

GAO

Report to the Subcommittee on
Readiness and Management Support,
Committee on Armed Services,
U.S. Senate

August 2008

DOD BUSINESS SYSTEMS MODERNIZATION

Key Navy Programs'
Compliance with
DOD's Federated
Business Enterprise
Architecture Needs to
Be Adequately
Demonstrated





Highlights of [GAO-08-972](#), a report to the Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate

Why GAO Did This Study

For decades, the Department of Defense (DOD) has been challenged in modernizing its thousands of business systems. Since 1995, GAO has designated the department's business systems modernization efforts as high risk. One key to effectively modernizing DOD's systems environment and satisfying relevant legislative requirements is ensuring that business system investments comply with an enterprisewide strategic blueprint, commonly called an enterprise architecture. For DOD's business systems modernization, it is developing and using a federated Business Enterprise Architecture (BEA), which is a coherent family of parent and subsidiary architectures. GAO was requested to determine whether key Department of the Navy business systems modernization programs comply with DOD's federated BEA. To determine this, GAO examined the BEA compliance assessments, certifications, and approvals for selected Navy programs against relevant guidance.

What GAO Recommends

GAO is making several recommendations aimed at improving DOD's guidance, assessment tool, and related approval processes for ensuring that business system investments comply with the department's federated BEA. DOD agreed with GAO's recommendations and described actions planned and under way to address them.

To view the full product, including the scope and methodology, click on [GAO-08-972](#). For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

DOD BUSINESS SYSTEMS MODERNIZATION

Key Navy Programs' Compliance with DOD's Federated Business Enterprise Architecture Needs to Be Adequately Demonstrated

What GAO Found

Key DOD business systems modernization programs do 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 entities. In particular, the programs' BEA compliance assessments did not

- include all relevant architecture products, such as products that specify the technical standards needed to promote interoperability among related systems;
- 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
- address compliance with the Department of the Navy's enterprise architecture, which is a major BEA federation member.

These important steps were not performed for a variety of reasons, including the fact that the department's guidance does not provide for performing them and its assessment tool is not configured to do so.

In addition, even though the department's investment oversight and decision-making authorities 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. According to DOD officials, department policy and guidance do not require these authorities to do so. Instead, they said that this responsibility is assigned to DOD's component organizations, such as the Department of the Navy. However, Department of the Navy oversight and decision-making authorities also did not validate the programs' assessments and assertions. According to department officials from the Office of the Chief Information Officer, this is because these authorities do not have the resources needed to do so and because important aspects of the Department of the Navy enterprise architecture are not yet sufficiently developed to permit a compliance determination. In addition, guidance does not exist that specifies how an assessment should be validated.

Because of these limitations, these and other DOD programs are at increased risk of being defined and implemented in a way that does not sufficiently ensure interoperability and avoid duplication and overlap, which are both goals of the BEA and the department's related investment management approach. Unless this changes, DOD and its components will not have a sufficient basis for knowing if its business system programs have been defined to effectively and efficiently support corporate business operations, and DOD's business systems modernization efforts will likely remain on GAO's high-risk list.

Contents

Letter		1
	Briefing Summary	2
	Conclusions	4
	Recommendations for Executive Action	4
	Agency Comments	5
Appendix I	Briefing to Staff, Subcommittee on Readiness and Management Support, Senate Committee on Armed Services	7
Appendix II	Comments from the Department of Defense	57
Appendix III	GAO Contact and Staff Acknowledgments	60

Abbreviations

ACART	Architecture Compliance and Requirements Traceability
BEA	business enterprise architecture
BTA	Business Transformation Agency
CIO	Chief Information Officer
DBSMC	Defense Business Systems Management Committee
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DON	Department of the Navy
FAM	functional area manager
GCSS-MC	Global Combat Support System-Marine Corps
IRB	Investment Review Board
Navy ERP	Navy Enterprise Resource Planning
NDAAs	National Defense Authorization Act
SOAP	simple object access protocol

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



United States Government Accountability Office
Washington, DC 20548

August 7, 2008

The Honorable Daniel K. Akaka
Chairman
The Honorable John Thune
Ranking Member
Subcommittee on Readiness and Management Support
Committee on Armed Services
United States Senate

For decades, the Department of Defense (DOD) has been challenged in its efforts to modernize its thousands of business systems. In 1995, we first designated DOD's business systems modernization program as a high-risk program, and we continue to designate it as such today.¹ As our research shows, one key ingredient to effectively modernizing an organization's systems environment is ensuring that system investments are in compliance with an enterprisewide strategic blueprint—commonly called an enterprise architecture. Accordingly, we first recommended DOD's development and implementation of an enterprise architecture for its business mission area in 2001. In addition, the *Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*² requires DOD to develop and implement a business enterprise architecture (BEA).

DOD has adopted an incremental, federated³ approach to developing the operational, system, and technical products that comprise its BEA.⁴ We have previously reported that this approach is consistent with best practices and appropriate given the department's size and scope of

¹GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

²*Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*, Pub. L. No. 108-375, § 332 (2004) (codified at 10 U.S.C. §§ 186 and 2222).

³A federated architecture consists of a family of coherent but distinct member architectures in which subsidiary architectures conform to an overarching corporate architectural view and rule set.

⁴The BEA's content is governed by DOD's architecture framework, which describes various architecture products that define different aspects of an enterprise architecture, such as business or operational activities and relationships and information exchanges among these activities.

operations.⁵ According to DOD, one purpose of the federated BEA is to identify and provide for sharing common applications and systems across the department and the components and promote interoperability and data sharing among related programs. To accomplish this, it is important for programs to ensure that they are in compliance with the federated BEA throughout their life cycles. Accordingly, you asked us to determine whether key Department of the Navy (DON)⁶ modernization programs comply with DOD's federated BEA.

To accomplish this objective, we focused on two business systems modernization programs—the Global Combat Support System-Marine Corps and Navy Enterprise Resource Planning. We selected these programs because they involve relatively large amounts of modernization funding; are reviewed, certified, and approved by different investment review bodies; and are at different stages in their acquisition life cycles. For each program, we reviewed its architecture compliance assessments and system architecture products as well as relevant BEA products. We also reviewed DOD's architecture compliance guidance and assessment tool and interviewed DOD and DON officials.

On May 30, 2008, we briefed your staff on the results of our review. This report transmits those results. The full briefing, including our objective, scope, and methodology, is reprinted in appendix I.

Briefing Summary

Key DOD business systems have not adequately demonstrated that they are in compliance with DOD's BEA, even though they largely followed DOD's compliance guidance and used its compliance assessment tool. Specifically:

- The programs did not include all relevant architecture products in the scope of their compliance assessments. For example, the assessments did not address compliance with key BEA products that describe technical standards and system characteristics. They did not address compliance with these products because DOD guidance does not provide for doing so and, according to department officials, because some BEA products

⁵GAO, *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).

⁶DON consists of two military services—the Navy and the Marine Corps.

(e.g., technical standards profile) are not yet sufficiently defined. Compliance with these products is important because they govern how systems physically communicate with other systems, and they permit the identification of common system components and services that could potentially be shared.

