United States Government Accountability Office

GAO

Report to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

August 2004

HOMELAND SECURITY

Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains

GAO-04-777

August 2004

HOMELAND SECURITY

Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-777, a report to Chairman, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives .

Why GAO Did This Study

The Department of Homeland Security (DHS) is attempting to integrate 22 federal agencies, each specializing in one or more interrelated aspects of homeland security. An enterprise architecture is a key tool for effectively and efficiently accomplishing this. In September 2003, DHS issued an initial version of its architecture. Since 2002, the Office of Management and Budget (OMB) has issued various components of the Federal Enterprise Architecture (FEA), which is intended to be, among other things, a framework for informing the content of agencies' enterprise architectures. GAO was asked to determine whether the initial version of DHS's architecture (1) provides a foundation upon which to build and (2) is aligned with the FEA.

What GAO Recommends

GAO is making recommendations to the Secretary of Homeland Security aimed at improving the department's architecture content and development approach. GAO is also making a recommendation to the Director of OMB to clarify the expected relationship between agencies' enterprise architectures and the FEA. In comments on this report, DHS stated that it was not realistic for the initial version of its architecture to satisfy all of the key elements recommended by GAO, but that future versions would do so. OMB stated that it would address the FEA and agency architecture relationship issues that GAO reported.

www.gao.gov/cgi-bin/getrpt?GAO-04-777.

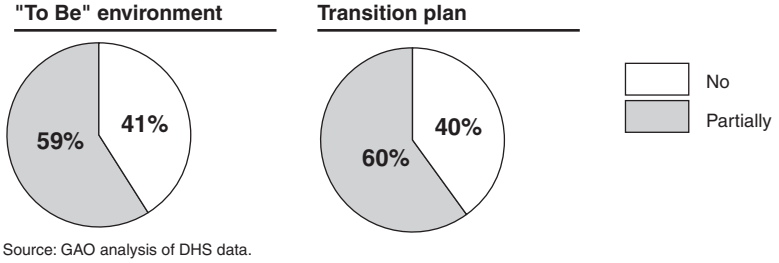
To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

DHS's initial enterprise architecture provides a partial foundation upon which to build future versions. However, it is missing, either in part or in total, all of the key elements expected to be found in a well-defined architecture, such as descriptions of business processes, information flows among these processes, and security rules associated with these information flows, to name just a few (see figure below for a summary of key elements present). Moreover, the key elements that are at least partially present in the initial version were not derived in a manner consistent with best practices for architecture development. Instead, they are based on assumptions about a DHS or national corporate business strategy and, according to DHS, are largely the products of combining the existing architectures of several of the department's predecessor agencies, along with their respective portfolios of system investment projects. DHS officials agreed that their initial version is lacking key elements, and they stated that this version represents what could be done in the absence of a strategic plan, with limited resources, and in the 4 months that were available to meet an OMB deadline for submitting the department's fiscal year 2004 information technology budget request. In addition, they stated that the next version of the architecture, which is to be issued in September 2004, would have much more content. As a result, DHS does not yet have the necessary architectural blueprint to effectively guide and constrain its ongoing business transformation efforts and the hundreds of millions of dollars that it is investing in supporting information technology assets. Without this, DHS runs the risk that its efforts and investments will not be well integrated, will be duplicative, will be unnecessarily costly to maintain and interface, and will not optimize overall mission performance.

The department's initial enterprise architecture can be traced semantically with the FEA, which means that similar terms and/or definitions of terms can be found in the respective architectures. However, traceability in terms of architecture structures and functions is not apparent. Because of this, it is not clear whether the substance and intent of the respective architectures are in fact aligned, meaning that, if both were implemented, they would produce similar outcomes. This is due at least in part to the fact that OMB has yet to clearly define what it expects the relationship between agencies' enterprise architectures and the FEA to be, including what it means by architectural alignment.

Summary of Extent to Which Version 1.0 Satisfies Key Elements Governing Architectural Content



Source: GAO analysis of DHS data.

Contents

Letter

1

Results in Brief 2
Background 5
Initial Version of DHS's Architecture Provides a Partial Foundation upon Which to Build, but Not a Sufficient Basis to Guide Investment Decisions 23
Initial Architecture Can Be Partially Traced to the Federal Enterprise Architecture, but the Extent of Alignment Is Unclear 34
Conclusions 36
Recommendations for Executive Action 37
Agency Comments and Our Evaluation 38

Appendixes

Appendix I: Objectives, Scope, and Methodology 42

Appendix II: Detailed Results of GAO's Analyses of Version 1.0 of DHS's "To Be" Architecture 45

Appendix III: Detailed Results of GAO's Analyses of Version 1.0 of DHS's Transition Plan 58

Appendix IV: Comments from the Department of Homeland Security 61
GAO Comments 81

Appendix V: GAO Contact and Staff Acknowledgments 85
GAO Contact 85
Staff Acknowledgments 85

Tables

Table 1: Overview of Key DHS Component Organizations' Roles 8
Table 2: Summary of Key Architecture Entities and Individuals and Their Responsibilities 9
Table 3: GAO's Framework for Enterprise Architecture Management Maturity 14
Table 4: Service Domains, the Capabilities That They Describe, and Associated Service Types 19

Figures

Figure 1: Simplified Diagram of DHS Organizational Structure 7
Figure 2: Summary of Extent to Which Version 1.0 Satisfies Key Elements Governing Architectural Content 26

Abbreviations

CIO	chief information officer
CURE	create, update, reference, and eliminate
DHS	Department of Homeland Security
DOD	Department of Defense
EAI	enterprise application integration
FEA	Federal Enterprise Architecture
GIG	Global Information Grid
IT	information technology
OMB	Office of Management and Budget
TRM	technical reference model

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

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

August 6, 2004

The Honorable Adam H. Putnam
Chairman, Subcommittee on Technology, Information
Policy, Intergovernmental Relations and
the Census
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

Following September 11, 2001, homeland security emerged as a more prominent federal mission. To improve the federal government's ability to fulfill this mission, Congress passed and the President signed the Homeland Security Act of 2002. Among other things, this act created the Department of Homeland Security (DHS) by merging 22 separate agencies, each specializing in one or more interrelated and interdependent aspects of homeland security, such as intelligence analysis, law enforcement, border security, transportation security, biological research, critical infrastructure protection, and disaster recovery. The effective interaction, integration, and synergy of these agencies are critical to homeland security mission performance.

Because of the importance of the department's mission operations and the enormity of the challenges associated with creating the federal government's third largest department, we designated the implementation and transformation of DHS as a high-risk area in January 2003.[1] We also reported in June 2002 that DHS needed to, among other things, develop and implement an enterprise architecture to aid in optimizing departmentwide operations and its supporting systems environments.[2] As we have

[1]U.S. General Accounting Office, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003) and *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).

[2]An enterprise architecture is a blueprint that defines, both in logical terms (including interrelated business processes and business rules, integrated functions, applications, systems, users, work locations, and information needs and flows) and in technical terms (including hardware, software, data, communications, and security), how an organization's information technology systems operate today, how they are to operate in the future, and a road map for the transition.

repeatedly reported,[3] a well-defined enterprise architecture is essential to an organization's ability to transform its operations and supporting systems in a way that eliminates duplication, promotes interoperability, reduces costs, and optimizes mission performance.

Recognizing the pivotal role that an architecture will play in successfully merging the diverse operating and systems environments that the department inherited, DHS issued an initial version in September 2003. The department also stated its intention to improve on this initial version and issue a second version in September 2004. You requested that we determine whether the initial version of the architecture (1) provides a foundation upon which to build and (2) is aligned with the Office of Management and Budget's (OMB) Federal Enterprise Architecture (FEA).[4] We performed our work in accordance with generally accepted government auditing standards. Details on our objectives, scope, and methodology are in appendix I.

Results in Brief

The department's initial enterprise architecture provides a partial basis upon which to build future versions. However, it is missing most of the content necessary to be considered a well-defined architecture. Moreover, the content in this version was not systematically derived from a DHS or a national corporate business strategy; rather, it was more the result of an amalgamation of the existing architectures that several of DHS's predecessor agencies already had, along with their respective portfolios of system investment projects. Such a development approach is not consistent with recognized architecture development best practices. DHS officials agreed with our content assessment of their initial architecture,

[3]See, for example, U.S. General Accounting Office, *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, GAO-04-43 (Washington, D.C.: Nov. 21, 2003); *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, GAO-03-1018 (Washington, D.C.: Sept. 19, 2003); *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*, AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

[4]The Federal Enterprise Architecture (FEA) is a collection of five "reference models" developed by the Office of Management and Budget, which are intended to provide a governmentwide framework to guide and constrain federal agencies' enterprise architectures and information technology investments.

stating that it is largely a reflection of what could be done without a strategic plan to drive architectural content and with limited resources and time. They also stated that the primary purposes in developing this version were to meet an OMB deadline for submitting the department's fiscal year 2004 information technology (IT) budget request and to mature the department's understanding of enterprise architecture and its ability to execute an approach and methodology for developing and using the next version of the architecture. Regardless, the fact remains that DHS does not yet have the architectural content that it needs to effectively guide and constrain its business transformation efforts and the hundreds of millions of dollars it is investing in supporting systems. Without such content, DHS runs the risk that its investments will not be well integrated, will be duplicative, will be unnecessarily costly to maintain and interface, and will not effectively optimize mission performance. To their credit, the department's chief information officer and senior architecture officials recognize the architecture's limitations and are in the process of developing a new version.

DHS's initial enterprise architecture can be aligned semantically with the FEA,[5] that is, similar terms and/or definitions of terms can be found in the respective architectures. However, alignment in terms of architecture structures and functions is not apparent. Because of this, it is not clear whether the substance and intent of each has the same meaning and would produce similar outcomes if implemented. This is at least in part due to the fact that OMB has yet to clearly define what it expects the relationship to be between agencies' enterprise architectures and the FEA, including what OMB means by the term architectural alignment.

To assist DHS in developing a well-defined enterprise architecture, we are recommending 41 actions aimed at having DHS's architecture executive steering committee provide the resources necessary to add needed architecture content and ensure that architecture development best practices are employed. In addition, to assist DHS and other agencies in developing and evolving their respective architectures, we are making a recommendation to OMB to clarify the expected relationship between the FEA and federal agencies' architectures.

