts have yet to benefit from any independent verification and validation (IV&V) assessments.[67] As we previously reported, such assessments are important to ensure the completeness, consistency, understandability, and usability of the federated family of architectures.[68] Accordingly, we recommended that DOD have its BEA IV&V contractor perform such assessments and disclose the results in its annual report to Congress. However, DOD's March 2009 annual report does not include this information. According to BTA officials, from October 2007 through March 2009, BTA expended approximately $3 million on BEA-related IV&V activities. However, these activities have focused on the corporate BEA and not the entire federated

[66]An access control mechanism is a means for determining the permissible activities of users and authorizing or prohibiting activities by each user.

[67]Use of an independent verification and validation agent is an architecture management best practice for identifying architecture strengths and weaknesses and disclosing to department and congressional oversight bodies the information they need to better ensure that DOD's family of architectures and associated transition plans satisfy key quality parameters.

[68]GAO-07-733.

family of architectures. BTA officials also stated that future IV&V activities are not currently focused on the federated family of architectures. They added that they are engaged in discussions with ASD(NII)/DOD CIO on how and who to best perform such assessments, given that the federated BEA is a part of DOD's overall federated enterprise architecture, which is led by ASD(NII)/DOD CIO.

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 the current state of the military departments' enterprise architecture programs. Specifically, we recently reported 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,[69] which are outlined in our Enterprise Architecture Management Maturity Framework.[70] While the Air Force's architecture efforts are well ahead of those of the Navy and Army, all three had yet to fully satisfy important aspects of our framework. 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 their 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

[69]GAO-08-519.

[70]GAO-03-584G.

obtaining unbiased insight into such essential architecture qualities as completeness, understandability, usability, and consistency.

- None of the military departments could demonstrate that its IT investments were actually in compliance with its architecture. 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 made recommendations aimed at improving the management and content of these architectures. DOD agreed with our recommendations. However, our recommendations have yet to be fully implemented. Specifically, none of the military departments provided documentation demonstrating that the above-cited limitations have been addressed. Until DOD has a well-defined family of architectures for its business mission area, it will not fully implement the requirements of the Act and will remain challenged in its ability to effectively manage its business system modernization efforts.

DOD Continues to Update Its ETP, but Important Elements Are Still Missing, as Are Individual Component Plans

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.

On September 30, 2008, DOD released the latest version of its ETP,[71] which in general provides information on about 645 business systems, including, to varying degrees, the required information on 54 systems that are linked to key transformational objectives and priorities.[72] For example, it includes specific time-phased milestones with status indicators (e.g., met, on track, or deleted) for about 47 out of the 54 systems, and it includes performance metrics (e.g., voucher payment time and integration test

[71]From 2006 to 2008, DOD's March Congressional Report also represented an update of its ETP. However, this year's March Congressional Report does not include an ETP update. As a result, the most recent version of the ETP was released in September 2008. According to BTA, the department is revisiting its approach to releasing the ETP.

[72]Key transformational objectives include the business enterprise priorities: Personnel Visibility, Acquisition Visibility, Materiel Visibility, Common Supplier Engagement, Real Property Accountability, and Financial Visibility.

progress) for about 26 of these.[73] Further, the latest version of the ETP discusses progress made since March 2008 on business system investments, as well as descriptions of planned near-term activities (e.g., next 12 months). However, previously identified limitations in the scope and completeness of the latest version of the ETP remain. Examples of improvements and remaining issues are summarized below.

- The ETP provides a range of information for some, but not all, business system investments, such as 3 years of budget information for about 342 out of 645 systems (about 50 percent), 46 of which are linked to key transformation objectives and priorities. However, the ETP does not yet include system and budget information for all the business systems identified in the department's IT systems repository. According to the ETP, it does not include budget information for about half of the business systems identified because the budget data for some of these systems were not included in the fiscal year 2009 budget submission. Further, according to BTA officials, the ETP continues to focus on tier 1 and 2 business systems. However, not all DOD components have developed subordinate transition plans that would address all the business system investments. For example, as we reported last year, the Navy and Army have not yet developed subordinate transition plans.[74] More specifically, Navy officials stated that they are revising their enterprise architecture development and governance approach and, according to draft Navy enterprise architecture documentation associated with this approach, an enterprise architecture transition plan will be developed. Further, as we reported, the Air Force's transition plan is limited. For example, it is not based on an analysis of the gap in capabilities between the department's "as is" and "to be" environments. Collectively, this means that a complete family of DOD and component transition plans does not exist. According to the BTA official responsible for the ETP, BTA and the military departments are currently discussing whether component-level plans should be published separately from or incorporated into the corporate ETP. This is further complicated by the uncertainty surrounding how the Deputy CMO will work with other senior leaders who have responsibility for business operations, including the military department CMOs.

[73]Time-phased milestones refer to milestones, such as milestone A (which occurs at the end of the Material Solution Analysis phase), milestone B (which occurs at the completion of the Technology Development phase), milestone C (which occurs at the end of the Engineering and Manufacturing Development phase), initial operating capability, and full operating capability.

[74]GAO-08-705.

- The ETP continues to provide performance measures for some, but not all, enterprise and component investments (i.e., programs), including key milestones (e.g., initial operating capability) and status indicators. However, the plan has yet to include other important information needed to understand the sequencing of new systems becoming operational and legacy systems being phased out. In particular, the planned investments have not been 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 of competing investments.[75] Rather, the ETP continues to be largely based on a bottom-up process in which ongoing programs have been compiled and categorized in the plan around business enterprise priorities. For example, many of these investments are dependent on Net-Centric Enterprise Services, and as such the plans and milestones for each should reflect the incremental capability deployment of these enterprise services.[76]

- The ETP and the business mission area federation strategy describe the department's approach to enterprise application integration, including plans for using specific services and standards for integrating financial application systems.[77] Including such information in the ETP and associated documentation will help to clarify relationships and dependencies among legacy applications and systems and new or modernized applications and systems. However, all systems needed to achieve integration are not specified. For example, the ETP does not identify all of the systems that must be integrated for each end-to-end business flow (e.g., budget-to-report) to support activities that are cross-functional and cross-cutting across organizational boundaries.

- The ETP does not include all legacy systems that will not be part of the target BEA and does not provide the schedule for terminating these legacy

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

[76]Net-Centric Enterprise Services is intended to provide capabilities that are key to enabling ubiquitous access to reliable decision-quality information. Its capabilities include a 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).

[77]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.

systems, as required by the Act. For example, while the Navy Enterprise Resource Planning program's August 2008 investment review board documentation identifies 41 legacy systems, the ETP identifies only 25 of these systems.[78] In addition, the plan is missing information about some legacy systems and modernization programs. Specifically, the plan does not include termination dates for 40 out of 514 legacy systems. Including a comprehensive and reliable list of legacy systems is important for the department to have a meaningful and reliable basis for managing the disposition of legacy systems and for sequencing the introduction of modernized business operations and supporting systems.