- The compliance assessments were not used to identify potential areas of duplication across programs, which DOD has stated is a goal of its BEA and associated investment review and decision-making processes. Potential duplication was not assessed because the compliance guidance does not provide for such analyses to be conducted, and programs have not been granted access to this functionality in the compliance tool. As a result, these programs may be investing in duplicative functionality.
- The compliance assessments did not address compliance with the DON's enterprise architecture, which is one of the biggest members of the federated BEA. This is particularly important given that DOD's approach to fully satisfying the architecture requirements of the *Fiscal Year 2005 National Defense Authorization Act* is to develop and use a federated architecture in which component architectures are to provide the additional business system data and technical content needed to supplement the thin layer of corporate policies, rules, and standards included in the corporate BEA. As we have recently reported,⁷ the DON enterprise architecture is not mature because, among other things, it is missing a sufficient description of its current and future environments in terms of business and information/data. However, certain aspects of an architecture nevertheless exist and, according to department officials, these aspects will be leveraged in the department's efforts to develop a complete enterprise architecture. Therefore, opportunities exist to assess programs in relation to these architecture products and to understand where its programs are exposed to risks because products do not exist, are not mature, or are at odds with other programs. According to DOD officials, compliance with the DON architecture was not assessed because DOD policy is limited to the corporate BEA compliance and because aspects of the DON enterprise architecture have yet to be sufficiently developed.
- The programs' compliance assessments or assertions were not validated by either DOD or DON investment oversight and decision-making

⁷GAO, *DOD Business Systems Modernization: Military Departments Need to Strengthen Management of Enterprise Architecture Programs*, [GAO-08-519](#) (Washington, D.C.: May 12, 2008).

authorities. According to department officials, relevant department policy and guidance do not require the DOD oversight authorities to do so. Instead, they said that the department's investment approach assigns this responsibility to its component organizations. However, DON oversight and decision-making authorities did not validate the assessments and assertions. According to DON officials, this is because these authorities do not have the resources needed to validate the assessments, and because aspects of the DON enterprise architecture are not yet sufficiently developed. In addition, guidance does not exist that specifies how an assessment should be validated.

Conclusions

A demonstrated ability to repeatedly ensure that DOD's business system investments are defined and implemented within the context of the department's federated BEA is a legislative requirement and a prerequisite for removal of DOD's business systems modernization program from our high-risk list. To its credit, DOD has recently taken steps aimed at demonstrating that its business systems comply with its BEA, including issuing compliance assessment guidance, providing a compliance assessment tool, and making the compliance assessment results part of a program's certification and approval by department investment decision-making authorities. Nevertheless, the extent to which the two key programs comply with the federated BEA was not adequately demonstrated. Moreover, the compliance assertions provided by these programs were not subject to oversight by either DOD or DON program investment decision-making authorities. This situation can be attributed to limitations in existing BEA compliance-related policy and guidance, the supporting compliance assessment tool, and the federated BEA, as well as the absence of DON compliance guidance. Accordingly, these and other DOD programs are at increased risk of being defined and implemented in a way that does not sufficiently ensure interoperability and avoid duplication and overlap, which are both goals of the BEA and related investment management approach. Unless this situation changes, the department's business systems modernization efforts will likely remain a high-risk endeavor.

Recommendations for Executive Action

To adequately ensure that DOD business system investments are defined and implemented within the context of its federated BEA, we recommend that the Secretary of Defense direct the responsible authorities in the department to take the following four actions:

-
- Revise the DOD BEA compliance assessment guidance to (1) include assessment of all relevant operational, technical, and system architecture products and (2) provide for the development and use of key program architecture products in conducting the assessment early enough in the program's life cycle to permit the results of the assessments to have a timely impact on the program's definition, design, and implementation.
 - Use the program-specific data in the compliance assessment tool for identifying and analyzing potential overlap and duplication, and thus opportunities for reuse and consolidation among programs and provide programs access rights to use this functionality.
 - Amend relevant DOD policy to explicitly require business system program compliance with the federated BEA, to include both the corporate BEA and the component enterprise architectures as a condition for program certification and approval.
 - Amend relevant DOD policy to explicitly assign responsibility for validating program BEA compliance assertions to military departments and defense agencies and issue guidance that describes the nature, scope, and methodology for doing so.

Agency Comments

In written comments on a draft of this report, signed by the Deputy Under Secretary of Defense (Business Transformation) and reprinted in appendix II, the department agreed with our recommendations and described actions under way or planned to address them. It also stated that as the federated family of BEA parent and subsidiary architectures mature, it will meet the intent of our recommendations in future versions of its compliance guidance, policies, and methodologies.

We are sending copies of this report to interested congressional committees; the Director, Office of Management and Budget; the Congressional Budget Office; the Secretary of Defense; and the Department of Defense Inspector General. We also will make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-3439 or at 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 have made significant contributions to this report are listed in appendix III.

A handwritten signature in black ink, reading "Randolph C. Hite". The signature is written in a cursive style with a large initial "R" and a distinct "Hite" at the end.

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Appendix I: Briefing to Staff, Subcommittee on Readiness and Management Support, Senate Committee on Armed Services



DOD Business Systems Modernization: Key Navy Programs’ Compliance with DOD’s Federated Business Enterprise Architecture Needs to be Adequately Demonstrated

Briefing for staff members of the

Subcommittee on Readiness and Management Support,
Senate Armed Services Committee

May 30, 2008



Overview

Introduction

Results in Brief

Background

Results: Federated BEA Compliance

Conclusions

Recommendations for Executive Action

Appendix I: Objective, Scope, and Methodology

Appendix II: DOD's Federated Business Enterprise Architecture

Appendix III: Descriptions of Business Enterprise Architecture Products



Introduction

For decades, the Department of Defense (DOD) has been challenged in modernizing its thousands of business systems. In 1995, we first designated DOD's business systems modernization program as a high risk program, and we continue to designate it as such today.¹ As our research shows, one key ingredient to effectively modernizing an organization's systems environment is ensuring that system investments are in compliance with an enterprise-wide strategic blueprint—commonly called an enterprise architecture. Accordingly, we first recommended DOD's development and implementation of an enterprise architecture for its business mission area in 2001. In addition, the Fiscal Year 2005 Ronald W. Reagan National Defense Authorization Act (NDAA) requires DOD to develop and implement a business enterprise architecture (BEA).

DOD has adopted an incremental, federated approach to developing its BEA.² We have previously reported that this approach is consistent with best practices and appropriate given the department's size and scope of operations.³ According to DOD, one purpose of

¹GAO, *High-Risk Series: An Update*, [GAO-07-310](#) (Washington, D.C.: January 2007).

²A federated architecture consists of a family of coherent but distinct member architectures in which subsidiary architectures conform to an overarching corporate architectural view and rule set.

³GAO, *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).



Introduction

the federated BEA is to identify and provide for sharing common applications and systems across the department and the components and promote interoperability and data sharing among related programs. To accomplish this, it is important for programs to ensure that they are in compliance with the BEA throughout their life cycle.

Concurrent with its efforts to develop a BEA, DOD and its components continue to invest billions of dollars annually in thousands of business systems. Within the Department of the Navy (DON),⁴ two of these systems are the Global Combat Support System—Marine Corps (GCSS-MC) and Navy Enterprise Resource Planning (ERP).

⁴DON consists of two military services—the Navy and the Marine Corps.



Introduction

Because of the importance of developing business systems within the context of the DOD BEA, you asked us to determine whether key Navy modernization programs comply with DOD's federated BEA.

To accomplish this objective, we performed case studies on two business system modernization programs—GCSS-MC and Navy ERP. We selected these programs because they involve relatively large amounts of modernization funding; are reviewed, certified, and approved by different investment review bodies; and are at different stages in their acquisition life cycles. For each program, we reviewed its architecture compliance assessments and system architecture products as well as relevant BEA products. We also reviewed DOD's architecture compliance guidance and assessment tool and interviewed DOD and DON officials.