[5]For purposes of this review, we mapped the department's architecture to the FEA's business, services, and technical reference models.

In written comments on a draft of our report that was signed by the Director, Bankcard Programs and GAO/OIG Liaison within the Office of the Chief Financial Officer, DHS stated that it took exception to several aspects of our report, including the appropriateness and prior disclosure of the criteria that we used to evaluate the initial version of its architecture and to the premature nature of our recommendations, given the limited scope and intent of this initial version. Nevertheless, DHS agreed with our position that much work remains to develop an architecture that can support business and IT transformation. Moreover, despite taking exception to the criteria and our recommendations, the department also stated that it would ensure that the criteria we used to evaluate the initial version, which we reference in our recommendations, are addressed to the extent possible in the next version of its architecture. While we do not agree with DHS's view of the criteria we used and the recommendations we made—for reasons discussed later in this report—or with other comments that DHS provided stating that some of our facts about the content of the initial version are not correct, we do agree with the department's decision to address our recommendations incrementally. As we have long held and reported, enterprise architecture development should be incremental, with each version of the architecture adding more depth and detail to an enterprisewide, business-driven foundation. Accordingly, the intent of our recommendations is to provide DHS with a constructive road map, grounded in explicit criteria, for incrementally developing a mission-derived blueprint for business and technology transformation.

In its oral comments on a draft of this report, OMB's Office of E-Government and Information Technology and Office of General Counsel stated that its continuing evolution of the FEA will clarify the FEA's relationship with agencies' architectures and will address issues raised in our report.

Background

The creation of DHS in November 2002[6] represents the most significant transformation of the U.S. government since 1947, when the various branches of the U.S. Armed Forces were combined into the Department of Defense (DOD) to better coordinate the nation's defense against military threats. In January 2003, we cited numerous management and leadership challenges facing DHS as it attempted to merge 22 separate federal agencies, and we designated the department's transformation as high risk.[7] Shortly thereafter, the department stated that it faced significant transformational challenges, such as (1) developing new business processes, (2) unifying multiple organizational structures, (3) integrating multiple border-security and interior-enforcement functions, (4) integrating information technology (application systems and infrastructures), and (5) improving information sharing. The magnitude of these challenges is enormous. For example, DHS reports that it has redundancies in such business processes as human resources management, financial management, and procurement—including about 300 application systems that support inconsistent and duplicative processes. DHS also reports that it plans to invest about $4.1 billion during fiscal year 2004 in IT for both new and existing systems, to more effectively and efficiently support its mission operations and business processes.

An enterprise architecture is a key tool for effectively and efficiently overcoming the kinds of transformational challenges that face DHS. In short, it is a business and technology blueprint that links an organization's strategic plan to the program and supporting system implementations that are needed to systematically move the organization from how it operates today to how it intends to operate tomorrow. As we have repeatedly reported,[8] without an enterprise architecture to guide and constrain IT investments, it is unlikely that an organization will be able to transform its

[6]Homeland Security Act of 2002 (Public Law 107-296, Nov. 25, 2002).

[7]GAO-03-119.

[8]See, for example, U.S. General Accounting Office, *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, GAO-04-43 (Washington, D.C.: Nov. 21, 2003); *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, GAO-03-1018 (Washington, D.C.: Sept. 19, 2003); *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*, AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

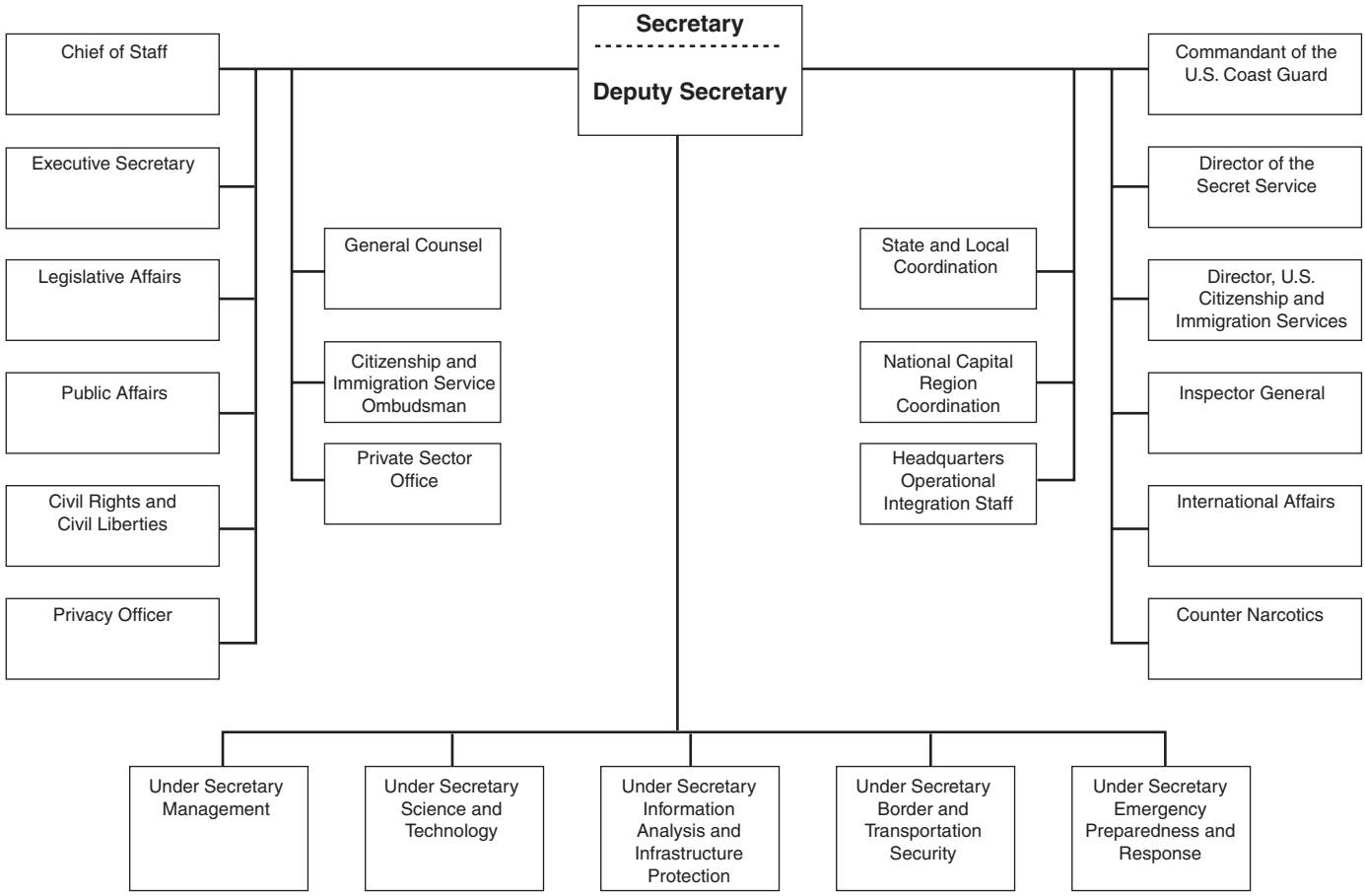
business processes and modernize its supporting systems in a way that minimizes overlap and duplication, and thus costs, and maximizes interoperability and mission performance.

DHS's Mission and Organizational Structure: A Brief Description

According to DHS's strategic plan, its mission is to lead a unified national effort to secure America by preventing and deterring terrorist attacks and protecting against and responding to threats and hazards to the nation. DHS also is to ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce. As part of its responsibilities, the department must also coordinate and facilitate the sharing of information both among its component agencies and with other federal agencies, state and local governments, the private sector, and other entities.

As illustrated in DHS's organizational structure (see fig. 1), to accomplish its mission it has five under secretaries with responsibility over the directorates or offices for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response. Each DHS directorate is responsible for leading its specific homeland security mission area and coordinating relevant efforts with other federal agencies and state and local governments. The department is also composed of other component organizations, such as the U.S. Coast Guard and the U.S. Secret Service. Table 1 describes the primary roles of these five directorates and several of these component organizations.

Figure 1: Simplified Diagram of DHS Organizational Structure



Source: DHS.

Table 1: Overview of Key DHS Component Organizations' Roles

Key organizations	Roles
Management	Manages budgets, appropriations, expenditure of funds, accounting and finance, procurement, human resources and personnel, information technology, facilities, property, and equipment in support of the other four directorates.
Science and technology	Organizes scientific and technological resources to prevent or mitigate the effects of catastrophic terrorism; unifies and coordinates efforts to develop and implement scientific and technological countermeasures; sponsors research and evaluates new vaccines, antidotes, diagnostics, and therapies against biological and chemical warfare agents.
Information analysis and infrastructure protection	Analyzes intelligence and information obtained from other agencies (including the Central Intelligence Agency, Federal Bureau of Investigation, and National Security Agency) involving threats to homeland security; evaluates vulnerabilities in the nation's infrastructure; and works with stakeholders to develop and implement an integrated national plan for the physical and cyberprotection of critical infrastructures and key assets.
Border and transportation security	Prevents the illegal entry of people or goods while facilitating the unimpeded flow of lawful commerce and people across our borders, secures our nation's transportation systems, and enforces immigration laws.
Emergency preparedness and response	Prepares for, mitigates the effects of, responds to, and recovers from major domestic disasters, both natural and man-made, including incidents of terrorism.
Coast Guard	Protects the public, the environment, and U.S. economic and security interests in international waters and America's coasts, ports, and inland waterways.
Secret Service	Protects the President and other government leaders, provides security for designated national events, and preserves the integrity of the nation's financial and critical infrastructures.
Citizenship and immigration services	Administers services, such as immigrant and nonimmigrant sponsorship, adjustment of status, work authorization and other permits, naturalization of qualified applicants for U.S. citizenship, and asylum or refugee processing.
Counter narcotics	Coordinates policy and operations within the department and between the department and other federal agencies with respect to illegal drug trafficking and its terrorist-related ramifications; facilitates the tracking and severing of connections between drug trafficking and terrorism.
State and local coordination	Facilitates and coordinates departmental programs that affect state, local, territorial, and tribal governments.
National capital region coordination	Oversees and coordinates federal programs and domestic preparedness initiatives for state, local, and regional authorities in the National Capital Region, including the District of Columbia, Maryland, and Virginia.