BTA officials said that a number of actions are envisioned to address the above-cited areas and further improve the ETP, such as working with the military departments and defense agencies to determine which systems should be included in the corporate-level ETP and ensuring that the next version of the ETP includes more information about dependencies among systems. 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 and the department's capability to manage them), it will not provide a sufficient basis for sequencing the introduction of modernized systems. To help DOD improve its ETP, we have previously made recommendations that the department is in the process of addressing aimed at formalizing its plans for incrementally improving its transition plan.

Fiscal Year 2009 Budget Submission Did Not Include Key Information on All Business Systems

Another requirement of the Act is that DOD's annual IT budget submission must 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).

As we reported last year, the department's fiscal year 2009 budget submission included a range of information required by the Act on business system investments.[79] Specifically, for 273 investments that

[78]The Navy Enterprise Resource Planning program is to standardize the Navy's business processes, such as acquisition and financial management.

[79]GAO-08-705.

involve development/modernization activities, the submission included such information as the system's (1) name, (2) approval authority, and (3) appropriation type. The submission also identified the amount of the fiscal year 2009 request that was for development/modernization versus operations/maintenance. Further, for those system investments in excess of $1 million in modernization funding, the submission cited the certification status (e.g., approved, approved with conditions, not applicable, and withdrawing) and the DBSMC approval date, where applicable.

However, the fiscal year 2009 budget submission does not reflect all business system investments. To prepare the submission, DOD relied on business system investment information (e.g., funds requested, mission area, and system description) that is entered by the components into DOD's Select and Native Programming Data Input System–Information Technology (SNAP-IT). In accordance with DOD guidance and according to ASD(NII)/DOD CIO officials, the business systems listed in SNAP-IT should match the systems listed in the Defense Information Technology Portfolio Repository (DITPR)—the department's authoritative business systems inventory. However, the number of business systems in DITPR is unclear. Specifically, in March 2009, DITPR data provided by DOD included about 6,800 systems, and in April 2009, BTA officials stated that the number of operational business systems in the repository was 2,480, adding that the 6,800 number included systems that were not business systems and systems that may no longer be operational. However, they have yet to provide support for this revised number of business systems.

Regardless, SNAP-IT is potentially missing thousands of business systems that are identified in DITPR. Specifically, SNAP-IT contains about 2,100 systems, of which only about 1,500 are categorized as business systems.[80] Restated, the fiscal year 2009 budget submission is missing somewhere between 980 and 5,300 business systems. For example, the Department of the Navy's Personnel Information System for Training, Operations, and Logistics and the Air Force's Contractor Responsibility Information System are listed in DITPR but not listed in SNAP-IT. Moreover, as stated

[80]Of the 2,100 systems, 600 are categorized as either national security systems (i.e., intelligence systems, cryptologic activities related to national security, military command and control systems, and equipment that is an integral part of a weapon or weapons system or is critical to the direct fulfillment of military or intelligence missions or systems that store, process, or communicate classified information) or are not within the business mission area (e.g., warfighting mission area).

earlier in the report, DOD has also recognized limitations in its budget submission in its ETP. The ASD(NII)/DOD CIO official responsible for administering the SNAP-IT data said that while the components are responsible for ensuring that information about their respective systems is accurate and complete, the department recognizes the need to reconcile the information between SNAP-IT and DITPR to improve the systems' comprehensiveness and accuracy. However, the department has yet to develop a plan or time frame for doing so. Without a reliable comprehensive inventory of all defense business systems, DOD will not be able to ensure the completeness and reliability of its IT budget submissions.

DOD Has Made Progress in Establishing Corporate and Component Investment Management Structures, but Associated Policies and Procedures Are Not Yet Fully Defined and Implemented

The Act also requires DOD to establish business system investment review structures, such as the previously discussed DBSMC and five IRBs, as well as processes that are consistent with the investment management provisions of the Clinger-Cohen Act.[81] As we have previously reported, organizations that satisfy Stages 2 and 3 of our ITIM framework have 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.

DOD and the Air Force have largely established the kind of investment management structures provided for in the Act and our ITIM framework.[82] However, the Navy has not. Moreover, neither DOD nor these components 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 programs (Stage 2) and as portfolios of programs (Stage 3). Until all of DOD has put these requisite investment management structures and supporting policies and procedures into place, the billions of dollars that the department and its components invest annually in business systems will remain at risk.

[81] 40 U.S.C. § 11312.

[82] GAO-04-394G.

Corporate and Air Force Investment Management Structures Are Largely Established, but Navy Structures Remain a Work in Progress

DOD has largely established corporate-level organizational structures that are associated with Stages 2 and 3 of our framework. As we reported in May 2008, the department has an enterprisewide investment board and four subordinate boards, and has assigned them responsibility for business systems investment governance, including conducting investment certification and approval reviews and annual reviews as provided for in the Act.[83] The enterprisewide board—the DBSMC—is composed of the department's top executives, such as the Deputy Secretary of Defense and the ASD(NII)/DOD 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 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.[84] 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 Under Secretary of Defense for Acquisition, Technology, and Logistics for managing business system portfolio selection criteria.

Since 2008, the department has taken additional steps to establish a fifth IRB, the DOD Chief Information Officer's review board, which is to oversee investments in business systems whose primary purpose is to support infrastructure and information assurance activities. According to DOD officials, this board is to replace the Enterprise Information Environment Mission Area review board, which was the fifth board required by the Act, and its charter has been drafted, but not approved.[85]

With respect to the military departments' investment management structures, we reported in May 2008 that the Air Force had established the

[83]GAO-08-705.

[84]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.

[85]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.

organizational structures associated with Stages 2 and 3 of our framework, such as a business systems IRB consisting of senior executives from the functional business units, including the Office of the Air Force CIO.[86] Among other things, this board is responsible for business system investment governance, including conducting investment precertification, approval, and annual reviews, as required by the Act.