We conducted our work at DOD and DON offices and contractor facilities in the Washington, DC metropolitan area, in Annapolis, Maryland, and in Triangle, Virginia, between June 2007 and May 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For details on our objective, scope, and methodology, see appendix I.



Results in Brief

Key DOD business system modernization programs do not adequately comply with the department's federated BEA, even though each program largely followed the BEA compliance guidance, used the compliance assessment tool, and was certified and approved as compliant with the BEA by investment oversight and decisionmaking entities. In particular, the programs' BEA compliance assessments did not

- include all relevant architecture products, such as products that specify the technical standards needed to promote interoperability among related systems;
- 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
- address compliance with the DON's enterprise architecture, which is a major component of the federated BEA.

These important steps were not performed for a variety of reasons, including that the department's guidance does not provide for them and its assessment tool is not configured to do so.

In addition, business system certification and approval authorities did not validate the programs' compliance assessments and assertions. According to DOD Business Transformation Agency (BTA) officials, relevant department policy and guidance



Results in Brief

do not require these authorities to do so. Instead, they said that the department’s “tiered accountability” investment approach assigns this responsibility to its component organizations. However, DON oversight and decisionmaking authorities did not validate the assessments and assertions. According to DON Chief Information Officer (CIO) officials, this is because these authorities do not have the resources needed to validate the assessments and because the DON enterprise architecture is not yet sufficiently developed. In addition, guidance does not exist that specifies how an assessment should be validated.

Because of these limitations, DOD does not have a sufficient basis for knowing if programs like GCSS-MC and Navy ERP have been defined to effectively and efficiently support corporate business operations. To address these limitations, we are recommending that the department (1) revise the compliance assessment guidance to provide for assessment of all relevant architecture products; (2) use program-specific compliance assessment data in the tool for identifying and analyzing potential overlap and duplication among programs; (3) require business system program compliance with the federated BEA, including the component enterprise architectures; and (4) assign responsibility for validating program BEA compliance assertions to military departments and defense agencies.



Results in Brief

In comments on a draft of this briefing, DOD and DON officials agreed with our findings, conclusions, and recommendations.



Background

DOD's business system environment includes approximately 3,000 business system investments, which are supported by billions of dollars in annual expenditures and are intended to support business functions and operations, such as financial management and logistics. For fiscal year 2009, the department requested about \$15 billion for its business systems and related IT infrastructure.

DOD's business system modernization was added to GAO's high-risk list in 1995. Because the department continues to face longstanding challenges in delivering promised system capabilities and benefits on time and within budget, it remains on our high risk list today.⁵

⁵[GAO-07-310](#).



Background

Successful Systems Modernization Depends on Effective Implementation of a Well-Defined Enterprise Architecture

As our research on public and private sector organizations shows, one key to a successful systems modernization program is having and using a well-defined enterprise architecture. A well-defined 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., personnel management). This picture consists of snapshots of both the enterprise's current or "As Is" environment and its target or "To Be" environment, as well as a capital investment road map for transitioning from the current to the target environment. These snapshots consist of integrated "views," which are one or more architecture products that describe, for example, the enterprise's business processes and rules; information needs and flows among functions, supporting systems, services, and applications; and data and technical standards and structures.



Background

As we have previously reported,⁶ not having and using such an architecture produces agency system environments that:

- display little standardization (and thus interoperability);
- have multiple systems performing the same tasks;
- exhibit data duplication and redundancy across multiple systems; and
- require manual reentry of data into multiple systems.

DOD's business operations have long been hampered by such a system environment, due in large part to decades of investing in business systems outside the context of an enterprise architecture.

⁶GAO, *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, [GAO-04-777](#) (Washington, D.C.: Aug. 6, 2004) and [GAO-04-731R](#); *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, [GAO-04-43](#) (Washington, D.C.: Nov. 21, 2003).



Background

Overview of DOD, GAO, and Congressional Efforts Related to Using a DOD-wide Architecture for Business Systems Modernization

To assist DOD in addressing this high risk area, we have made numerous recommendations for establishing institutional and program-level modernization management capabilities. Among others, in 2001, we made recommendations aimed at effectively developing and implementing an architecture and limiting components' systems investments until DOD had a well-defined architecture and the means to enforce it.⁷ Further, we made additional recommendations as to how to accomplish this goal.

In 2004, Congress passed the Fiscal Year 2005 NDAA,⁸ which included provisions consistent with our recommendations, including:

- developing a well-defined departmentwide BEA and
- certifying business system investment compliance with the BEA.

⁷GAO, *Information Technology: Architecture Needed to Guide Modernization of DOD's Financial Operations*, [GAO-01-525](#) (Washington, D.C.: May 17, 2001).

⁸*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 at 10 U.S.C. § 2222).



Background

DOD's initial efforts to develop the BEA were focused on developing a single, monolithic architecture for the entire department. The department invested about 4 years and about \$300 million without adequately implementing our recommendations addressing the development and use of the architecture. In July 2005, we reported that the BEA provided limited utility to guide and constrain the department's ongoing and planned business investments.⁹ Accordingly, we made recommendations relative to the content of the BEA, among other things. Subsequently, DOD adopted an incremental, federated architecture development approach. As we have previously stated, this approach is appropriate given DOD's size and scope and is consistent with best practices. One of the purposes of this approach is to identify and provide for sharing of common applications and systems across the department and the components. Appendix II provides additional information about DOD's federated BEA.

⁹GAO. *DOD Business Systems Modernization: Long-standing Weaknesses in Enterprise Architecture Development Need to Be Addressed*, [GAO-05-702](#) (Washington, D.C., July 22, 2005).



Background

The latest version of the corporate BEA (version 5.0) was issued on March 14, 2008. On May 15, 2008, we reported that this version largely provides the thin layer of DOD-wide architectural policies, capabilities, rules, and standards for the business mission area¹⁰ and that this layer is essential to a well-defined federated architecture, but was still missing important content.¹¹ We also said that the corporate BEA alone does not provide the total federated family of DOD parent and subsidiary architectures for the business mission area that are needed to comply with the legislative requirements in the fiscal year 2005 NDAA. Specifically, we stated that the latest version had yet to be augmented by the DOD component organizations' subsidiary architectures. Moreover, we also recently reported that the Departments of the Army, Air Force, and Navy did not have sufficiently mature enterprise architecture programs, although the Air Force was considerably further along in developing its architecture than either the Navy or the Army.¹²

¹⁰[GAO-08-705](#).

¹¹For example, we recently reported that the latest version of the BEA does not describe information flows for all organizational units, such as information exchanges among the organizations that support the Human Resources Management enterprise priority area, and continues to lack information flows among DOD corporate and components organizations.

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



Background

We have also recently reported on management weaknesses in a number of DOD business system programs. Among other things, we reported that these programs had not been developed in the context of well-defined DOD and component architectures. Examples of these programs include

- the Navy's Naval Tactical Command Support System and
- the Army's (1) Transportation Coordinators' Automated Information for Movements System II, (2) General Fund Enterprise Business System, (3) Global Combat Support System-Army, and (4) Logistics Modernization programs.¹³

¹³GAO, *DOD Business Transformation: Lack of an Integrated Strategy Puts the Army's Asset Visibility System Investments at Risk*, [GAO-07-860](#) (Washington, D.C.: July 27, 2007); *DOD Systems Modernization: Planned Investment in the Naval Tactical Command Support System Needs to Be Reassessed*, GAO-06-215 (Washington: D.C.: Dec. 5, 2005), and *DOD Systems Modernization: Uncertain Joint Use and Marginal Expected Value of Military Asset Deployment System Warrant Reassessment of Planned Investment*, [GAO-06-171](#) (Washington, D.C.: Dec. 15, 2005).