Source: DHS.

Within the Management directorate is the DHS Office of the Chief Information Officer (CIO), which has primary responsibility for addressing departmentwide information technology integration issues. According to the CIO, this office's responsibilities include developing and facilitating the implementation of such integration enablers as the department's IT strategic plan and its enterprise architecture. The CIO released an initial version of the enterprise architecture in September 2003 and plans to issue

the next version in September 2004. According to the CIO, updated releases of the architecture will be issued on an annual basis. To provide the necessary leadership, direction, and management to create the architecture, the CIO established various entities and assigned specific responsibilities to each. Table 2 describes the key architecture entities and individuals involved in developing and maintaining the architecture, along with their respective responsibilities.

Table 2: Summary of Key Architecture Entities and Individuals and Their Responsibilities

Entity/position	Responsibilities
Office of Planning and Enterprise Architecture	Manages the department's architecture program and is led by the chief architect, who oversees the development, verification, and adoption of the architecture. Reports to the department's CIO.
Enterprise architecture executive steering committee (also called the DHS Management Council)	Is accountable and responsible for the enterprise architecture. Makes decisions that affect the enterprise architecture and the associated program; determines projects' compliance with the architecture. Provides advice or guidance to the department's CIO. Composed of senior executives from technical and business organizations across the department (e.g., DHS CIO, Under Secretary for Border and Transportation Security, the Commandant of the Coast Guard, and the Director of the U.S. Secret Service).
Enterprise architecture core team	Trains users and core team members. Promotes and evaluates the architecture program. Collects and analyzes performance data on architecture activities. Provides consulting support to project personnel to help achieve compliance with the architecture.
Enterprise architecture configuration control board working group	Controls changes to architecture products and processes in accordance with configuration management principles. Establishes and oversees the processes for submitting, evaluating, and implementing change requests, and is directed by the chief architect.

Source: DHS.

Enterprise Architecture: A Brief Description

Effective use of enterprise architectures is a trademark of successful public and private organizations. For a decade, we have promoted the use of architectures to guide and constrain systems modernization, recognizing them as a crucial means to a challenging goal: establishing agency operational structures that are optimally defined in both business and technological environments. Congress, OMB, and the federal 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 IT architecture. This should provide the means for managing the integration of business processes and supporting systems. Further, the E-Government Act of 2002[9] requires OMB to oversee the development of enterprise architectures within and across agencies.

Generally speaking, an enterprise architecture connects an organization's strategic plan with program and system solution implementations by providing the fundamental information details needed to guide and constrain implementable investments in a consistent, coordinated, and integrated fashion. An enterprise architecture provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department) or a functional or mission area that cuts across more than one organization (e.g., homeland security). This picture consists of snapshots of both the enterprise's current or "As Is" operational and technological 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 further consist of "views," which are basically one or more architecture products that provide conceptual or logical representations of the enterprise.

The suite of products and their content that form a given entity's enterprise architecture are largely governed by the framework used to develop the architecture. Since the 1980s, various frameworks have emerged and been applied. For example, John Zachman developed a structure or framework for defining and capturing an architecture.[10] This framework provides for six windows from which to view the enterprise, which Zachman calls "perspectives" on how a given entity operates: the perspectives of (1) the

[9]E-Government Act of 2002, Public Law 107-347 (Dec. 17, 2002).

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

strategic planner, (2) the system user, (3) the system designer, (4) the system developer, (5) the subcontractor, and (6) the system itself. Zachman also proposed six abstractions or models that are associated with each of these perspectives: these models cover (1) how the entity operates, (2) what the entity uses to operate, (3) where the entity operates, (4) who operates the entity, (5) when entity operations occur, and (6) why the entity operates.

Other frameworks also exist. Each of these frameworks use somewhat unique nomenclatures to define themselves. However, they all generally provide for defining an enterprise's operations in both (1) logical terms, such as interrelated business processes and business rules, information needs and flows, and work locations and users and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. The frameworks also provide for defining these perspectives for both the enterprise's current or "As Is" environment and its target or "To Be" environment, as well as a transition plan for moving from the "As Is" to the "To Be" environment.

Our research and experience show that for major program investments, such as the development of an enterprise architecture, successful organizations approach product development in an incremental fashion, meaning that they initially develop a foundational product that is expanded and extended through a series of follow-on products that add more capability and value. In doing so, these organizations can effectively mitigate the enormous risk associated with trying to deliver a large and complex product that requires the execution of many activities over an extended period of time as a single monolithic product. In effect, this incremental approach permits a large undertaking to be broken into a series of smaller projects, or incremental versions, that can be better controlled to provide reasonable assurance that expectations are met.

The importance of developing, implementing, and maintaining an enterprise architecture is a basic tenet of both organizational transformation and IT management. Managed properly, an enterprise architecture can clarify and help to optimize the interdependencies and relationships among an organization's business operations and the underlying IT infrastructure and applications that support these operations. Employed in concert with other important management controls—such as portfolio-based capital planning and investment control practices—architectures can greatly increase the chances that an organization's operational and IT environments will be configured to optimize mission performance. Our experience with federal agencies has shown that investing in IT without defining these investments in the context of an architecture often results in systems that are duplicative, not well integrated, and unnecessarily costly to maintain and interface.[11]

Our Prior Work Has Emphasized the Need for a DHS Enterprise Architecture

For the last 2 years, we have promoted the development and use of a homeland security enterprise architecture. In June 2002, we testified[12] on the need to define the homeland security mission and the information, technologies, and approaches necessary to perform this mission in a way that is divorced from organizational parochialism and cultural differences. At that time, we stressed that a particularly critical function of a homeland security architecture would be to establish processes and information/data protocols and standards that could facilitate information collection and permit sharing.

[11] See, for example, U.S. General Accounting Office, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458 (Washington, D.C.: Feb. 28, 2003); *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

[12] U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 7, 2002).

In January 2003, when we designated DHS's transformation as high risk, we again emphasized the need to develop and implement an enterprise architecture. In May 2003 testimony,[13] we reiterated this need, stating that, for DHS to be successful in addressing threats of domestic terrorism, it would need to establish effective systems and processes to facilitate information sharing among and between government entities and the private sector. We stated that to accomplish this the department would need to develop and implement an enterprise architecture.

In August 2003,[14] we reported that DHS had begun to develop an enterprise architecture and that it planned to use this architecture to assist its efforts to integrate and share information between federal agencies and among federal agencies, state and city governments, and the private sector. In November 2003,[15] we reported on DHS's progress in establishing key enterprise architecture management capabilities, as described in our architecture management maturity framework.[16] This framework associates specific architecture management capabilities with five hierarchical stages of management maturity, starting with creating architecture awareness and followed by building the architecture management foundation, developing the architecture, completing the architecture, culminating in leveraging the architecture to manage change (see table 3 for a more detailed description of the stages).

[13]U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-715T (Washington, D.C.: May 8, 2003).

[14]U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: Aug. 27, 2003).

[15]U.S. General Accounting Office, *Information Technology: Leadership Remains Key to Agencies Making Progress on Enterprise Architecture Efforts*, GAO-04-40 (Washington, D.C.: Nov. 17, 2003).

[16]U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management* (Version 1.1), GAO-03-584G (Washington, D.C.: April 2003).

Table 3: GAO's Framework for Enterprise Architecture Management Maturity

Maturity stage	Description
Stage 1: Creating enterprise architecture awareness	Organization does not have plans to develop and use an architecture or it has plans that do not demonstrate an awareness of the value of having and using an architecture. While stage 1 agencies may have initiated some architecture activity, these agencies' efforts are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation that is necessary for successful architecture development.
Stage 2: Building the enterprise architecture management foundation	Organization recognizes that the architecture is a corporate asset by vesting accountability for it in an executive body that represents the entire enterprise. At this stage, an organization assigns architecture management roles and responsibilities and establishes plans for developing enterprise architecture products and for measuring program progress and product quality; it also commits the resources necessary for developing an architecture—people, processes, and tools.
Stage 3: Developing the enterprise architecture	Organization focuses on developing architecture products according to the selected framework, methodology, tool, and established management plans. Roles and responsibilities assigned in the previous stage are in place, and resources are being applied to develop actual enterprise architecture products. The scope of the architecture has been defined to encompass the entire enterprise, whether organization-based or function-based.
Stage 4: Completing the enterprise architecture	Organization has completed its enterprise architecture products, meaning that the products have been approved by the architecture steering committee or an investment review board and by the CIO. Further, an independent agent has assessed the quality (i.e., completeness and accuracy) of the architecture products. Additionally, evolution of the approved products is governed by a written architecture maintenance policy approved by the head of the organization.
Stage 5: Leveraging the enterprise architecture to manage change	Organization has secured senior leadership approval of the enterprise architecture products and a written institutional policy stating that IT investments must comply with the architecture unless they are granted an explicit compliance waiver. Further, decision makers are using the architecture to identify and address ongoing and proposed IT investments that are conflicting, overlapping, not strategically linked, or redundant. Also, the organization tracks and measures architecture benefits or return on investment, and adjustments are continuously made to both the architecture management process and the enterprise architecture products.

Source: GAO.

Based on information provided by DHS, we reported that the department had established an architecture management foundation and was developing architecture products, and we rated the department to be at stage 3 of our maturity framework. In particular, we reported that it had (1) established a program office responsible for developing and maintaining the architecture; (2) assigned a chief architect to oversee the program; (3) established plans for developing metrics for measuring progress, quality, compliance, and return on investment; and (4) placed the architecture products under configuration management. According to our framework, effective architecture management is generally not achieved until an enterprise has a completed and approved architecture that is being

effectively maintained and is being used to leverage organizational change and support investment decision making. An enterprise with these characteristics would need to satisfy all of the requirements associated with stage 3 of our framework, and many of the requirements of stages 4 and 5.