We recently reported that, in contrast to the Air Force, the Navy had not yet established an enterprisewide IRB composed of senior executives from its IT and business units, to define and implement a Navy-wide business system governance process.[87] We concluded that without such structures, the Navy's ability to ensure that business system investment decisions are made consistently and reflect the needs of the organization was limited. Accordingly, we recommended that the Navy establish these management structures. Navy officials told us that a Secretary of the Navy Instruction that is intended to address these limitations has been drafted but not yet approved.[88]

Corporate and Air Force Investment Management Policies and Procedures Are Being Established, but Navy's Remain Largely Undefined

DOD has partially defined the full range of corporate and component-level policies and procedures that we previously recommended it establish to effectively support project-level (Stage 2) and portfolio-based (Stage 3) investment management practices.[89] Specifically, DOD recently issued new corporate-level policies and procedures that further address key practices in our ITIM framework associated with project-level investment management (Stage 2), such as instituting the investment board and providing investment oversight. In particular, DOD's revised 2008 acquisition policy[90] and draft business capability life cycle acquisition policy and guidance outline aspects of how the business investment review processes are to be coordinated with other decision-support processes used at DOD, such as the Joint Capabilities Integration and

[86]GAO-08-705.

[87]GAO-08-705.

[88]Secretary of Navy Instruction 5230.14.

[89]GAO-07-538.

[90]DOD Instruction 5000.02, Dec. 2, 2008.

Development System and the Defense Acquisition System.[91] For example, the revised policies and guidance now require a team to assess the risks associated with each Major Automated Information System and to share the results with the program manager and component functional sponsor,[92] who in turn are to collaboratively report the risks to both the IRB and the program's milestone decision authority prior to each milestone decision.[93] They further require the DBSMC to approve the obligation of funds prior to the first milestone review of each major business system. In addition, DOD also recently revised its policy for overseeing the acquisition of systems that provide joint capabilities, to require all business system investments to comply with the business system investment review process and the business capability life cycle process.[94]

The department has also recently established guidance associated with portfolio-level investment management (Stage 3) practices. However, DOD's updated corporate-level policies and procedures are still missing critical project- and portfolio-based investment management practices that we previously recommended, as discussed below.[95]

- Policies and procedures for instituting the investment board do not address how all investments that are past the development/modernization stage (i.e., in operations and maintenance) are to be governed. Given that DOD invests billions of dollars annually in operating and maintaining business systems, this is significant. For example, while the 2009 update to

[91]The Joint Capabilities Integration and Development System is a need-driven management system used to identify future capabilities for DOD, and the Defense Acquisition System is an event-driven system for managing product development and procurement and guides the acquisition process for DOD.

[92]According to DOD, the component functional sponsor is the component executive responsible for defining and managing capabilities, verifying that capability requirements are met, representing the user community's interests, and ensuring funding for defense business system investments.

[93]According to DOD, the milestone decision authority is the designated individual who has overall responsibility for an investment. This person has the authority to approve an investment's progression in the acquisition process and is responsible for reporting cost, schedule, and performance results. For example, the milestone decision authority for a Major Automated Information System is the ASD(NII)/DOD CIO or a designee.

[94]DOD, *Chairman of the Joint Chiefs of Staff Instruction: Joint Capabilities Integration and Development System*, 3170.01G, March 1, 2009.

[95]GAO-07-538.

the IRB guidance now requires an annual review of all investments previously certified by IRBs, including those in operations and maintenance, this review is not required for systems in operations and maintenance that were not previously certified by the IRBs. Our ITIM framework emphasizes that the corporate investment boards should review important information about an investment, such as cost and performance baselines, throughout the investment's life cycle. In addition, while the department's investment process addresses how investment-related processes are to be coordinated with the Joint Capabilities Integration and Development System and the Defense Acquisition System, these processes do not apply to all business systems. For example, DOD's updated acquisition policy states that IRB involvement in acquisition decisions is required only for Major Automated Information Systems. Moreover, the 2008 acquisition policy and draft business capability life cycle acquisition policy and guidance do not address how these processes are to be coordinated with the Planning, Programming, Budgeting, and Execution process.[96] Furthermore, the business capability life cycle acquisition policy and guidance has yet to be approved. Without approved policies and procedures that provide clear visibility into all investments, including linkages to related management systems, inconsistent investment decisions may result.

- Procedures for selecting an investment do not specify how the IRBs use the full range of cost, schedule, and benefit data in making selection (i.e., certification) decisions. Specifically, while the revised 2009 IRB guidance states that the IRBs will consider cost, schedule, and benefit data in making certification decisions, the guidance does not define how the boards are to consider these factors. According to our ITIM guidance, a structured selection method should provide investment boards, business units, and IT developers with a common understanding of the selection process to be followed, including how cost, schedule, and benefit data are to be used to compare and select projects. Furthermore, while DOD issued an IRB roles and responsibilities policy in January 2009 that states that the certification authorities will define the selection criteria for determining

[96]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.

whether an investment is to be an enterprisewide system or remain component specific,[97] those certification authorities have yet to do so.[98] Without documenting how the IRBs employ such factors when making selection decisions, the department cannot ensure that the boards consistently and objectively select proposals that best meet the department's needs and priorities.

- Policies and procedures for overseeing an investment do not provide for sufficient 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. Such visibility is important because DOD reports that only 346 system modernization efforts have been IRB certified and DBSMC approved. This means that the vast majority of business systems are reviewed and approved only within the component organizations. While the January 2009 IRB roles and responsibilities policy requires that each component submit an end-of-the-fiscal-year report listing those systems that have been reviewed by the cognizant IRB, this report lacks important project information. For example, it does not address components' adherence to cost, schedule, and risk investment selection and control criteria. According to our ITIM framework, an investment board should have visibility into each project's performance and progress toward predefined cost, schedule, and benefit expectations as well as each project's exposure to risk. Without such visibility, DOD components risk making investment decisions that are inconsistent and not fully grounded in objective data.

- Policies and procedures have not been fully established for defining the portfolio selection criteria or for creating and evaluating the portfolio of business systems. Specifically, the department has assigned responsibility to its certification authorities for defining the criteria to be used for making portfolio selection decisions, creating portfolios, and evaluating the performance of portfolio investments. However, these authorities have yet to fulfill these responsibilities.

[97]Directive-Type Memorandum 08-020 "Investment Review Board Roles and Responsibilities," signed by the Deputy Secretary of Defense (Jan. 26, 2009).

[98]The certification authorities are the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); Under Secretary of Defense for Personnel and Readiness; ASD(NII)/DOD CIO; and the Deputy Secretary of Defense.

According to our ITIM framework, the development and use of portfolio selection criteria focuses on the synergistic benefits to be found among an agency's entire collection of investments, rather than just from the sum of the individual investments.

- Policies and procedures for conducting postimplementation reviews do not address all business systems. Specifically, in its January 2009 update to its IRB guidance, the department added a new type of review, called a closeout annual review, to be performed when a business system modernization has been completed. According to the guidance, this review is to function as a postimplementation review for IRB-certified systems and is to provide the IRBs with lessons learned and metrics about completed investment efforts. However, the guidance does not address how expected benefits were achieved. According to our ITIM framework, examining the differences between estimated and actual investment costs and benefits is a key aspect of conducting postimplementation reviews.