Background

Overview of DOD Architecture Framework Products

DOD's corporate BEA was developed according to the Department of Defense Architecture Framework (DODAF),¹⁴ which specifies a set of three "views"—operational, systems, and technical—each of which includes various architecture products that apply to DOD, component, and program-level system architectures.

- Operational view products include the high level, DOD-wide operational activities and business processes and rules, as well as the data standards and information flows among these activities and processes.
- Systems view products include systems capabilities, functions, and related data exchanges.
- Technical view products describe the set of technology constraints that will drive the manner of system implementation.

Appendix III describes key DODAF products that are associated with the BEA.

¹⁴DODAF is DOD's guide for developing architectures. See for example DOD, *Department of Defense Architecture Framework*, Version 1.5, Volume 1 (April 2007).



Background

Overview of DOD's BEA Compliance Guidance

In 2006, the Business Transformation Agency (BTA), which is responsible for leading and coordinating business transformation efforts across DOD, issued guidance to assist components in assessing their respective programs' compliance with the BEA.¹⁵ This guidance

- defines compliance as adherence to the controls (requirements), business rules, and standard data elements of those BEA operational activities that the program being assessed supports;
- identifies the program architecture products to be used for assessing BEA compliance at various points during a program's life cycle; and
- identifies the BEA products against which program compliance is to be assessed.

¹⁵Department of Defense, *Business Enterprise Architecture Compliance Guidance*, (April 2006).



Background

The specific BEA and program DODAF products to be used in assessing compliance are described below. (See figure 1 for examples of relationships between BEA products.)

Operational information exchange matrix (OV-3): Describes the information exchanges associated with operational activities. For example, after an inventory is complete, information about “equipment” and “property location” would be exchanged between the activity “conduct physical inventory” and the activity “maintain asset information.”

Operational activity model (OV-5): Describes the operations conducted by the business mission area and the relationships (e.g., inputs and outputs) between operational activities. For example, the activity “conduct physical inventory” involves verifying the existence, location, and quantity of real property. This activity produces physical asset inventory information that is used by the operational activity “maintain asset information.”

Operational rules model (OV-6a): Describes the business rules that constrain operations. For example, the business rule “asset unique identifier 1” requires real property unique identifiers¹⁶ to be validated and cross-referenced at creation to prevent duplication.

¹⁶Real property unique identifiers are codes that identify specific assets.



Background

Operational event-trace description (OV-6c): Describes the business processes needed to execute an operational activity. For example, the business process “count assets” involves physically counting assets to ensure accountability (existence, quantity, and condition) to enable accurate valuation of existing assets.

Logical data model (OV-7): Describes data entities and their attributes. For example, “property_identifier” is an attribute of the data entity¹⁷ “equipment” that distinguishes one form of property from another.

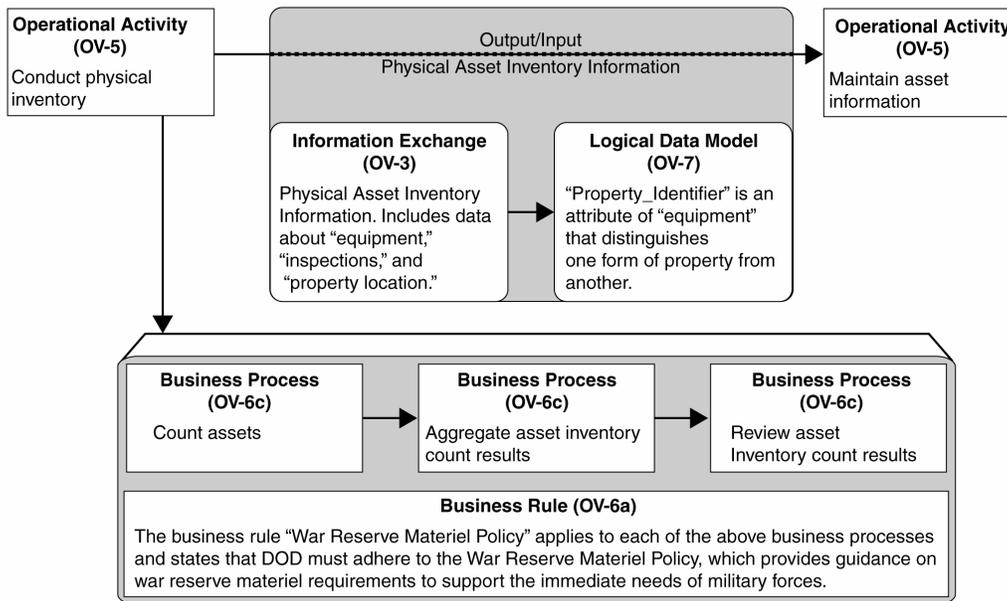
Operational activity to systems function traceability matrix (SV-5): Identifies the relationships between operational activities and system functions. For example, the “conduct physical inventory” activity is supported by the “manage asset record” system function, which is to ensure that electronic information about the status of assets is consistent with the actual status of the asset, including the item's physical, legal, and financial status.

¹⁷Data entities refer to a thing or event about which information is kept in a database. For example, “address” is an entity in the BEA that identifies a location at which an “organization” or “person” may be contacted. Data attributes refer to properties/characteristics of an entity, such as “address street number/name and postal zone.”



Background

Figure 1: Examples of Relationships Among Selected BEA Products



Source: GAO analysis of DOD data.



Background

Table 1 identifies when in the program’s lifecycle¹⁸ program architecture products are to be used to support BEA compliance assessments.

Table 1: Investment Life cycle Phases at Which Program Level Architecture Products Are Used in BEA Compliance Assessment

Program architecture product	Technology development	System development and demonstration	Production and deployment
Operational information exchange matrix			X
Operational activity model	X	X	X
Operational rules model		X	X
Operational event-trace description		X	X
Logical data model			X
Operational activity to systems function traceability matrix			X

Source: DOD

¹⁸The life cycle phases are (1) technology development, which is between milestones A and B, and is when the program is to determine the appropriate set of technologies to be integrated into the investment solution; (2) system development and demonstration, which is between milestones B and C, and is when the program is developed and tested to demonstrate that it can function in its target environment; and (3) production and deployment, which is between milestone C and post-deployment, and is when operational capability, verified through independent operational test and evaluation, is achieved.



Background

According to the guidance, programs are to perform four steps to assess program compliance with the BEA:

- Identify relevant activities: Identify the operational activities in the BEA that the program supports.
- Assess activity control compliance: (1) Identify controls (laws, regulations, and policies) in the BEA that are associated with the relevant operational activities identified in step 1; and (2) determine if the program complies with these controls.
- Assess business rule compliance: (1) Identify the business processes in the BEA that support the operational activities identified in step 1; (2) identify the business rules associated with each of these processes; and (3) determine if the program complies with these business rules.
- Assess data compliance: (1) Identify the inputs and outputs associated with the operational activities identified in step 1; (2) identify information exchange requirements associated with these inputs and outputs; (3) identify the data entities that support these information exchanges; and (4) determine if the program's data entity definitions conform to the BEA data entity definitions.