In addition, we reported in May 2004[17] that DHS was in the process of defining its strategic IT management framework for, among other things, integrating its current and future systems and aligning them with the department's strategic goals and mission. We also reported that a key component of this initiative was the development of the department's enterprise architecture. Accordingly, we recommended that, until the framework was completed, the department limit its spending on IT investments to cost-effective efforts that

- are congressionally directed;
- take advantage of near-term, relatively small, low-risk opportunities to leverage technology in satisfying a compelling homeland security need;
- support operations and maintenance of existing systems that are critical to DHS's mission;
- involve deploying an already developed and fully tested system; or
- support establishment of a DHS strategic IT management framework, including IT strategic planning, enterprise architecture, and investment management.

[17]U. S. General Accounting Office, *Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems*, GAO-04-509 (Washington, D.C.: May 21, 2004).

Prior DHS Testimony Has Recognized the Importance of an Enterprise Architecture for Departmental Transformation

In May 2003,[18] the department's CIO testified that development of the homeland security enterprise architecture had begun in July 2002 and that the department expected to complete the "As Is" and "To Be" architectures by June and August 2003, respectively. The CIO also stated that the department would develop a migration or transition strategy and plan by fall 2003 in order to achieve its target environment. Moreover, the CIO testified that DHS had coordinated its architecture development efforts with other key federal agencies (e.g., the Departments of Justice, Energy, and Defense), the intelligence community, and the National Association of State and Local CIOs.

In October 2003,[19] DHS's CIO testified that the department had completed the first version of its target architecture in September 2003 and was beginning to implement the objectives of its transition strategy. The CIO stated that the department had designed and delivered a comprehensive and immediately useful business-driven target architecture in under 4 months and that the architecture was enabling DHS to make IT investment decisions.

OMB's Federal Enterprise Architecture: A Brief Description

On February 6, 2002, OMB established the FEA Program Management Office and charged it with responsibility for developing the FEA. According to OMB, the FEA is intended to provide a governmentwide framework to guide and constrain federal agencies' enterprise architectures and IT investments and is now being used by agencies to help develop their budgets and to set strategic goals. The FEA is composed of five reference models: Performance, Business, Service, Data, and Technical. To date, versions of all but the data reference model have been released for use by the agencies. More information on each reference model follows.

Performance reference model. The performance reference model is intended to describe a set of performance measures for major IT initiatives

[18]Statement of Steven I. Cooper, Chief Information Officer, Department of Homeland Security, before the Committee on Government Reform, House of Representatives, May 8, 2003.

[19]Statement of Steven I. Cooper, Chief Information Officer, Department of Homeland Security, before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives, October 8, 2003.

and their contribution to program performance. According to OMB, this model will help agencies produce enhanced performance information; improve the alignment and better articulate the contribution of inputs, such as technology, to outputs and outcomes; and identify improvement opportunities that span traditional organizational boundaries. Version 1.0 of the model was released in September 2003.

Business reference model. The business reference model serves as the foundation for the FEA. It is intended to describe the federal government's businesses, independent of the agencies that perform them. The model consists of four business areas: (1) services for citizens, (2) mode of delivery, (3) support delivery of services, and (4) management of government resources.

Thirty-nine *lines of business*, which together are composed of 153 *subfunctions*, make up the four business areas. Examples of lines of business under the "services for citizens" business area are homeland security, law enforcement, and economic development. Each of these lines of business includes a number of subfunctions. For example, for the homeland security line of business, a subfunction is border and transportation security; for law enforcement, a subfunction is citizen protection; and for economic development, a subfunction is financial sector oversight.

Version 1.0 of the business reference model was released to agencies in July 2002, and OMB reports that it was used in the fiscal year 2004 budget process. According to OMB, Version 1.0 helped to reveal that many federal agencies were involved in each line of business and that agencies' proposed IT investments for fiscal year 2004 offered multibillion-dollar consolidation opportunities. In June 2003, OMB released Version 2.0 which, according to OMB, addresses comments from agencies and reflects changes to align the model as closely as possible with other governmentwide management frameworks (e.g., budget function codes[20]) and improvement initiatives (e.g., the President's Budget Performance Integration Initiative[21]) without compromising its intended purpose. OMB expects agencies to use the model, as part of their capital planning and investment control processes, to help identify opportunities to consolidate IT investments across the federal government.

Service component reference model. The service component reference model is intended to identify and classify IT service (i.e., application) components that support federal agencies and promote the reuse of components across agencies. According to OMB, this model is intended to provide the foundation for the reuse of applications, application capabilities, components (defined as "a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface"), and business services, and is organized as a hierarchy beginning with seven *service domains*, as shown in table 4.

[20]Budget function codes are used to describe the budget of the United States in terms of the major purpose served, such as national defense and international affairs. By grouping together functionally related items, regardless of the responsible agency, this classification enables Congress and the public to see what the government is doing or expects to do and, in general, focuses upon the ultimate purpose that the government programs are designed to solve.

[21]This initiative is intended to support budget decision making by providing more useful performance information (i.e., better information on how inputs are used to produce outputs, which affect outcomes).

Table 4: Service Domains, the Capabilities That They Describe, and Associated Service Types

Service domain	Description	Service types
Customer services	Interaction between the business and the customer and customer-driven activities or functions (directly related to the end customer)	Customer preferences, customer relationship management, and customer-initiated assistance
Process automation services	Automation of process and activities that support managing the business	Tracking and workflow, and routing and automation
Business management services	Management and execution of business functions and organizational activities that maintain continuity across the business and value chain participants	Management of process, organizational management, supply chain management, and investment management
Digital asset services	Generation, management, and distribution of intellectual capital and electronic media across the business and extended enterprise	Content management, knowledge management, document management, and records management
Business analytical services	Extraction, aggregation, and presentation of information to facilitate decision analysis and business evaluation	Analysis and statistics, business intelligence, visualization, and reporting
Back office services	Management of enterprise planning transactional-based functions	Data management, human resources, financial management, assets/materials management, development and integration, and human capital/workforce management
Support services	Cross-functional capabilities that can be leveraged independent of service domain objective and mission	Security management, systems management, forms, communications, collaboration, and search

Source: OMB.

These service domains are decomposed into 29 service types, which together are further broken down into 168 components. For example, the customer services domain is made up of 3 service types: customer relationship management, customer preferences, and customer-initiated assistance. Components of the customer relationship management service type include call center management and customer analytics; components of the customer preferences service type include personalization and subscriptions; and components of the customer-initiated assistance service type include online help and online tutorials.

Version 1.0 of the service component reference model was released in June 2003. According to OMB, the model is a business-driven, functional framework that classifies service components with respect to how they support business and/or performance objectives. Further, the model is structured across horizontal service areas that, independent of the business functions, is intended to provide a leverageable foundation for the

reuse of applications, application capabilities, components, and business services.

Data and information reference model. The data and information reference model is intended to describe the types of data and information that support program and business-line operations and the relationships among these types. The model is intended to help describe the types of interactions and information exchanges that occur between the government and its customers. OMB officials told us that the release of Version 1.0 is to occur imminently.

Technical reference model. The technical reference model is intended to describe the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of service components. OMB describes the model as being made up of the following four core service areas:

Service access and delivery: the collection of standards and specifications that support external access, exchange, and delivery of service components.

Service platform and infrastructure: the delivery platforms and infrastructure that support the construction, maintenance, and availability of a service component or capability.

Component framework: the underlying foundation, technologies, standards, and specifications by which service components are built, exchanged, and deployed.

Service interface and integration: the collection of technologies, methodologies, standards, and specifications that govern how agencies will interface internally and externally with a service component.

Each of these service areas is made up of *service categories*, which identify lower levels of technologies, standards, and specifications; *service standards*, which define the standards and technologies that support the service category; and the *service specification*, which details the standard specification or the provider of the specification. For example, within the first core service area (service access and delivery), an example of a service category is *access channels*, and examples of service standards are *Web browsers* and *wireless personal digital assistants*. Examples of

service specifications for the Web browser service standard are Internet Explorer and Netscape Navigator.

Version 1.0 of the technical reference model was released in January 2003, followed in August 2003 by Version 1.1, which reflected minor revisions that were based, in part, on agencies' comments. Version 1.1 was used during the 2005 budget process. The model is intended to help agencies define their target technical architectures.

In May 2004, we testified[22] that, through the FEA, OMB is attempting to provide federal agencies and other decision makers with a common frame of reference or taxonomy for informing agencies' individual enterprise architecture efforts and their planned and ongoing investment activities and to do so in a way that, among other things, identifies opportunities for avoiding duplication of effort and launching initiatives to establish and implement common, reusable, and interoperable solutions across agency boundaries. We testified that we supported these goals. However, we also recognized that development and use of the FEA is but the first step in a multistep process to realize the promise of interagency solutions. In addition, because the FEA is still maturing both in content and in use, we raised a number of questions that we believed OMB needed to address in order to maximize understanding about the tool and thus facilitate its advancement. Specifically, we asked the following:

- *Should the FEA be described as an enterprise architecture?* As we discussed earlier, a true enterprise architecture is intended to provide a blueprint for optimizing an organization's business operations and implementing the IT that supports them. Accordingly, well-defined enterprise architectures describe, in meaningful models, both the enterprise's "As Is" and "To Be" environments, along with the plan for transitioning from the current to the target environment. To be meaningful, these models should be inherently consistent with one another, in view of the many interrelationships and interdependencies among, for example, business functions, the information flows among the functions, the security needs of this information, and the services and applications that support these functions.

[22]U.S. General Accounting Office, *Information Technology: The Federal Enterprise Architecture and Agencies' Enterprise Architectures Are Still Maturing*, GAO-04-798T (Washington, D.C.: May 19, 2004).

Our reading of the four available reference models does not demonstrate to us that this kind of content exists in the FEA and thus we believe that it is more akin to a point-in-time framework or classification scheme for federal government operations. Accordingly, if agencies use the FEA as a model for defining the depth and detail for their own architectures, the agencies' enterprise architectures may not provide sufficient content for driving the implementation of their systems.

- *Is the expected relationship between agencies' enterprise architectures and the FEA clearly articulated?* Among other things, the FEA is to inform agencies' enterprise architectures. For example, OMB has stated that although it is not mandating that the business reference model serve as the foundation for every agency's business architecture, agencies should invest time mapping their respective business architectures to the FEA. Similarly, OMB has stated that agencies' alignment of their respective architectures to the services component reference model and the technical reference model will enable each agency to categorize its IT investments according to common definitions.