  According to BTA officials, these limitations are due to the newness of its investment review policies and procedures, which they said will be revised over time to address the limitations. Adequately documenting both the policies and the associated procedures that provide predictable, repeatable, and reliable investment selection and that control and govern how an organization manages its IT investment portfolios reduces investment risk of failure and provides the basis for rigor, discipline, and repeatability in how investments are selected and controlled across the entire organization.

  With respect to the military departments' investment management policies and procedures, we recently reported that the Air Force and the Navy did not have fully documented policies and procedures for overseeing the management of business system investments and for developing and managing complete business systems investment portfolios.[99] To address these areas, we made recommendations aimed at implementing our framework's Stage 2 and 3 practices, and DOD partially agreed with these recommendations. Under DOD's tiered accountability approach to reviewing and approving business systems investments, in which investment review begins at the component level and proceeds through a hierarchy of review and approval authorities, depending on the size and significance of the investment, it is vital that DOD components implement these practices. BTA officials told us that the success of the department's

[99] GAO-08-52 and GAO-08-53.

overall process for managing business system investments depends on each component performing a thorough analysis and making informed decisions relative to each business system before it is submitted for higher-level review and approval.

To the Air Force's credit, it has recently updated its policies and procedures to address our project-level investment management recommendations (Stage 2 of our framework).[100] For example, the Air Force's recently developed IT investment review guidance provides for the review of all business systems, to include those in operations and maintenance, and it defines the process by which its IRB will review these systems. Further, the guidance specifies how business investments, including those in operations and maintenance, are to be prioritized using factors such as mission and strategic value and risk. The Air Force has also addressed key practices associated with portfolio-level investment management (Stage 3), such as creating and modifying IT portfolio selection criteria and assigning responsibility for the development and modification of IT portfolio selection criteria. Specifically, the guidance describes the criteria to be used to make portfolio selection, assigns responsibility for developing the criteria to an integrated working team, and assigns responsibility for approval of the criteria to a senior working group.

However, the Air Force's recent investment review guidance is still missing critical elements needed to effectively carry out essential investment management activities. For example, the guidance does not yet specify how the business investment management activities are coordinated with other DOD management systems, such as the Joint Capabilities Integration and Development System, the Defense Acquisition System, and the Planning, Programming, Budgeting, and Execution process. Further, the guidance does not provide for sufficient oversight and visibility into investment management activities. Specifically, while the Air Force has predefined criteria for adherence to cost, schedule, and performance milestones, and requires the development of corrective actions when a system deviates from milestones, it does not have policies and procedures that guide the implementation of these corrective actions when program expectations are not met. Moreover, the Air Force has yet

[100]U.S. Air Force, *Air Force Instruction 33-141: Air Force Information Technology Portfolio Management and IT Investment Review*, Dec. 23, 2008, and *Air Force Information Technology Investment Review Guide, Version 2.2*, Nov. 24, 2008.

to develop policies and procedures for maintaining investment portfolios. According to the Air Force, such key practices will be addressed in future revisions to its guidance.

In contrast, the Navy has not made as much progress as the Air Force in addressing either our project-level or portfolio-level recommendations. For example, the Navy has yet to fully document policies and procedures for overseeing the management of business system investments and for developing and managing complete business systems investment portfolios. Among other things, it does 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. According to the Navy, a policy for addressing our recommendations has been drafted, but has yet to be approved.

As discussed in our ITIM framework, adequately documenting both the policies and associated procedures that govern how an organization manages its IT projects and investment portfolios is important because doing so provides the basis for rigor, discipline, and repeatability in how investments are selected and controlled across the entire organization. Until these missing policies and procedures are fully defined at both the corporate and the component levels, it is unlikely that the thousands of DOD business system investments will be managed in a consistent, repeatable, and effective manner.

DOD Continues to Certify and Approve Business Systems, but Decisions Are Sometimes Based on Limited Information

The Act specifies two basic requirements that took effect October 1, 2005, relative to DOD's use of funds for business system modernization investments that involve more than $1 million in obligations. First, it requires that these investments be certified by a designated approval authority[101] as meeting specific criteria, such as

[101]The approval authorities, as discussed earlier in this report, are the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); the Under Secretary of Defense for Personnel and Readiness; the ASD(NII)/DOD CIO; and the Deputy Secretary of Defense. They are responsible for the review, approval, and oversight of business systems and must establish investment review processes for systems under their cognizance.

demonstrating compliance with the BEA.[102] Second, it requires that the DBSMC approve each of these certifications, adding that failure to do so before the obligation of funds for any such investment constitutes a violation of the Anti-deficiency Act.[103] In addition, DOD's business system approval and certification guidance directs programs to submit additional information, such as a program's economic analysis, to designated approval authorities.

As it has since 2005, DOD continues to certify and approve business system modernization investments in excess of $1 million. However, since 2006, we have identified limitations in the information used to certify and to approve several major programs.[104] Moreover, although IRB certification and annual review guidance calls for DOD's authoritative business systems repository (i.e., DITPR) to be used to inform business system investment certification and annual review decisions, information in this repository is not always current and accurate. As a result, DOD risks making certification and approval decisions that are not prudent and justified.

DOD Has Continued to Certify and Approve Business Modernizations in Excess of $1 Million

The department has established an approach to meeting the Act's requirements that reflects its philosophy of tiered accountability. Under this approach, investment review begins within the military departments and defense agencies and advances through a hierarchy of review and decision-making authorities, depending 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.

[102]The Act requires 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.

[103]10 U.S.C.§2222(b); 31 U.S.C.§1341(a) (1) (A).

[104]GAO-06-171, GAO-06-215, GAO-08-972, GAO-08-822, and GAO-08-896.

Certification/approval reviews. Certification/approval reviews apply to new modernization investments with planned obligations in excess of $1 million. These reviews focus on program alignment with the BEA and must be completed before components obligate modernization funds. Tier 1, 2, and 3 investments that involve development and modernization funds are certified and approved at three levels—component precertification, IRB certification, and DBSMC approval.

At the component level, program managers are responsible for the information about their respective programs that is in DITPR. Examples of information contained in DITPR are regulatory compliance reports, architectural profiles, financial benefit information (i.e., benefit-to-cost ratio), and system life cycle costs. According to the process, the component precertification authority is responsible for precertifying BEA compliance and reviewing system modernization funding requests, in addition to ensuring that IRBs receive complete, current, and accurate information within the prescribed deadlines. The precertification authority asserts the status and validity of the investment information by submitting a component precertification letter to the appropriate IRB.

At the corporate level, the IRB reviews the precertification letter and related material, and if it decides to certify the investment, 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's certification, 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 continuing to comply with the BEA, meeting its milestones, and addressing its IRB certification conditions. Tier 1, 2, and 3 business system investments are annually reviewed by the relevant component and IRB.