Background

Overview of DOD Architecture Compliance Tool

The BTA has developed a tool that DOD component organizations are given the option of using in assessing compliance with the BEA—the Architecture Compliance and Requirements Traceability (ACART) tool. DON requires all of its business programs to use ACART.

ACART is to:

- Identify for the program the BEA products that the program needs to assess and assert compliance against based on the program’s self-identification of relevant BEA operational activities.
- Serve as a repository of all BEA products that the program actually asserts compliance against.



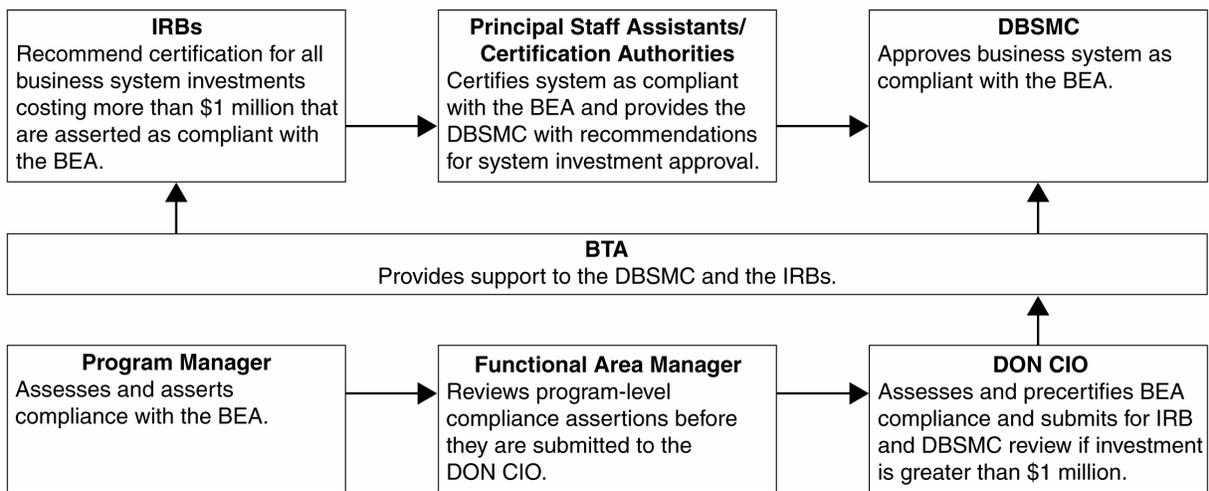
Background

The program-level compliance assessments form the basis for program assertions of compliance. These assertions in turn are used by the cognizant investment and oversight authorities, the Investment Review Boards (IRB) and the Defense Business Systems Management Committee (DBSMC) when reviewing, certifying, and/or approving systems as compliant with the BEA. The roles and responsibilities of those entities involved in BEA compliance determinations for the two systems that we reviewed are summarized in figure 2.



Background

Figure 2: BEA Compliance Roles and Responsibilities



Source: GAO analysis of DOD data.



Background

Overview of Two Key Business System Programs

GCSS-MC and Navy ERP are two of DON's largest and most costly business system modernization programs. Together, the two programs have an estimated life cycle cost of about \$3 billion. According to the requirements of the fiscal year 2005 NDAA, these programs are required to be certified as compliant with the BEA and to undergo annual review by DOD's business system investment review boards and the Defense Business Systems Management Committee.

- GCSS-MC was initiated in 2003 to modernize the Marine Corps logistics systems and to provide the Corps with timely and complete logistics information to support the warfighter.¹⁹ This program consists of a series of major increments, the first of which has an expected life cycle cost of approximately \$442 million through fiscal year 2019. It is to be fully deployed in fiscal year 2010.
- Navy ERP was initiated in 2003 to modernize and standardize the Navy's acquisition, financial, program management, maintenance, plant and wholesale supply, and workforce management business processes. This program is planned to be deployed

¹⁹Warfighter refers to a member of the United States armed forces.



Background

in a series of major increments, the first having an estimated life cycle cost of approximately \$2.4 billion through fiscal year 2023. It is to be fully deployed in fiscal year 2013.

According to program officials, both GCSS-MC and Navy ERP are under the leadership of DON's Program Executive Office for Enterprise Information Systems, which is responsible for developing, acquiring and deploying seamless enterprise-wide information technology systems. The Deputy Program Executive Office stated that one of the goals for the department would be to determine the extent of integration needed across all of DON's business systems (includes both GCSS-MC and Navy ERP).



Results
Federated BEA Compliance

DOD Has Not Adequately Demonstrated that Key Programs Comply with the Federated BEA

The GCSS-MC and Navy ERP programs were assessed for compliance with the BEA and, based on each program's assertion of compliance, were certified by an IRB and approved by the DBMSC as compliant. These assessments largely followed DOD's compliance guidance and used its compliance tool (ACART). However, the assessments

- did not include all relevant architecture products,
- did not examine duplication across programs,
- did not address compliance against DON's enterprise architecture, and
- were not subject to oversight or validation.



Results
Federated BEA Compliance

Key reasons for this included compliance policy, guidance, and tool limitations. In addition, officials told us that the DON architecture was not yet sufficiently developed to support validations of program compliance assessments. As a result, the DOD does not have a sufficient basis for knowing if programs, like GCSS-MC and Navy ERP have been defined to optimize DOD and DON business operations.



Results
Federated BEA Compliance

Compliance Assessments Did Not Include All Relevant Architecture Products

The GCSS-MC and Navy ERP BEA compliance assessments addressed compliance with some key BEA products, such as those that describe business rules and standard data elements,²⁰ but they did not address compliance with other key BEA products, such as those that describe technical and system standards. GCSS-MC and Navy ERP did not do this because DOD guidance does not provide for doing so and, according to BTA officials, because some BEA products (e.g., technical standards profile) are not sufficiently defined. According to these officials, BTA plans to continue to define these products as the BEA evolves.

²⁰For example, if the program selects a business process to which the business rule “War Reserve Material Policy” applies, the program must assess whether the system enforces or will enforce this business rule as part of its functionality. As another example, if the program exchanges information related to asset inventories, it must determine if the system’s definition of the data entity “equipment” conforms to the corresponding BEA definition for the same data entity.



Results Federated BEA Compliance

Technical Products Were Not Included

- Neither of the programs assessed compliance with the BEA's technical standards profile, which outlines for example, standards governing how systems physically communicate with other systems and how they secure data from unauthorized access. This is particularly important because systems that need to share information with other systems need to employ common standards to accomplish this effectively and efficiently. A case in point is the GCSS-MC and the Navy Enterprise Resource Planning (ERP) programs.
- Navy ERP has identified 25 technical standards in its program-level technical standards profile, or TV-1, that are not identified in the BEA, and GCSS-MC has identified 13. For example, the programs have identified standards related to networking protocols and information security that are not included in the BEA. Such differences could limit information sharing between these and other programs. For example,
 - Navy ERP has identified the Simple Object Access Protocol (SOAP) 1.1,²¹ which is a key standard for facilitating data sharing, but GCSS-MC has not. Other

²¹SOAP describes a standard method for exchanging XML-based information. XML describes a standard method for sharing structured data, such as data contained in documents, across different information systems--particularly via the Internet.