  In our view, such descriptions of the agency enterprise architecture/FEA relationship are not clear, in part because definitions of such key terms as *alignment*, *mapping*, *and consistency* are not apparent in the FEA. As with any endeavor, the more ambiguity and uncertainty there is in requirements and expectations, the greater the use of assumptions; the more assumptions that are made, the higher the risk of deviation from the intended course of action. This is particularly true in the area of enterprise architecture.

- *How will the security aspects of the FEA be addressed?* Our work has found that a well-defined enterprise architecture should include explicit discussion of security, including descriptions of security policies, procedures, rules, standards, services, and tools.[23] Moreover, security is an element of the very fabric of architecture artifacts and models and thus should be woven into them all. As our experience in reviewing agency security practices and our research into leading practices shows, security cannot be an afterthought when it comes to engineering systems or enterprises.[24]

  OMB has stated that it plans to address security through what it refers to as a "security profile" to be added to the FEA. However, OMB could not comment on the profile's status or on development plans for it, beyond stating that the CIO Council is taking the lead in developing the profile.

Initial Version of DHS's Architecture Provides a Partial Foundation upon Which to Build, but Not a Sufficient Basis to Guide Investment Decisions

The initial version of DHS's enterprise architecture is missing many of the key elements[25] of a well-defined architecture. Further, those elements that are in the initial version are not based on the department's strategic business plan, as architecture development best practices advocate. Instead, the architecture is largely the result of combining the architectures and ongoing IT investments that several of the 22 agencies brought with them when the department was formed. According to DHS senior architecture officials, including the chief architect, Version 1.0 was developed in this manner because it pre-dated completion of the department's first strategic plan, only had limited staff assigned to it, and needed to be done in only 4 months in order to meet OMB's deadline for submitting the department's fiscal year 2004 IT budget. They also stated that this initial version was intended to mature the department's approach and methodology for developing the next version of the architecture, rather than to develop a version of the architecture that could be acted on and implemented. As a result, even though Version 1.0 provides a partial

[23]U.S. General Accounting Office, *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).

[24]U.S. General Accounting Office, *Executive Guide: Information Security Management—Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[25]These key elements are described in detail later in the report.

foundation upon which to build a well-defined architecture, DHS has spent and continues to spend large sums of money on IT investments without having such an architecture to effectively guide and constrain these investments. Our experience with federal agencies has shown that this often results in systems that are duplicative, are not well integrated, are unnecessarily costly to maintain and interface, and do not effectively optimize mission performance.

Initial Version of Architecture Is Missing Important Content

As previously discussed, the various frameworks used to develop architectures consistently provide for describing a given enterprise in both logical and technical terms, and for doing so for both the enterprise's current or "As Is" environment and its target or "To Be" environment; these frameworks also provide for defining a capital investment sequencing plan to transition from the "As Is" to the "To Be" environment. However, the frameworks do not prescribe the degree to which the component parts should be described to be considered correct, complete, understandable, and usable—essential attributes of any architecture. This is because the depth and detail of the descriptive content depend on what the architecture is to be used for (i.e., its intended purpose).

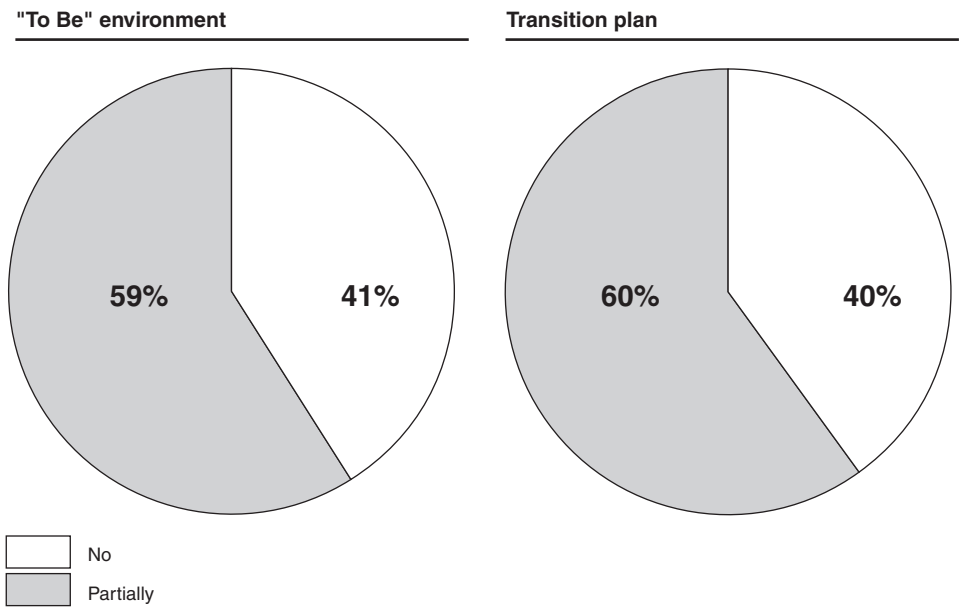
DHS's stated intention is to use an architecture as the basis for departmentwide and national operational transformation and supporting systems modernization and evolution. The CIO stated that the department was already using the architecture to help guide IT investment decisions. This purpose necessitates that the architecture products provide considerable depth and detail, as well as logical and rational structuring and internal linkages. More specifically, it means that these architecture products should contain sufficient scope and detail so that, for example, (1) duplicative business operations and systems are eliminated; (2) business operations are standardized and integrated and supporting systems are interoperable; (3) use of enterprisewide services is maximized; and (4) related shared solutions are aligned, like OMB's e-government initiatives.[26] Moreover, this scope and detail should be accomplished in a way that (1) provides flexibility in adapting to changes in the enterprise's internal and external environments; (2) facilitates the architecture's usefulness and comprehension from varying perspectives, users, or

[26]OMB's E-Government Task Force identified 23 initiatives (two additional initiatives were subsequently added) aimed at improving service to individuals, service to businesses, intergovernmental affairs, and federal agency-to-agency efficiency and effectiveness.

stakeholders; and (3) provides for properly sequencing investments to recognize, for example, the investments' respective dependencies and relative business value.

While the initial version of the architecture does provide some content that can be used to further develop it, it does not contain sufficient breadth and depth of departmentwide operational and technical requirements to effectively guide and constrain departmentwide business transformation and systems modernization efforts. More specifically, we found that DHS's "To Be" architecture products (Version 1.0) do not satisfy 14 of 34 (41 percent) key elements and only partially satisfy the remaining 20 (59 percent), and that its transition plan only partially satisfies 3 of 5 elements (60 percent) and does not satisfy the remaining 2 (40 percent) (see fig. 2.). This means that while Version 1.0 does provide some of the foundational content that can be used to extend and expand the architecture, it does not yet provide an adequately defined frame of reference to effectively inform business transformation and system acquisition and implementation decision making. Our specific analysis of the "To Be" and transition plan products follows.

Figure 2: Summary of Extent to Which Version 1.0 Satisfies Key Elements Governing Architectural Content



Source: GAO analysis of DHS data.

"To Be" Architecture: According to relevant guidance,[27] a "To Be" architecture should capture the vision of future business operations and supporting technology. That is, it should describe the desired capabilities, structures (e.g., entities, activities, and roles), and relationships among these structures at a specified time frame in the future. It should also describe, for example, future business processes, information needs, and supporting infrastructure characteristics, and it should be fiscally and technologically achievable. More specifically, a well-defined "To Be" architecture should provide, among other things, a description of

[27]See, for example, Office of Management and Budget, *Federal Enterprise Architecture Business Reference Model*, Version 2.0 (June 2003); Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001); Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130 (Nov. 28, 2000); M.A. Cook, *Building Enterprise Information Architectures: Reengineering Information Systems* (Prentice Hall Inc.: 1996); and National Institute of Standards and Technology, *Information Management Directions: The Integration Challenge*, Special Publication 500-167 (September 1989).

- the enterprise's business strategy, including its desired future concept of operations, its strategic goals and objectives, and the strategic direction to be followed to achieve the desired future state;
- future business processes, functions, and activities that will be performed to support the organization's mission, including the entities that will perform them and the locations where they will be performed;
- a logical database model that identifies the primary data categories and their relationships, which are needed to support business processes and to guide the creation of the physical databases where information will be stored;
- the systems to be acquired or developed and their relative importance in supporting the business operations;
- the enterprise application systems and system components and their interfaces;
- the policies, procedures, processes, and tools for selecting, controlling, and evaluating application systems;
- the technical standards to be implemented and their anticipated life cycles;
- the physical infrastructure (e.g., hardware and software) that will be needed to support the business systems;
- common policies and procedures for developing infrastructure systems throughout their life cycles;
- security and information assurance-related terms;
- the organizations that will be accountable for implementing security and the tools to be used to secure and protect systems and data;
- a list of the protection mechanisms (e.g., firewalls and intrusion detection software) that will be implemented to secure the department's assets; and

- the metrics that will be used to evaluate the effectiveness of mission operations and supporting system performance in achieving mission goals and objectives.

Architectures that include these elements can provide the necessary frame of reference to enable the engineering of business solutions (processes and systems) in a manner that optimally supports departmentwide goals and objectives, such as information sharing.

Version 1.0 of the department's "To Be" architecture provides some of the descriptive content mentioned above. For example, it contains (1) a high-level business strategy that includes a vision statement and a list of projects that may become future technology solutions; (2) a list of systems to be acquired or developed; (3) a description of the enterprise application systems and system components; (4) the technical standards to be implemented; (5) a description of the physical infrastructure (e.g., hardware and software) that will be needed to support the business systems; (6) definitions of security and information assurance-related terms; (7) a list of protection mechanisms, such as firewalls; and (8) high-level performance metrics.