At the component level, program managers update information on all tiers of system investments that are identified in their component's data repository. For Tier 1, 2, or 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 investments to the appropriate IRB in an annual memo.

At the IRB level, Tier 1, 2, and 3 business system development or modernization investment 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, schedule, 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 obligations in excess of $1 million. Since fiscal year 2005, DOD has reported that the DBSMC had approved system modernization efforts for a total of 346 systems. According to DOD:

- All but one of the 346 system modernization efforts were certified and approved as meeting the first condition in the Act—being in compliance with the BEA.[105] These systems involved about $8.5 billion in development/modernization funding.
- About 60 percent of the 346 system modernization efforts (208) are owned by the military departments and were accordingly precertified within the military departments. More specifically, 63 were precertified within the Air Force, 79 within the Army, and 66 within the Navy.

DOD Certification and Approval Decisions Have Been Based on Limited Information

Although DOD has been meeting the Act's requirement to certify and approve business system modernization programs, it has at times relied on limited information in doing so. For example, we recently reported that two large Navy business system programs did not adequately demonstrate compliance with the department's federated BEA, even though each program largely followed DOD's existing compliance guidance, used its compliance assessment tool, and was certified and approved as being compliant by department investment oversight and decision-making

[105]The one system that was not certified and approved as compliant was certified and approved as meeting the Act's other condition—being necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security.

entities.[106] In particular, these programs' BEA compliance assessments did not (1) include all relevant architecture products, such as products that specify the technical standards needed to promote interoperability among related systems; (2) examine overlaps with other business systems, even though a stated goal of the BEA is to identify duplication and thereby promote the use of shared services; and (3) address compliance with the Department of the Navy's enterprise architecture, which is a major BEA federation member. We attributed these limitations to various reasons, including the fact that the department's guidance did not provide for performing these steps.

In addition, we reported that although the department's investment oversight and decision-making authorities certified and approved these business system programs as compliant with the BEA, they did not validate each program's compliance assessment and assertions. According to DOD officials, this was because responsibility for doing so is assigned to DOD's component organizations, such as the Department of the Navy, under the department's tiered accountability approach. However, the Department of the Navy oversight and decision-making authorities also did not validate the programs' assessments and assertions. We concluded that such architecture compliance limitations increase the risk of DOD programs being defined and implemented in a way that does not sufficiently ensure interoperability and avoid duplication and overlap. Accordingly, we made a number of recommendations to address these limitations, which the department agreed to implement.

Another example of limited information used to certify and approve business system investments is the unreliable economic justifications for the programs. According to relevant DOD guidance, the economic viability of system investments is to be analyzed on the basis of reliable estimates of costs and benefits. However, we have continued to report on limitations in the cost/benefit analyses used to economically justify major DOD business system investments.[107] More recently, we reported that the Global Combat Support System–Marine Corps cost estimate was not reliable, as it was not based on historical data from similar programs and it did not account for schedule risks, both of which are needed for the estimate to be considered accurate and credible.[108] In addition, we reported that the

[106]GAO-08-972.

[107]See, for example, GAO-06-215, GAO-06-171, GAO-08-822, GAO-08-896, and GAO-08-922.

[108]GAO-08-822.

Navy Enterprise Resource Planning program did not employ similar cost-estimating practices.[109] As a result, we concluded that neither program had a sufficient basis for deciding if it was the most cost-effective solution for meeting mission needs, and we made recommendations to address these weaknesses. DOD agreed with our recommendations.

Accurate Information about Modernization Investments Is Not Maintained in DOD's IT System Repository

Since 2005, DITPR has been designated as the authoritative repository of information about all DOD business systems. According to DOD's business system certification and annual review guidance, information in DITPR is to be updated by component staff, validated by program managers, and reviewed by component precertification authorities to ensure its accuracy, and it is to be used by the IRBs and the DBSMC in making certification and approval decisions, respectively.

The information in DITPR is not always accurate, and thus does not always provide an adequate basis for informed decision making. According to ASD(NII)/DOD CIO officials, information entered in DITPR at the component level is not always reliable and validated. Our analysis of selected business system information contained in DITPR confirmed such inaccuracies:

- At least 900 systems, such as the Contractor Performance Assessment Reporting System[110] and the Air Force's Virtual Personnel Service Center,[111] showed life cycle phase start dates as the year 1900 or 1901.
- At least 960 systems, such as the Armed Forces Health Longitudinal Technology Application[112] and BTA's Wide Area Workflow System,[113] show a life cycle phase end date of 2099 or later.

[109]GAO-08-896.

[110]The Contractor Performance Assessment Reporting System is a Web-enabled application that collects and manages a library of automated contractor performance reports.

[111]The Air Force's Virtual Personnel Service Center is to provide the Air Force unique human resources services not provided by the Defense Integrated Military Human Resources System.

[112]The Armed Forces Health Longitudinal Technology Application is the military's electronic health record system.

[113]The Wide Area Workflow System is an enterprise solution for electronic submission, acceptance and processing of invoices and receiving reports, and matching them with contracts to authorize payment.

Moreover, as stated earlier in this report, DOD provided inconsistent information about the number of business systems contained in DITPR. Specifically, in March 2009, DITPR data provided by DOD included about 6,800 systems, and in April 2009 BTA officials stated that the number of operational business systems in the repository was 2,480.[114] Thus, the number of business systems in DITPR is also unclear.

According to ASD(NII)/DOD CIO officials, a policy is being developed to have the DOD Inspector General periodically validate the accuracy of the information in DITPR. Given that the information from DITPR is used to make certification and approval decisions, serious limitations in the accuracy of information could affect the quality of the decisions.

Conclusions

The pace of DOD's progress in defining and implementing key institutional modernization management controls has slowed relative to each of the prior 4 years, leaving much to be accomplished. Specifically, the corporate BEA continues to be 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 updated its strategy for federating the BEA, this strategy is still missing important content and it has yet to be implemented. Compounding this situation are recurring limitations in the scope and completeness of the department's enterprise transition plan, as well as the immaturity of the military department architecture programs, including the completeness of their own transition plans. In addition, the corporate and the military departments' approaches to business systems investment management continue to lack the requisite structures and defined policies and procedures to be considered effective investment selection, control, and evaluation mechanisms. Finally, information used to support the development of the transition plan and DOD's budget requests, as well as to inform certification and annual reviews, is of questionable reliability. Collectively, these long-standing limitations in the department's

[114]The preceding information about business system life cycle start and end dates was obtained from DOD's March 2009 DITPR data. Nevertheless, the specific examples cited in this report (e.g., BTA's Wide Area Workflow System) are defined as business systems in DOD's SNAP-IT system and were reported as business systems in DOD's fiscal year 2009 budget request.

institutional modernization management controls continue to put billions of dollars spent each year on thousands of business system investments at risk.