Results Federated BEA Compliance

programs that need information or services from Navy ERP or that provide information to Navy ERP will also need to use SOAP to exchange requests.²² By not specifying SOAP as the messaging protocol, the programs could experience interoperability problems that may require investment in middleware to ensure the programs can successfully communicate.

- Areas of noncompliance with technical standards may indicate the need for the BEA technical standards profile to be expanded, or they may indicate the need for the programs to refrain from employing a given standard that the department does not intend to support. Regardless, because compliance with the BEA technical standards profile was not assessed, such needs have not been identified and therefore cannot be assessed.

²²If the other programs use some other middleware, such as CORBA, MQSeries, Java Messaging Service, Remote Method Invocation, etc., then additional software will be needed to handle the SOAP messages.



Results Federated BEA Compliance

System Products Were Not Included

- Neither of the programs assessed compliance with the BEA products that describe system characteristics. This is important because creating a body of information about programs permits identification of common system components and services that could potentially be shared by the programs, thus avoiding wasteful duplication.
- Both GCSS-MC and Navy ERP program documentation cite system functions associated with receiving goods, taking physical inventories, and returning goods. However, because compliance with the BEA system products (e.g., the Operational Activities to Systems Functions Traceability Matrix) was not assessed, it is not known to what extent these functions are common to both programs, potentially duplicative, and thus candidates for services to be shared by both.
- Neither program assessed compliance with the BEA products describing data exchanges between systems. As we previously reported, establishing and using standard system interfaces is a critical enabler to sharing data.²³
 - Both GCSS-MC and Navy ERP are to exchange order and status data with other

²³ [GAO-08-705](#).



Results Federated BEA Compliance

systems. System interfaces, which are defined in DODAF's SV-6 products, are important for understanding how information is to be exchanged between systems. However, neither program was assessed for compliance with these products. In the case of GCSS-MC, its SV-6 was not fully developed.

Compliance Assessments Did Not Examine Duplication Across Programs

None of the programs' compliance assessments were used to identify and compare potential areas of duplication across programs, which DOD has stated as a goal of its BEA and associated investment review and decisionmaking processes. This is because the compliance guidance does not provide for such analyses to be conducted and programs have not been granted access rights to use this functionality. As a result, these programs may be investing in duplicative functionality. For example:

- GCSS-MC and Navy ERP support at least 11 of the same operational activities (e.g., "manage property and materiel" and "perform asset accountability") and at least 31 of the same business processes (e.g. processes associated with assigning and generating unique asset identifiers and verifying that asset information is correct). Each of these are potentially duplicative and wasteful.



Results Federated BEA Compliance

- Six of these 11 common operational activities are also intended to be addressed by two Air Force programs (Defense Enterprise Accounting and Management System - Air Force and the Air Force Expeditionary Combat Support System).²⁴ Moreover, 3 of these 4 programs²⁵ share 18 operational activities. Given that the federated BEA is intended to identify and avoid not only duplications within DOD components, but also between DOD components, it is important that such commonality be addressed. Examples of shared activities include conduct physical inventory, deliver property and forces, perform budgeting, and manage receipt and acceptance.

²⁴We currently have work underway to evaluate these Air Force programs, which are in early stages of development.

²⁵The four programs are Navy ERP, GCSS-MC, Defense Enterprise Accounting and Management System-Air Force, and the Air Force Expeditionary Combat Support System.



Compliance Assessments Did Not Address Compliance with the DON Enterprise Architecture

Neither of the programs assessed compliance against the DON enterprise architecture, which is one of the biggest members of the federated BEA. This is particularly important given that DOD's approach to fully satisfying the architecture requirements of the fiscal year 2005 NDAA is to develop and use a federated architecture in which component architectures are to provide the additional business system data and technical content needed to supplement the thin layer of corporate policies, rules, and standards included in the corporate BEA.

- As we have recently reported,²⁶ the DON enterprise architecture is not mature because, among other things, it is missing a sufficient description of its current and future environments in terms of business and information/data. However, certain aspects of an architecture nevertheless exist and, according to department officials, these aspects will be leveraged in its efforts to develop a complete enterprise architecture. For example, the FORCEnet architecture documents Navy's technical infrastructure. Therefore, opportunities exist to assess programs in relation to these architecture products, and to understand where its programs are exposed to risks

²⁶[GAO-08-519](#).



Results
Federated BEA Compliance

because products do not exist, are not mature, or at odds with other programs.

According to DOD officials, compliance with the DON architecture was not assessed because DOD compliance policy is limited to the corporate BEA compliance, and because the DON enterprise architecture has yet to be sufficiently developed.



Results
Federated BEA Compliance

Compliance Assessments/Assertions Were Not Subject to Oversight or Validation

None of the programs' BEA compliance assessments or assertions were validated by either DOD or DON investment oversight and decisionmaking authorities for a range of reasons.

- Neither the DOD IRBs, the DBSMC, nor the BTA reviewed the programs' assessments and assertions. According to BTA officials, under DOD's tiered approach to investment accountability, the DBSMC, IRBs, and BTA are not responsible for doing so. Rather, this is a responsibility of DOD components.
- The DON Office of the CIO, which is responsible for pre-certifying investments as compliant before they are reviewed by the IRBs, did not evaluate any of the programs' compliance assessments or assertions. According to CIO officials, they rely on Functional Area Managers (FAMs) to validate a program's BEA assessments and assertions. However, no DON policy or guidance exists that describes how FAMs should conduct such validations. Moreover, according to the Navy's logistics FAM, who oversees Navy ERP, no FAM-level guidance has been developed for validating BEA compliance reviews. Instead, the logistics FAM process only provides for determining whether a BEA compliance assessment has been completed. According to CIO officials, this is because these authorities do not have the



Results Federated BEA Compliance

resources that they need to validate the assessments and because the DON enterprise architecture is not yet sufficiently developed. In addition, guidance does not exist that specifies how an assessment should be validated.

- Any validation of program assessments and assertions would be complicated by the absence of information captured in the assessment tool about what program documentation or other source materials were used by the program offices in making their compliance determinations. Specifically, the tool is only configured, and thus was only used, to capture the results of a program's comparison of program architecture products to BEA products. It was not used to capture the program products used in making these determinations.
- In addition, the programs did not develop the program-level architecture products that are needed to support and validate their respective compliance assessments and assertions. For example, GCSS-MC did not develop a program level OV-3, which describes information exchanges between operational activities. According to the compliance guidance, program-level architecture products, such as those defining information exchanges (OV-3) and system data requirements



Results
Federated BEA Compliance

(OV-7) are not required to be used until after the system has been deployed. This is too late to avoid costly rework to address areas of noncompliance, and is not consistent with DOD guidance,²⁷ which states that program-level architecture products that describe important information, such as information exchanges, should be developed before a program begins system development.

²⁷Department of Defense, *Business Transformation Guidance*. Version 1.1. (July 2007).



Conclusions

A demonstrated ability to repeatedly ensure that DOD's business system investments are defined and implemented within the context of the department's federated BEA is a legislative requirement and a prerequisite for removal of DOD's business system modernization program from our high-risk list. To its credit, DOD has recently taken steps aimed at demonstrating that its business systems comply with its BEA, including issuing compliance assessment guidance, providing a compliance assessment tool, and making the compliance assessment results part of a program's IRB certification and DBSMC approval. Nevertheless, the extent to which the two key programs comply with the federated BEA was not adequately demonstrated. Moreover, the compliance assertions provided by these programs were not subject to oversight by either DOD or DON program investment decision making authorities. This situation can be attributed to limitations in existing BEA compliance-related policy and guidance, the supporting compliance assessment tool, and the federated BEA, as well as the absence of DON compliance guidance. Accordingly, these and other DOD programs are at increased risk of being defined and implemented in a way that does not sufficiently ensure interoperability and avoid duplication and overlap, which are both goals of the BEA and related investment management approach. Unless this changes, the department's business system modernization efforts will likely remain a high-risk endeavor.