However, the business strategy does not define the desired future concept of operations, the business-specific objectives to be achieved, and the strategic direction to be followed. Such content is important because the "To Be" architecture must be based on and driven by business needs. In contrast to this, the DHS "To Be" architecture is primarily focused on how to employ technology to improve current mission operations and services, instead of on identifying and addressing needed business changes through the use of technology. In addition, the systems listed are not described in terms of their relative importance to achieving the department's vision based on business value and technical performance, and the application systems and system components are not linked to the specific business processes they will support. Further, the technical standards are incomplete (e.g., do not specify standards that support narrowband wireless access) and do not include the anticipated life cycle of each standard. The physical infrastructure description is too high level (e.g., it does not define networks and their configurations or relate the technology platforms to specific applications and business functions). The architecture also does not define certain security and information assurance-related terms (e.g., security services) and, in some instances, it defines other terms (e.g., authentication and availability) differently than do the department's homeland security partners. For example, DHS's

definitions of authentication, availability, confidentiality, and integrity differ from DOD's definitions of these terms. In addition, the list of protection mechanisms is neither complete, nor does it describe all of the mechanisms shown and the interrelationships among them.

Other key elements that are not included are (1) a description of future business processes, functions, and activities that will be performed to support the organization's mission, including the entities or people that will perform them and the locations where they will be performed; (2) a logical database model; (3) the policies, procedures, processes, and tools for selecting, controlling, and evaluating application systems; (4) common policies and procedures for developing infrastructure systems throughout their life cycles; (5) the organizations that will be accountable for implementing security and the tools to be used to secure and protect systems and data; and (6) explicit metrics for the department's primary (e.g., identifying threats and vulnerabilities and facilitating the flow of people and goods) and mission-support (e.g., human resources and budget and finance) business areas. Detailed results of our analysis are provided in appendix II.

Transition Plan: According to relevant guidance and best practices,[28] the transition plan should provide a temporal road map for moving from the "As Is" to the "To Be" environment. An important step in the development of a well-defined transition plan is a gap analysis—a comparison of the "As Is" and "To Be" architectures to identify differences. Other important steps include analyses of technology opportunities and marketplace trends, as well as assessments of fiscal and budgetary realities and institutional acquisition and development capabilities. Using such analyses and assessments, options are explored and decisions are made regarding which legacy systems to retain, modify, or retire and which new systems to introduce on a tactical (temporary) basis or to pursue as strategic solutions. Accordingly, transition plans identify legacy, migration, and new systems and sequence them to show, for example, the phasing out and termination of systems and capabilities and the timing of the introduction of new systems and capabilities, and they do so in light of resource

[28]See, for example, Office of Management and Budget, *Federal Enterprise Architecture Business Reference Model*, Version 2.0 (June 2003); Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001); and Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130 (Nov. 28, 2000).

constraints such as budget, people, acquisition/development process maturity, and associated time frames.

Version 1.0 of DHS's transition plan generally does not possess any of these attributes. Specifically, it does not (1) include a gap analysis identifying the needed changes to current business processes and systems; (2) identify the legacy systems that will not become part of the "To Be" architecture or the time frames for phasing them out; (3) show a time-based strategy for replacing legacy systems, including identifying intermediate (i.e., migration) systems that may be temporarily needed; or (4) define the resources (e.g., funding and staff) needed to transition to the target environment. The result is that DHS does not have a meaningful and reliable basis for managing the disposition of its legacy systems or for sequencing the introduction of modernized business operations and supporting systems. Detailed results of our analysis are in appendix III.

A DHS contractor responsible for evaluating the quality of Version 1.0 reported weaknesses that are similar to ones that we identified. For example, the contractor reported the following:

- The "To Be" architecture did not address the reality that the department's systems would be a federated combination of legacy and new systems for many years. Rather, it assumes that its systems will be transformed into an ideal future state in the near term.

- The "To Be" architecture did not consistently address topics at the same level of detail, and it contained inconsistencies (i.e., some topics were addressed in more detail than others).

- The architecture did not sufficiently address security (i.e., network, data, physical, and information).

DHS's senior enterprise architecture officials, including the chief architect, agreed with the results of our analysis and stated that considerable work remained to adequately address all of the key architectural elements. According to the CIO and these officials, this initial version was prepared in 4 months, with limited resources (i.e., three DHS staff and minimal contractor support), based on the information available at that time. Further, it was prepared primarily to meet OMB's fiscal year 2004 IT budget submission deadline and to help educate DHS's senior executives about the importance of this architecture in the department's overall transformation effort. Senior architecture officials also stated that a transition plan was

not intended to be part of the scope of Version 1.0, and that the department's initial focus was on maturing its ability to execute an approach and methodology for developing the next version of the architecture.

Notwithstanding these reasons, constraints, and intentions, the fact remains that Version 1.0 is missing important content and, without this content, the department—as well as homeland security stakeholders in other federal agencies, state and local governments, and the private sector—will not have the sufficiently detailed, authoritative frame of reference that is needed to provide a common understanding of future homeland security operational, business, and supporting technology needs. Such a frame of reference is important to effectively guide and constrain the transformation of mission operations, business functions, and associated IT investments. Without it, DHS and other homeland security stakeholders will be challenged in their ability to effectively leverage technology to affect the kind of logical and systematic institutional change needed to optimize enterprisewide mission performance.

Content of Initial Architecture Is Based on Strategic Business Assumptions and Existing Agencies' Architectures Rather Than Departmental Strategic Vision

The various architecture frameworks and architecture management best practices recognize the need to define the "To Be" environment using a top-down, business-driven approach in which the content of the organization's strategic plan (mission, goals, objectives, scope, and outcomes) drives operational processes, functions, activities, and associated information needs, which in turn drive system application and services and supporting technology standards. The architecture development methodology[29] being employed by DHS also calls for this top-down, mission- and business-driven approach, which engages mission and business area subject matter experts. It specifically states that an architecture should be based on a functional business model that reflects the nature of the operational mission, the business strategy, and the information to be used to accomplish them.

[29]Steven H. Spewak with Steven C. Hill, *Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology* (Princeton, N.J.: John Wiley and Sons, Incorporated, 1992).

DHS did not follow this approach in developing Version 1.0 of its architecture, primarily because the department did not issue a strategic plan until February 2004. Specifically, the department released its initial architecture in September 2003, approximately 5 months before it issued its strategic plan. Without an explicit strategic direction to inform the architecture, the architecture's business representation was derived from the existing architectures and the ongoing and planned IT investments of some of its component agencies (i.e., Immigration and Naturalization Service, Customs and Border Protection, Coast Guard, and the Federal Emergency Management Agency). As a result, Version 1.0 did not contain a departmentwide and national corporate business strategy that described such things as (1) the desired future state of its mission operations and business activities, (2) the specific goals and objectives to be strategically achieved, and (3) the strategic direction to be followed by the department to realize the desired future state. Rather, the architecture's strategic operational and business content is basically the sum of its component agencies' business strategy parts. Moreover, although the department is using generally accepted architecture development techniques, the architecture artifacts that have been derived using these techniques (i.e., the value chain analysis,[30] CURE matrix,[31] conceptual data model, and sequencing diagram) do not provide a consistent view of the scope of the department's mission. In some instances, the vision focuses internally on departmental activities only, while in other instances, it focuses on homeland security at a national level (i.e., addresses other homeland security stakeholders, such as other federal agencies and state and local government). The architecture's business strategy also does not identify corporate priorities and constraints to be considered when making departmentwide and national decisions about future homeland security activities. The DHS contractor responsible for evaluating the quality of Version 1.0 made similar comments concerning the architecture's business strategy. Specifically, the contractor reported that the scope of the architecture was unclear, at times being internally focused on only the department, while at other times being more broadly focused on national

[30]The value chain provides a holistic view of business activities across the enterprise, showing high-level business functions that are central to mission fulfillment and add value to the services provided by the enterprise. The value chain cuts across organizational boundaries.

[31]A CURE (create, update, reference, and eliminate) matrix shows the business functions and applications that create, update, reference, and/or eliminate specific data elements, enabling the organization to develop applications.

homeland security. Further, the contractor reported that the business strategy did not include all DHS mission activities.

According to the chief architect, the fiscal year 2004 IT budget submission deadline did not allow the department to delay development of the architecture until the strategic plan had been completed. A senior architecture official also stated that this time constraint (i.e., 4-month development period) did not allow subject matter experts (i.e., both internal and external DHS stakeholders) to be consulted and to participate in developing Version 1.0. According to the CIO, subject matter experts are now participating in the department's architecture development activities.

As stated above, having a mission- and business-driven enterprise architecture is a fundamental principle. Until the department uses an enterprisewide understanding of its mission operations and business as the basis for developing its architecture, its architecture's utility will be greatly diminished, and it is unlikely that changes to existing operations and systems that are based on this architecture will provide for optimization of mission performance and satisfaction of stakeholder needs. Moreover, because DHS did not base Version 1.0 on such an understanding, the content of this version may prove to be invalid if future work shows that the strategic business assumptions used to develop it were inaccurate. This in turn would limit the value of Version 1.0 as a basis for building the next version.

Initial Architecture Can Be Partially Traced to the Federal Enterprise Architecture, but the Extent of Alignment Is Unclear

OMB guidance does not explicitly require agency enterprise architectures to align with the FEA. However, a requirement for alignment is implicit in the OMB guidance. For example, this guidance states that agencies' major IT investments must align with each of the FEA's published reference models (business, performance, services, and technical), and that agencies' nonmajor IT investments must align with the business reference model.[32] Since an agency's enterprise architecture is to include a transition plan that strategically sequences its planned IT investments in a way that moves the agency from its current architectural environment to its target environment, this means that the agency's investments would need to align with both the FEA and the agency enterprise architecture, which in turn would necessitate alignment between the FEA and the agency architecture. Aligning agencies' architectures with the FEA is also an implied requirement in recently released OMB guidance for its enterprise architecture assessment tool.[33] According to this guidance, agency enterprise architectures are "a basic building block to support the population of the FEA." Further, OMB states that one of the purposes of the FEA is to inform agency efforts to develop their agency-specific enterprise architectures.

We have previously reported that OMB's expected relationship between the FEA and agency enterprise architectures has not been clearly articulated, in part because OMB has not defined key terms, such as architectural alignment.[34] In the absence of clear definitions, we also reported that assumptions must be made about what alignment means, and that the greater the use of assumptions, the greater the chances of expectations about these relationships not being met and intended outcomes not being realized. For the purposes of this report, we have assumed that alignment can be examined from three perspectives: functional, structural, and semantic. Functional alignment means that the architecture and the reference models have been decomposed to the same level of detail to determine if the business operations, services, and technology components are similar in nature and purpose. Structural alignment means that the

[32]Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (July 25, 2003; revised Nov. 14, 2003).