A well-defined federated architecture and accompanying transition plans for the business mission area, along with well-defined investment management policies and procedures across all levels of the department, are critical to effectively addressing DOD's business systems modernization high-risk area. Relatedly, it is important for the department to obtain independent assessments of the completeness, consistency, understandability, and usability of the federated family of business mission area architectures, including associated transition plans, and to share the results of these assessments with its authorizing and appropriations committees. Equally important is for the department to actually implement its architecture and investment management controls in the years ahead on each and every business system investment, and in doing so to ensure that it has reliable information on each investment upon which to base executive decision making.

Our previous recommendations to the department have been aimed at accomplishing these and other important activities related to its business systems modernization. While not a guarantee, having an architecture-centric investment management approach, combined with the actual implementation of other key system acquisition disciplines that are reflected in our existing recommendations, can provide a recipe for the business systems modernization program's removal from our high-risk list. To the department's credit, it has agreed with these recommendations and committed to implementing them. Moreover, over the previous several years, it has made important progress in doing so, as prior reports have recognized. However, the pace of the progress has slowed over the last year as the roles, responsibilities, authorities, and relationships among recently established executive positions that are integral to defining and implementing these controls are worked out. In light of this, it is essential that the DBSMC, which is chaired by the DOD CMO, resolve these positional matters, as doing so is on the department's critical path for fully establishing the full range of institutional management controls needed to address its business systems modernization high-risk area.

Recommendations for Executive Action

Because we have existing recommendations that address most of the institutional management control weaknesses discussed in this report, we reiterate these recommendations.

In addition, to ensure that DOD continues to implement the full range of institutional management controls needed to address its business systems modernization high-risk area, we recommend that the Secretary of Defense direct the Deputy Secretary of Defense, as chair of the DBSMC and as DOD's CMO, to resolve the issues surrounding the roles, responsibilities, authorities, and relationships of the Deputy CMO and the military department CMOs relative to the BEA and ETP federation and business system investment management.

Further, to ensure that business system investment reviews and related certification and approval decisions, as well as annual budget submissions, are based on complete and accurate information, we recommend that the Secretary of Defense direct the appropriate DOD organizations to develop and implement plans for reconciling and validating the completeness and reliability of information in its DITPR and SNAP-IT system data repositories, and to include information on the status of these efforts in the department's fiscal year 2010 report in response to the Act.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the Assistant Deputy Chief Management Officer and reprinted in appendix II, the department stated that it has made important progress over the past year on its business system modernization, adding that this progress partly addresses our prior recommendations. We agree that the department has continued to make progress, and our report recognizes this. However, our report also recognizes that the pace of this progress has slowed in relation to prior years, and it links this slowdown to implementation of recent management structural changes within the department, which DOD's comments acknowledge have had to occur simultaneously.

To facilitate implementation of these structural changes, we recommended that DOD resolve the issues surrounding the roles, responsibilities, authorities, and relationships of the Deputy CMO and the military department CMOs relative to the BEA and ETP federation and business system investment management. DOD partially agreed with this recommendation. In particular, the department agreed that additional clarity would be useful in defining the roles and responsibilities of these positions and stated that it is committed to resolving this ambiguity through formal policy in the near future. However, the department stated that it believes that the Deputy CMO has the necessary authority, working on behalf of the Deputy Secretary of Defense, and that the Deputy CMO has a sufficiently close working relationship with the Deputy CMOs of the military departments to make significant strides in the department's

business operations improvement efforts, even in the absence of near-term formal guidance. We do not agree. As we have previously reported, the department has designated the role of the Deputy CMO as an advisor to the CMO, and it has not assigned the Deputy CMO clear decision-making authority.[115] Further, the absence of clarity around the Deputy CMO's role and responsibilities, which DOD acknowledged in its comments, combined with this absence of clear decision-making authority, directly affects the nature of the Deputy CMO's relationship with other senior leaders in the department, as relationships are a function of roles, responsibilities, and authorities. Therefore, we stand by our recommendation.

With regard to our second recommendation, to develop and implement plans for reconciling and validating the completeness and reliability of information in its DITPR and SNAP-IT data repositories, and to include information on the status of these efforts in the department's fiscal year 2010 report in response to the Act, DOD stated that it partially agreed with the recommendation. In particular, it agreed with the need to reconcile information between the two repositories and stated that it has begun to take actions to address this. For example, it stated that policy and guidance now require the components to enter information in both DITPR and SNAP-IT using what it described as a "one-to-one" relationship for all defense business systems, and that the DOD CIO is working with the components to facilitate implementation of this requirement. In addition, it stated that the DOD CIO and Office of Program Analysis and Evaluation are currently developing a plan to modify both DITPR and SNAP-IT to eliminate duplicate data and integrate them.

Notwithstanding its actions aimed at reconciling DITPR and SNAP-IT data, DOD commented that it disagreed that the data in the two repositories are unreliable, stating that differences in the data between the two are due to differences in the purpose of each repository, and that the data in each are complete and accurate enough to support their purposes. In response, we recognize that the repositories are used for different purposes. However, DOD guidance calls for business system information in the two repositories to be consistent and maintained at the same level of detail, which, as we state in our report, is not occurring. In particular, the number of business systems in DITPR and SNAP-IT is not consistent, which means that one or both lack important information about DOD business systems.

[115] GAO-09-272R.

As also stated in our report, system-specific information contained in DITPR is not accurate. For example, at least 900 systems showed life cycle phase start dates as the year 1900 or 1901, and at least 960 systems show a life cycle phase end date of 2099 or later. In addition, during the course of our review, DOD officials that we interviewed and who operate these repositories recognized these data limitations and agreed that more needed to be done to ensure data reliability.

DOD also provided technical comments on a draft of this report 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. 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 III.