Recommendations for Executive Action

To adequately ensure that DOD business system investments are defined and implemented within the context of its federated BEA, we recommend that the Secretary of Defense direct the responsible authorities in the department to:

- Revise the DOD BEA compliance assessment guidance to (1) include assessment of all relevant operational, technical, and system architecture products, and (2) provide for the development and use of key program architecture products in conducting the assessment early enough in the program's life cycle to permit the results of the assessments to have a timely impact on the program's definition, design, and implementation.
- Use the program-specific data in the compliance assessment tool for identifying and analyzing potential overlap and duplication, and thus opportunities for reuse and consolidation among programs, and provide programs access rights to use this functionality.
- Amend relevant DOD policy to explicitly require business system program compliance with the federated BEA, to include both the corporate BEA and the component enterprise architectures, as a condition for program certification and approval.



Recommendations for Executive Action

- Amend relevant DOD policy to explicitly assign responsibility for validating program BEA compliance assertions to military departments and defense agencies, and issue guidance that describes the nature, scope, and methodology for doing so.



Appendix I: Objective, Scope, and Methodology

As requested, the objective of our review was to determine whether key Navy programs comply with the Department of Defense's federated Business Enterprise Architecture (BEA). To accomplish this objective, we focused on two Department of Navy systems—Navy Enterprise Resource Planning (ERP) and Global Combat Support System-Marine Corps (GCSS-MC)—because they involve relatively large amounts of modernization funding; are reviewed, certified, and approved by different investment review bodies and the Defense Business Systems Management Committee (DBSMC) according to the requirements of the Fiscal Year 2005 Ronald W. Reagan National Defense Authorization Act; and are at different acquisition life cycle stages.²⁸ In doing so, we

- Analyzed GCSS-MC and Navy ERP's BEA compliance assessments and system architecture products as well as versions 4.0, 4.1, and 5.0 of the BEA and compared them to the architecture compliance requirements of the Fiscal Year 2005 Ronald W.

²⁸The scope of our review also included the Navy Cash program. However, we have not included Navy Cash in our findings because our work showed that the business activities that it supports are neither reflected in the BEA nor planned by BTA officials to be reflected in the BEA. Therefore, Navy Cash was certified and approved on the basis that it does not conflict with the BEA. According to DOD, Navy Cash is intended to create workload efficiencies and improve the quality of life for sailors and marines through modern business practices and smart card technology, including a cashless environment on ships. Navy has estimated the program's total life cycle cost to be about \$223 million through fiscal year 2015.



Appendix I: Objective, Scope, and Methodology (cont.)

Reagan National Defense Authorization Act (NDAA) and BEA compliance guidance to determine the extent to which the compliance assessments addressed all relevant BEA products.

- Reviewed documentation from the GCSS-MC and Navy ERP programs, as well as the Air Force's Defense Enterprise Accounting and Management System and Air Force Expeditionary Combat Support System programs, such as the BEA compliance assessments, and compared the documentation obtained to identify potential redundancies or opportunities for reuse and determine if the BEA compliance assessments examined duplication across programs and if the tool that supports these assessments is being used to identify such duplication.
- Interviewed Department of Navy Office of the Chief Information Officer and program officials and reviewed recent GAO reports to determine the extent to which the programs were assessed for compliance against the Department of Navy enterprise architecture.
- Interviewed program officials and officials from the Business Transformation Agency and the Department of the Navy, including the logistics Functional Area Manager, and obtained guidance documentation and analyses from these officials to determine



Appendix I: Objective, Scope, and Methodology (cont.)

the extent to which the compliance assessments were subject to oversight or validation.

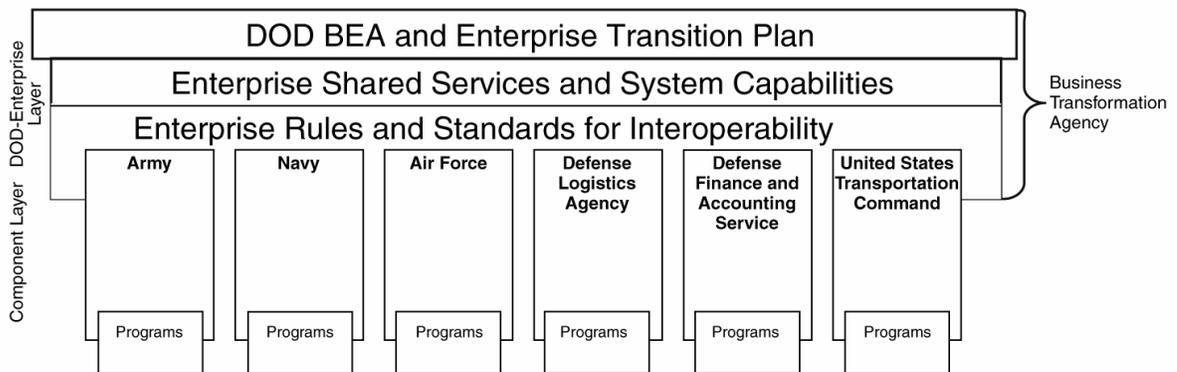
We conducted this performance audit at DON and DOD offices and contractor facilities in the Washington, D.C. metropolitan area, Annapolis, Maryland, and Triangle, Virginia between June 2007 and May 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.



Appendix II
DOD's Federated BEA

The Department of Defense's (DOD) federated Business Enterprise Architecture (BEA) consists of a family of coherent but distinct member architectures in which subsidiary architectures at the component and program levels conform to an overarching corporate architectural view and rule set. Each subsidiary architecture has unique goals and needs as well as common roles and responsibilities with the levels above and below it. These more specific architectures are substantially autonomous but inherit certain rules, policies, procedures, and services from higher-level architectures (see fig. 1).

Figure 1: Simplified Diagram of DOD's Federated BEA



Source: GAO analysis of DOD data.



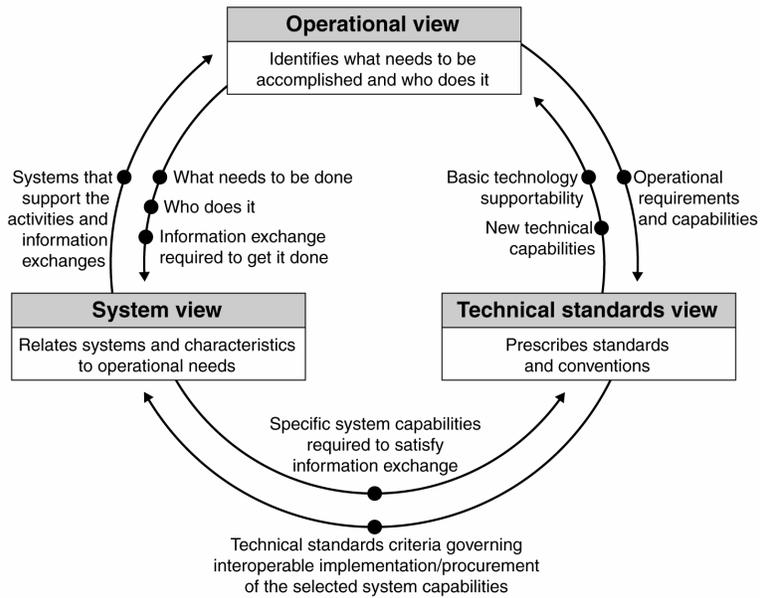
Appendix III
Descriptions of BEA Products

As described in this report, the Department of Defense’s (DOD) corporate Business Enterprise Architecture (BEA) was developed according to the DOD Architecture Framework (DODAF),²⁹ which specifies a set of three “views”—operational, systems, and technical. Figure 1 provides an overview of the DODAF product types and their relationships. Table 1 describes these products as they apply to the BEA.