[33]Office of Management and Budget, *Enterprise Architecture Assessment Framework*, Version 1.0, April 2004.

[34]GAO-04-798T.

architecture and the reference models are both constructed similarly, for example, they may share the same hierarchical construct whereby information is grouped by common levels of detail. Semantic alignment means that the department's architecture and the FEA reference models use similar terms and/or definitions that can be mapped to one another.

The FEA and Version 1.0 of DHS's enterprise architecture are not aligned functionally or structurally. Specifically, we could not map Version 1.0 to the FEA from either of these perspectives because the DHS architecture is not decomposed to the same level of detail as the reference models and thus does not permit association of the respective functional components and because the DHS architecture is not structured in a hierarchical fashion as the reference models are.

However, the terms or definitions used in the business, services, and technical components of Version 1.0 could be mapped to similar terms in the FEA business, services, and technical reference models. The results of this mapping are discussed below.

- We mapped all 79 of the high-level activities that we found in the business view of the DHS architecture to similar terms in the FEA business reference model. To achieve this degree of mapping, however, we needed to trace the 79 high-level activities to multiple levels of the reference models, including business areas, lines of business, and subfunctions. For example, for the DHS high-level business activity "stockpile and deploy supplies" (defined as including managing immunizations, as well as identification, acquisition, development, maintenance, and distribution of other pharmaceutical and medical supplies) we needed to go to the reference model's subfunction level to find "immunization management." In addition, we were not able to map any terms in the DHS architecture to several areas in the business reference model that would appear relevant to DHS, such as the business area "mode of delivery" or the line of business "defense and national security."

- We also mapped Version 1.0's applications/services view to the FEA services reference model. In this case, the initial architecture contained terms that could be associated with all of the FEA reference model's 7 service domains, 29 service types, and 168 service components.

- We also mapped terms used for technical services in the Version 1.0 technical view to the FEA technical reference model. However, this

mapping was again based on associating high-level descriptions in Version 1.0 with lower-level descriptions in the FEA. Moreover, some terms for technology elements in Version 1.0 could not be mapped to the FEA technical reference model, such as "narrowband wireless and broadband wireless." Conversely, some technical services and standards in the reference model that should be applicable to DHS were not evident in Version 1.0, such as software engineering (including test management services) and database middleware standards, respectively. In those instances where we could not semantically associate Version 1.0 to the FEA reference models, we found no associated explanations. As a result, we could not determine whether future alignment is envisioned or not.

According to the CIO and the chief architect, the steps that DHS took to align the initial architecture with the FEA reference models represent the most that could be done in the time available. The architect also stated that changes would be made to the technical views of the architecture to more closely reflect the content within the FEA's technical reference model. However, given that what is meant by agency architectural alignment to the FEA is not well defined, the degree to which DHS and other agencies can establish the intended relationship between the two is both challenging and uncertain. This in turn will constrain OMB's ability to meet the goals it has set for the FEA.

Conclusions

Having and using an enterprise architecture that reflects the department's strategic operational and business needs and enables it to make informed decisions about competing investment options is critical to DHS's business transformation and supporting system modernization efforts. DHS recognizes this and has produced an initial architecture in a short time with limited resources and is working on its next version. Nevertheless, the department is in the midst of transforming itself and investing hundreds of millions of dollars in supporting systems without a well-defined architecture to effectively guide and constrain these activities. Following this approach is a risky proposition, and the longer DHS goes without a well-defined and enforced architecture the greater the risk. Therefore, it is important that DHS ensure that the next version is based on a top-down, strategic business-based approach that involves key stakeholders, as advocated by best practices. It is also important for DHS to ensure that its architecture includes the necessary content. Until this is done, it will be prudent for the department to limit new system investments to those meeting certain criteria, as we have previously recommended. To do less

puts the department at risk of investing hundreds of millions of dollars in efforts that will not promote integration and interoperability and will not optimize mission performance.

Further, the relationships that OMB expects between the FEA and agency architectures, including DHS's are not clear. Until OMB clarifies what it means by architectural alignment, it is unlikely that the outcomes it envisions and desires through architectural alignment will result.

Recommendations for Executive Action

To ensure that DHS has a well-defined architecture to guide and constrain pressing transformation and modernization decisions, we recommend that the Secretary of Homeland Security direct the department's architecture executive steering committee, in collaboration with the CIO, to (1) ensure that the development of DHS's enterprise architecture is based on an approach and methodology that provides for identifying the range of mission operations and the focus of the business strategy and involving relevant stakeholders (external and internal) in driving the architecture's scope and content; and (2) develop, approve, and fund a plan for incorporating into the architecture the content that is missing.

In addition, we are recommending 39 actions to ensure that future versions of the architecture include (1) the six key elements governing the *business* view of the "To Be" architectural content that our report identified as not being fully satisfied, (2) the three key elements governing the *performance* view of the "To Be" architectural content that our report identified as not being fully satisfied, (3) the seven key elements governing the *information* view of the "To Be" architectural content that our report identified as not being fully satisfied, (4) the five key elements governing the *services/applications* view of the "To Be" architectural content that our report identified as not being fully satisfied, (5) the six key elements governing the *technical* view of the "To Be" architectural content that our report identified as not being fully satisfied, (6) the seven key elements governing the *security* view of the "To Be" architectural content that our report identified as not being fully satisfied, and (7) the five key elements governing the transition plan content that our report identified as not being fully satisfied.

In addition, to assist DHS and other agencies in developing and evolving their respective architectures, we recommend that the Director of OMB direct the FEA Program Management Office to clarify the expected relationship between the FEA and federal agencies' architectures. At a

minimum, this clarification should define key terms, such as architectural alignment.

Agency Comments and Our Evaluation

In DHS's written comments on a draft of this report, signed by the Director, Bankcard Programs and GAO/OIG Liaison within the Office of the Chief Financial Officer (reprinted in app. IV), the department agreed that much work remains to develop both a target enterprise architecture and a transition plan to support business and IT transformation, and it stated that it would ensure that the architecture criteria that we cite in our report, which our recommendations reference, are addressed to the extent possible in Version 2.0 of its architecture. Notwithstanding these statements, the department also stated that it took exception to several aspects of our report, including our criteria and recommendations. In particular, it stated that (1) the criteria were not realistic and assumed the existence of a comprehensive enterprise architecture, the development of which was inconceivable in the time available, (2) the criteria had not been provided to the federal community and were not available when Version 1.0 of DHS's architecture was being developed, and (3) the recommendations did not take into consideration the department's limited resources. DHS stated that it had accomplished one of the most important goals of Version 1.0, which was "positioning the department to more actively engage with our business representatives, with a strategic plan in hand and a greater awareness of the need for and value of an enterprise architecture generally on the part of our senior and executive management." DHS also provided specific comments on our findings relative to each criterion that we assessed Version 1.0 against. These comments fell into two general categories: agree that content is missing but content was not intended to be part of Version 1.0, and do not agree that content is missing (i.e., factually incorrect).

We do not agree with the department's comments concerning the criteria and our recommendations. In particular, our report does not state that DHS should have ensured that Version 1.0 of its enterprise architecture satisfied all of the criteria that we cite. We have long held and reported the position that enterprise architecture development should be done incrementally,[35] with each version of an architecture providing greater depth and detail to

[35]See, for example, *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).

an enterprisewide, business-driven foundational layer. We provide in the report an analytical assessment of where Version 1.0 stands against a benchmark of where it will need to be in order to be an effective blueprint to guide and constrain major investment decisions for organizational transformation. In doing so, we have provided the department with a road map, grounded in explicit criteria, for incrementally developing a mission-derived blueprint.

In addition, the criteria that we used in our review and cite in our report came from published literature on the content of enterprise architectures, which we structured into categories consistent with federal enterprise architecture guidance and have used in prior evaluations of other agencies' enterprise architectures, the results of the first of which we issued in September 2003.[36] We shared these criteria and categories with DHS at the time that we began our review, and we shared the results of our review relative to each criterion with DHS enterprise architecture program and contractor officials over a 2-day period after we completed our review. At that time, both the DHS and the contractor officials agreed with our results. While we acknowledge that we had yet to publish our categorization of the criteria at the time that Version 1.0 of DHS's architecture was being developed, the criteria that we drew from and used were both well established and publicly available.

In addition, we recognize in both the report and its recommendations the point made in DHS's comments about the initial architecture development effort being constrained by resources. It is because of this that our recommendations call for DHS's architecture executive steering committee, which is composed of those department business and technology executives who collectively control billions of dollars in resources, to develop, approve, and fund a plan for completing the architecture. In our view, the resource point cited in DHS's comments is a departmental funding allocation and prioritization decision, rather than a resource shortage issue.

Also, we do not question the department's comment concerning the intent and goal of Version 1.0, or whether its goal has been accomplished. Rather, the purpose and scope of our work was to determine the extent to which the initial architecture version contained the building blocks of a well-defined blueprint and to thereby identify what, if anything, remained to be

[36] GAO-03-1018.

accomplished. If more needed to be done, our objective was to determine whether the initial version provided a foundation upon which to build any missing content. As we previously stated, development of a well-defined enterprise architecture is by necessity incremental, and our report is intended to provide DHS with a criteria-based road map for incrementally accomplishing this. To avoid any misunderstanding about the need to develop the architecture incrementally, we have added further detail on this topic to this report.

With respect to DHS's specific comments on each of the findings and recommendations that acknowledged missing content, we support the department's statements indicating that it will address this missing content in the next or subsequent versions of the architecture. However, we do not agree with DHS's comments when it stated that our findings were factually incorrect or when it disagreed with the criteria. Our responses to DHS's comments for each of these areas of disagreement are provided in appendix IV.

In their oral comments on a draft of this report, OMB's Office of E-Government and Information Technology and the Office of General Counsel officials stated that OMB's Administrator for Electronic Government, Information and Technology had recently testified that additional work was needed to mature the FEA. In addition, the officials stated that OMB is committed to working to evolve the FEA and agency enterprise architectures, and that this work will clarify many of the issues raised in our report.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security and to the Director of OMB. We will also 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 have any questions on matters discussed in this report, please contact me at (202) 512-3439 or hiter@gao.gov. Key contributors to this report are acknowledged in appendix V.