Randolph C. Hite
Director
Information Technology Architecture
and Systems Issues

List of Committees

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 Thad Cochran
Ranking Member
Committee on Appropriations
Subcommittee on Defense
United States Senate

The Honorable Ike Skelton
Chairman
The Honorable John M. McHugh
Ranking Member
Committee on Armed Services
House of Representatives

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

Appendix I: Objective, Scope, and Methodology

As agreed with defense congressional committees, our objective was to assess the Department of Defense's (DOD) actions to comply with the requirements of section 2222 of Title 10, U.S. Code.[1] To address this, we used our last annual report under the Act as a baseline,[2] analyzing whether the department had taken actions to comply with five of the six requirements in section 2222, related best practices contained in federal guidance, and our prior recommendations that we previously identified as not yet addressed. Generally, these five requirements are (1) development of a business enterprise architecture (BEA), (2) development of an enterprise transition plan (ETP) 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, on delegating the responsibility for business systems to designated approval authorities, because our November 2005 report under the Act shows that it had been satisfied.[3] 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 6.0 of the BEA, which was released on March 13, 2009, relative to the Act's specific architectural requirements and related guidance that our last annual report under the Act identified as not being fully implemented. Specifically, we interviewed Business Transformation Agency (BTA) officials and reviewed written responses and related documentation on steps completed, under way, or planned to address these weaknesses. We then reviewed architectural artifacts in version 6.0 to validate the responses and identify any discrepancies. Further, we analyzed BEA supporting documentation (e.g., BEA compare reports) to determine the number of additions, updates, and deletions made to BEA artifacts (e.g., BEA business rules, data elements, data objects, data entities, information exchanges, system data exchanges,

[1]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).

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

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

system entities, system functions, system interfaces, and technical standards) as compared with the architectural content of version 5.0. We also analyzed BEA supporting documentation to identify the number of additions, updates, and deletions made to BEA artifacts (e.g., BEA business rules, data objects, system data exchanges, system entities, and system functions) that were specifically associated with the financial visibility business enterprise priority area.

To evaluate progress made in federating DOD's BEA, we reviewed DOD's Business Mission Area Architecture Federation Strategy and Roadmap Version 2.4, released in January 2008, comparing the strategy and any associated implementation plans with prior findings and recommendations relative to the content of the strategy. We also obtained documentation and interviewed cognizant DOD officials about efforts to establish a federated DOD business mission area enterprise architecture. Further, we reviewed the military departments' responses on actions taken or planned to address our previous recommendations on the maturity of their respective enterprise architecture programs.[4] In addition, we reviewed the independent verification and validation (IV&V) contractor's statement of work and IV&V reports to determine whether they addressed the quality of the department's federated family of corporate and component architectures, including the federated ETPs, and we interviewed the IV&V contractor and BTA officials to determine plans for future IV&V work to address the architectures' quality.

- To determine whether the DOD ETP addressed the requirements specified in the Act, we reviewed the updated version of the ETP, which was released on September 15, 2008, relative to the Act's requirements and related transition plan guidance that our last annual report under the Act identified as not being fully implemented.[5] Specifically, we interviewed BTA officials and reviewed written responses and related documentation on steps completed, under way, or planned to address these weaknesses. We then reviewed the plan to validate the responses and identify any discrepancies. In addition, to determine the extent to which the ETP included system and budget information for all the business systems identified in the department's information technology (IT) systems repository, we reviewed and compared the number of defense business systems listed in the department's authoritative business systems

[4]GAO, *DOD Business Systems Modernization: Military Departments Need to Strengthen Management of Enterprise Architectures*, GAO-08-519 (Washington D.C.: May 12, 2008).

[5]GAO-08-705.

inventory—the Defense Information Technology Portfolio Repository (DITPR)—with the number in its IT budget system, the Select and Native Programming Data Input System—Information Technology (SNAP-IT), with the number in the ETP. Further, we reviewed and compared business system information, such as legacy system migration information in the ETP, with the information obtained from our recently completed and ongoing business system reviews to determine whether the information was consistent. We interviewed BTA officials to discuss any discrepancies. Furthermore, we obtained and reviewed information from the Departments of the Air Force, Army, and Navy on the extent to which they have made progress in satisfying existing recommendations associated with developing their respective ETPs.

- We were unable to determine whether DOD's fiscal year 2010 information technology budget submission was prepared in accordance with the criteria set forth in the Act because the budget submission was not released in time for us to review for this report. Instead, we analyzed and compared information contained in the department's system that is used to prepare its budget submission (SNAP-IT) with information in the ETP and DOD's DITPR system to determine if DOD's fiscal year 2009 budget request included all business systems. We interviewed BTA and Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer (ASD(NII)/DOD CIO) officials to discuss the accuracy and comprehensiveness of information contained in the SNAP-IT system, the discrepancies in the information contained in the ETP, DITPR, and SNAP-IT systems, and efforts under way or planned to address these discrepancies. DOD officials were not able to provide the supporting data to address any discrepancies in the number of business systems contained in DITPR in time for inclusion in our report.

- To determine whether DOD has established investment review structures and processes, we focused on the one Investment Review Board specified in the Act that we previously reported had yet to be established. Accordingly, we obtained documentation from and interviewed cognizant DOD officials about actions completed, under way, and planned relative to the establishment of the DOD Chief Information Officer Investment Review Board. We also obtained and reviewed documentation—such as *DOD IT Defense Business Systems Investment Review Process Guidance and Operation of the Defense Acquisition System*, Department of

Defense Instruction Number 5000.02,[6] as well as the *Air Force Information Technology Investment Review Guide* and *Air Force Information Technology Portfolio Management and IT Investment Review*[7]—and interviewed knowledgeable DOD officials about efforts to address DOD corporate and component investment management-related weaknesses that we identified in previous reports. We also reviewed and leveraged our previous reports that addressed DOD corporate and component approaches to managing business system investments.[8]

- To determine whether the department was reviewing and approving business system investments exceeding $1 million, we obtained information from BTA on the number of defense business systems certified and approved since our last annual review, including information about Air Force, Army, and Navy actions that were taken in order to perform the annual systems reviews as required pursuant to the Act. In addition, we summarized the results of recent reports associated with information used during the certification and annual review process.[9] We also interviewed BTA and ASD(NII)/DOD CIO officials to determine the steps taken, planned, or under way to validate the accuracy of the information in DITPR to be used by the review boards in making certification and approval decisions. In addition, we analyzed selected

[6]DOD, *DOD IT Defense Business Systems Investment Review Process Guidance*, January 2009, and *Operation of the Defense Acquisition System*, Department of Defense Instruction Number 5000.02, Dec. 2, 2008.

[7]U.S. Air Force, *Air Force Information Technology Investment Review Guide, Ver. 2.2*, Nov. 24, 2008, and *Air Force Instruction 33-141: Air Force Information Technology Portfolio Management and IT Investment Review*, Dec. 23, 2008.

[8]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); *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); *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).

[9]GAO, *DOD Business Systems Modernization: Key Marine Corps System Acquisition Needs to Be Better Justified, Defined, and Managed*, GAO-08-822 (Washington, D.C.: July 28, 2008); *DOD Business Systems Modernization: Key Navy Programs' Compliance with DOD's Federated Business Enterprise Architecture Needs to Be Adequately Demonstrated*, GAO-08-972 (Washington, D.C.: Aug. 7, 2008); and *DOD Business Systems Modernization: Important Management Controls Being Implemented on Major Navy Program, but Improvements Needed in Key Areas*, GAO-08-896 (Washington, D.C.: Sept. 8, 2008).

business system information contained in DITPR, such as system life cycle start and end dates, to validate the reliability of the information.