²⁹DODAF is DOD’s guide for developing architectures. See for example Department of Defense, *Department of Defense Architecture Framework, Version 1.5, Volume 1* (April 2007).



Figure 1: Overview of DODAF Product Types and Their Relationships



Source: DOD.



Appendix III
Descriptions of BEA Products (cont.)

Table 1: BEA Products

View	Product	Description
Operational	OV-1	High-level graphical/textual description of what the architecture is supposed to do, and how it is supposed to do it.
	OV-2	Graphic depiction of the operational nodes (or organizations) with needlines that indicate a need to exchange information.
	OV-3	Information exchanged between nodes and the relevant attributes of that exchange.
	OV-5	Operational activities (or tasks) that are normally conducted in the course of achieving a mission or a business goal, input and output flows between activities.
	OV-6a	Business rules that constrain operations.
	OV-6c	Identified actions in a scenario or sequence of events.
	OV-7	System data requirements and business process rules of the operational view.
System	SV-1	Systems nodes, systems, and their interconnections, within and between nodes.
	SV-5	Relationships between the operational activities and the system functions.
	SV-6	Characteristics of the system data exchanged between systems.
Technical	TV-1	Standards that apply to systems view elements.

Source: GAO, based on data from the Business Transformation Agency.

Appendix II: Comments from the Department of Defense



ACQUISITION
TECHNOLOGY
AND LOGISTICS

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

AUG 01 2008

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

Dear Mr. Hite:

This is the Department of Defense (DoD) response to the GAO draft report GAO-08-972, "DOD BUSINESS SYSTEMS MODERNIZATION: Key Navy Programs' Compliance With DOD's Federated Business Enterprise Architecture Needs to Be Adequately Demonstrated," dated July 3, 2008 (GAO Code 310663). Detailed comments on the report recommendations are enclosed.

DoD concurred with all of the GAO's report recommendations. As the Business Enterprise Architecture (BEA) and Component architectures mature, and federation efforts progress, the Department will meet the intent of the GAO's recommendations in future versions of its compliance guidance, policies, and methodologies.

We appreciate the GAO's input on the Department's progress with its business transformation efforts and continue to value our partnership.

Sincerely,

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

Enclosure:
As stated



GAO DRAFT REPORT DATED JULY 3, 2008
GAO-08-972 (GAO CODE 310663)

“DOD BUSINESS SYSTEMS MODERNIZATION: KEY NAVY PROGRAMS’
COMPLIANCE WITH DOD’S FEDERATED BUSINESS ENTERPRISE
ARCHITECTURE NEEDS TO BE ADEQUATELY DEMONSTRATED”

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the responsible authorities in the department to revise the DoD Business Enterprise Architecture (BEA) compliance assessment to: (1) include assessment of all relevant operational, technical, and system architecture products, and (2) provide for the development and use of key program architecture products in conducting the assessment early enough in the program’s life cycle to permit the results of the assessments to have a timely impact on the program’s definition, design, and implementation. (Page 6/GAO Draft Report)

DOD RESPONSE: Concur. Development and use of Architecture is a continuing educational process. The DoD BEA is a collaborative effort with the Pre-Certifying Authorities (PCAs) who are fully aware of its purpose as the Department’s “TO-BE” business systems blue print.

1) We are currently working on developing the target compliance assertion criteria “of all relevant operational, technical, and system architecture products.” The assertion criteria will consist of key elements from the operational, technical, and system view products. The BEA Compliance Guidance states “Systems requesting certification should use the information contained in the specified BEA Department of Defense Architecture Framework (DoDAF) products to conduct their BEA compliance assessments. However, it is the architecture-related information (BEA Objects) contained in these products, and not the products themselves, which are most important for assessing a system’s compliance with the BEA.” This is consistent with DoDAF 2.0 focus on the data within the architecture products and not necessarily the products themselves.

2) DoD Guidance explicitly mandates development of architecture products for system development. Furthermore, the BEA Compliance Guidance states “PCAs are expected to assess their systems against the BEA, their Component architectures, and “other” Component architectures that serve to fill BEA gaps during investment reviews.” Consequently, the BEA Compliance adheres to this recommendation.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the responsible authorities in the department to: use the program-specific data in the

Attachment
Page 1 of 2

compliance assessment tool for identifying and analyzing potential overlap and duplication, and thus opportunities for reuse and consolidation among programs, and provide programs access rights to use this functionality.

DOD RESPONSE: Concur. The Architecture Compliance and Requirements Traceability (ACART) tool was developed and made available as a service to be shared by the entire Business Mission Area (BMA). One of the current capabilities of the ACART tool is the ability for a portfolio manager (e.g. PCA) to compare compliance assessment profiles of systems within their portfolio. Future plans include use of ACART and complementary services under the Integrated Management Information Environment (IMIE) to become standards for each of the Investment Review Boards (IRBs).

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the responsible authorities in the department to amend relevant DoD policy to explicitly require business system program compliance with the federated BEA, to include both the corporate BEA and the component enterprise architectures, as a condition for program certification and approval. (Page 6/GAO Draft Report)

DOD RESPONSE: Concur. The BEA Compliance Guidance reflects the Department's future intent to revise DoD policy governing certification requirements to explicitly include program compliance with its respective Component architecture. Specifically, the guidance states that "Pre-certification Authorities (PCAs) are expected to assess their systems against the BEA, their Component architectures, and 'other' Component architectures that serve to fill BEA gaps during investment reviews" (Page 2, *Business Enterprise Architecture (BEA) Compliance Guidance: BEA 5.0*, May 2008). The Department will continue to progress with its federation efforts, to include further definition of architecture federation rules, and will make the necessary revisions to DoD policy when practicable.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the responsible authorities in the department to amend relevant DoD policy to explicitly assign responsibility for validating program BEA compliance assertions to military departments and defense agencies, and issue guidance that describes the nature, scope, and methodology for doing so. (Page 7/GAO Draft Report)

DOD RESPONSE: Concur. DOD has specific structures and controls in place to assess program compliance to the BEA. Specifically, current guidance states that the Pre-Certification Authority (PCA) is responsible for the internal Component evaluations of systems in the investment governance process. This evaluation includes verification that a given system is in compliance with the DoD BEA. The PCA must assert via letter (i.e., "PCA Memo"), that the system is in compliance with the BEA as a part of the standard Investment Review Board Certification Package. Additional guidance may be issued in the future, and will be considered on an as needed basis.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Neela Lakhmani (Assistant Director), Nabajyoti Barkakati, Neil Doherty, Nancy Glover, Emily Longcore, Michael Holland, Anh Le, Josh Leiling, Lee McCracken, and Sushmita Srikanth made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

E-mail: fraudnet@gao.gov

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

Congressional Relations

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