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 offices in Arlington, Virginia, from January 2009 to May 2009, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Department of Defense

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

MAY 22 2009

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

Dear Mr. Hite:

This is the Department of Defense (DoD) response to the GAO draft report 09-586, "DOD BUSINESS SYSTEMS MODERNIZATION: Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed" dated April 27, 2009 (GAO Code 310675).

The Department welcomes GAO's insight and acknowledgement of its business systems modernization progress. DoD believes that it has made important progress over the past year while simultaneously implementing recently passed statutes involving changes to the management structure for its business operations. This progress partly addresses open business systems modernization GAO recommendations and DoD will continue to take steps to address open recommendations.

The Department partially concurs with GAO's recommendation to resolve issues surrounding the roles, responsibilities, authorities, and relationships of the Deputy Chief Management Officer (DCMO) and the Military Departments' Chief Management Officers (CMOs). DoD agrees that additional clarity would be useful in defining the roles and responsibilities of these positions and DoD is committed to resolving this ambiguity through formal policy sometime in the future. However, the Department believes that the DoD DCMO has the necessary authority, working on behalf of the Deputy Secretary of Defense, and a sufficiently close working relationship with the DCMOs of the Military Departments to make significant strides in the Department's business operations improvement efforts, even in the absence of near-term, formal guidance.

DoD partially concurs with the recommendation regarding the alignment of the data in the Defense Information Technology Portfolio Repository (DITPR) and

Select and Native Programming Data Input System – Information Technology (SNaP-IT) system data repositories. The Department recognizes the need to reconcile the information between the two systems, and has taken some steps in recent years to accomplish this, such as updating the Financial Management Regulation to include the requirement for Components to enter data in the two systems using a one-to-one relationship for all defense business systems, and is currently developing a plan to further align the data. However, DoD believes that the quality of the data in both systems supports the purposes for which those systems are intended to be used.

We appreciate the support of GAO as the Department further advances in its business transformation efforts, and look forward to continuing our partnership in achieving our shared goals.

Elizabeth A. McGrath
Assistant Deputy Chief Management Officer

GAO DRAFT REPORT DATED APRIL 24, 2009
GAO-09-586 (GAO CODE 310675)

"DOD BUSINESS SYSTEMS MODERNIZATION: RECENT SLOWDOWN IN INSTITUTIONALIZING KEY MANAGEMENT CONTROLS NEEDS TO BE ADDRESSED"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Deputy Secretary of Defense to resolve the issues surrounding the roles, responsibilities, authorities, and relationships of the Deputy Chief Management Officer and the military department Chief Management Officers relative to the Business Enterprise Architecture and enterprise transition plan federation and business system investment management. (p. 61/GAO Draft Report)

DOD RESPONSE: Partially Concur. The Department partially concurs with GAO's recommendation to resolve issues surrounding the roles, responsibilities, authorities, and relationships of the Deputy Chief Management Officer (DCMO) and the Military Departments' Chief Management Officers (CMOs). DoD agrees that additional clarity would be useful in defining the roles and responsibilities of these positions and DoD is committed to resolving this ambiguity through formal policy in the near future. However, the Department believes that the DoD DCMO has the necessary authority, working on behalf of the Deputy Secretary of Defense, and a sufficiently close working relationship with the DCMOs of the Military Departments to make significant strides in the Department's business operations improvement efforts, even in the absence of near-term, formal guidance. Federation of the Business Enterprise Architecture and Enterprise Transition Plan and improvement of the business system investment management process remain key objectives of the Department's improvement efforts. The Office of the DoD DCMO, in conjunction with the Business Transformation Agency, is currently working with the Military Department DCMOs and other appropriate officials to advance these initiatives.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the appropriate DoD organizations to develop and implement plans for reconciling and validating the completeness and reliability of information in its Defense Information Technology Portfolio Repository (DITPR) and Select and Native Programming Data Input System – Information Technology (SNaP-IT) system data repositories, and to include information on the status of these efforts in the department's FY 2010 report in response to the act. (p. 61/GAO Draft Report)

DOD RESPONSE: Partially Concur. DOD agrees with the GAO recommendation to synchronize information stored in SNaP-IT and DITPR, and has already taken steps to

Attachment
Page 1 of 2

address this need. Currently, a many-to-many relationship exists between "Systems" for which technical information is stored in DITPR, and "Initiatives" for which financial information is stored in SNaP-IT. An update to the regulation that provides financial management policy and procedures to the DOD was issued in June 2007[1] requiring components to start entering information in both DITPR and SNaP-IT using a one-to-one relationship for all defense business systems. The Department of Defense Chief Information Officer (DOD CIO) is now working with the components to help facilitate implementation of that policy. This policy is also stated in guidance issued in July 2008.[2]

In addition, the DOD CIO and the Office of Program Analysis and Evaluation (PA&E) are currently working on a plan to modify both DITPR and SNaP-IT to eliminate the duplication of data and use web services to provide seamless integration of the two systems. Completion of the technical effort is expected in the next 12 months. Challenges to completing the non-technical aspects of this effort include; a) changes in component-level policies and practices for budgeting and reporting information technology (IT) systems and b) alignment of IT investments currently reported in SNaP-IT and DITPR. DOD CIO will collaborate with the components to make the necessary changes to these policies and practices.

However, the Department disagrees with the GAO's implication that the data in the two systems is not reliable. It should be noted that differences in information between the two systems are due to the information being collected and displayed for different purposes. Current Investment Review Board (IRB) Guidance states that a program's Program Manager (PM) ensures and the Pre-Certification Authority (PCA) validates the information in DITPR as being current, complete and accurate. In addition, the DOD CIO currently requires components to certify the completeness and accuracy of required data in both DITPR and SNaP-IT. There has been significant improvement in the quality of information in both systems since the implementation of this requirement. DOD CIO believes the quality of information in both systems is complete and accurate enough to support their purposes.

[1] "Financial Management Regulation", DoD 7000.14-R, Volume 2B, Chapter 18, Section 180103.G, issued under the authority of DoD Instruction 7000.14, "DoD Financial Management Policy and Procedures."

[2] "Office of the Secretary of Defense (OSD) Guidance for FY2010 Information Technology Submissions".

Attachment
Page 2 of 2

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact person named above, key contributors to this report were Neelaxi Lakhmani (Assistant Director), Justin Booth, Michael Holland, Anh Le, Emily Longcore, Lee McCracken, Christine San, Sylvia Shanks, Jennifer Stavros-Turner, and Adam Vodraska.

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

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