Sincerely yours,

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

Objectives, Scope, and Methodology

Our objectives were to determine whether the initial version of the Department of Homeland Security's (DHS) enterprise architecture (1) provides a foundation upon which to build and (2) is aligned with the Federal Enterprise Architecture (FEA).

To address the first objective, we followed the approach that we have previously used to evaluate the content of an agency's enterprise architecture.[1] Specifically, we first segmented Version 1.0 of the architecture into the three primary component parts of any architecture: the "As Is," the "To Be," and the transition plan. We then further divided the "As Is" and "To Be" architectures into five architectural components similar to the Office of Management and Budget's (OMB) architecture reference models and defined in our enterprise architecture maturity framework: business, information/data, services/applications, technical, and performance; we added security as a sixth component because of its recognized importance in the various architecture frameworks and its relevance to the other five architectural components.[2] Because the department is currently investing about $4.1 billion in fiscal year 2004 for IT systems and supporting infrastructure, we focused our evaluation on the "To Be" architecture and the transition plan and did not analyze whether DHS's "As Is" architecture satisfied relevant "As Is" guidance. For each of these six architectural components, we used the key architectural requirements that we previously reported as necessary for a well-defined "To Be" architecture.[3] We also used the key architectural requirements that we previously reported as necessary for a well-defined transition plan.[4] We then compared the "To Be" architecture and transition plan (Version 1.0)

[1]See, for example, U.S. General Accounting Office, *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, GAO-04-43 (Washington, D.C.: Nov. 21, 2003); and *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).

[2]See, for example, Office of Management and Budget (OMB), *Federal Enterprise Architecture Business Reference Model*, Version 2.0 (June 2003); Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001); OMB, *Management of Federal Information Resources*, Circular No. A-130 (Nov. 28, 2000); M.A. Cook, *Building Enterprise Information Architectures: Reengineering Information Systems* (Prentice Hall Inc.: 1996); and National Institute of Standards and Technology, *Information Management Directions: The Integration Challenge*, Special Publication 500-167 (September 1989).

[3]GAO-04-43.

[4]GAO-04-43.

against the key elements. In doing so, we used the following criteria to determine whether the key element was fully,[5] partially,[6] or not satisfied.[7]

To assess the extent to which the architecture was aligned with the FEA, we compared the "To Be" architecture with the FEA business, services- and technical reference models, Versions 2.0, 1.0, and 1.1, respectively. We did not select the performance, information/data,[8] and security models[9] because department officials told us that these models were not part of the scope of their effort in developing Version 1.0. We, therefore, focused on the business, services, and technical models and attempted to map the architecture and FEA reference models at three levels: semantic, functional, and structural.[10] However, we were unable to do so from a functional or structural standpoint because the DHS architecture was neither decomposed to the same level of detail, nor constructed in a hierarchical fashion like the reference models. We therefore mapped key elements of the DHS architecture (e.g., business activities, target applications, and services) to the reference models by identifying similar terms and/or definitions. To augment our documentation reviews and analyses of the architecture, we also interviewed various officials, including the chief information officer and chief architect to determine, among other things, these officials' comments on our detailed analysis.

We also met with OMB officials to discuss its process for reviewing agencies' enterprise architectures and the results of its review of DHS's

[5]The architecture satisfies all aspects of this key architectural element.

[6]The architecture partially satisfies some aspects of this key architectural element but does not satisfy at least one significant aspect.

[7]The architecture does not satisfy any aspects of this key architectural element.

[8]OMB has not officially released the data reference model.

[9]OMB has not yet developed a "security profile" for the FEA.

[10]For purposes of this report, we defined semantic alignment to mean that the department's architecture and the FEA reference models use similar terms and/or definitions that can be mapped to one another. We defined functional alignment to mean that the architecture and the reference models have been decomposed to the same level of detail to determine if the business operations, services, and technology components are similar in nature and purpose. We defined structural alignment to mean that the architecture and the reference models are both constructed similarly, for example, they may share the same hierarchical construct whereby information is grouped by common levels of detail.

architecture. According to OMB officials, its review of DHS's architecture is still ongoing and thus we were not provided a copy of the review results.

We conducted our work at DHS headquarters in Washington, D.C. We performed our work from November 2003 to May 2004 in accordance with generally accepted government auditing standards.

Detailed Results of GAO's Analyses of Version 1.0 of DHS's "To Be" Architecture

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
Business				
A business assessment[a] that includes the enterprise's purpose, scope (e.g., organizations, business areas, and internal and external stakeholders' concerns), limitations or assumptions, and methods. A gap analysis[b] that describes the target outcomes and shortfalls, including strategic business issues, conclusions reached as a result of the analysis (e.g., missing capabilities), causal information, and rationales.			X	The architecture does not contain a business assessment or gap analysis results. However, the architecture recognizes the need to perform a business assessment and project-specific gap analyses. It also identifies possible concerns (e.g., inefficiencies in business function and technology) that may be addressed by the department.
A business strategy that describes the desired future state of the business, the specific objectives to be achieved, and the strategic direction that will be followed by the enterprise to realize the desired future state.			X	The architecture does not have a business strategy that adequately describes the desired future state of the business, the objectives to be achieved, and the strategic direction to be followed.
The business strategy should include:				However, the architecture does address to a limited degree the characteristics of a business strategy, as discussed below.
• A vision statement that describes the business areas requiring strategic attention based on the gap analysis.				The architecture does contain a vision statement; however, this statement does not highlight opportunities for strategic change to business processes, nor does it present a consistent view of the national responsibilities for homeland security at the various levels (i.e., federal, state, local, and international).
• A description of the business priorities and constraints, including their relationships to, at a minimum, applicable laws and regulations, executive orders, departmental policy, procedures, guidance, and audit reports.				The architecture recognizes that homeland security processes, procedures, and decisions about IT management should comply with applicable laws, regulations, and guidance, particularly those associated with privacy requirements. The architecture also specifically mentions the National Strategy for Homeland Security. However, the architecture does not explicitly identify, reconcile, prioritize, or align the applicable laws, regulations, and guidance. As a result, business priorities and constraints are not identified.

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
• A description of the scope of business change that is to occur to address identified gaps and realize the future desired business state. The scope of change, at a minimum, should identify expected changes to strategic goals, customers, suppliers, services, locations, and capabilities.				The architecture does not explicitly identify what will be changed in the "As Is" environment. It also does not explicitly identify key customers, suppliers, products, services, locations, and capabilities for homeland security at the national level.
• A description of the measurable strategic business objectives to be met to achieve the desired change.				The architecture does not describe measurable strategic business objectives; however, it does contain objectives in the transition strategy that may be used to develop strategic business objectives.
• A description of the measurable tactical business goals to be met to achieve the strategic objectives.				The architecture does not describe measurable tactical business goals; however, it does describe some high-level performance measures for several of its business areas.
• A listing of opportunities to unify and simplify systems or processes across the department, including their relationships to solutions that align with the strategic initiatives to be implemented to achieve strategic objectives and tactical goals.				The architecture does not align all opportunities for change with strategic initiatives and potential investments. However, the architecture does identify conceptual[c] projects and opportunities to address inefficiencies in systems and processes.
Common (standard and departmentwide) policies, procedures, and business and operational rules for consistent implementation of the architecture.		X		
A description of key business processes and how they support the department's mission, including the organizational units responsible for performing the business processes and the locations where the business processes will be performed. This description should provide for the consistent alignment of (1) applicable federal laws, regulations, and guidance; (2) department policies, procedures, and guidance; (3) operational activities; (4) organizational roles; and (5) operational events and information.		X		
A description of the operational management processes to ensure that the department's business transformation effort remains compliant with the business rules for fault, performance, security, configuration, and account management.		X		

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A description of the organizational approach (processes and organizational structure) for communications and interactions among business lines and program areas for (1) management reporting, (2) operational functions, and (3) architecture development and use (i.e., how to develop the architecture description, implement the architecture, and govern/manage the development and implementation of the architecture).		X		
Performance				
A description of the processes for establishing, measuring, tracking, evaluating, and predicting business performance regarding business functions, baseline data, and service levels.			X	The architecture does not describe these processes. However, the architecture recognizes the need for such processes and identifies a conceptual project and a business activity that will be used to establish these processes.
A description of measurable business goals and outcomes for business products and services, including strategic and tactical objectives.			X	The architecture does not describe explicit measurable business goals and outcomes for any of the department's primary and secondary business areas (e.g., identify threats and vulnerabilities; and prevent, prepare and recover from incidents). However, the architecture does provide a description of customer-focused, measurable business goals and outcomes (e.g., the average time taken to resolve customer inquiries) for all of the department's primary and secondary business areas (e.g., human resources and budget and finance), with one exception (i.e., the architecture does not contain customer-focused, measurable goals and outcomes for the primary line of business entitled "facilitate the flow of people and goods").

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A description of measurable technical goals and outcomes for managing technology products and services for the "To Be" architecture that enables the achievement of business goals and outcomes.			X	The architecture does not contain measurable technical goals and outcomes for managing technology products and services that enables the achievement of business goals and outcomes (e.g., identifying threats and preventing terrorist attacks). However, the architecture does contain performance measures for managing technology (e.g., percentage of data or information shared across organizational units and time to produce, create, and deliver products or services). The architecture also lists conceptual projects focused on improving technology management performance with respect to information sharing (e.g., infrastructure consolidation).
Information/data				
A description of data management policies, procedures, processes, and tools (e.g., CURE matrix[d]) for analyzing, designing, building, and maintaining databases in an enterprise architected environment.			X	The architecture does not describe or reference enterprise data management policies, procedures, or processes. However, the architecture does contain a CURE matrix. The utility of this CURE matrix for planning purposes is questionable because the relationships among business functions and applications are ambiguous—not uniquely identified or defined.
A description of the business and operational rules[e] for data standardization to ensure data consistency, integrity, and accuracy, such as business and security rules that govern access to, maintenance of, and use of data.		X		
A data dictionary, which is a repository of standard data definitions for applications.			X	The architecture does not contain a data dictionary. However, the architecture does contain an information dictionary that, while incomplete, does identify some data objects (e.g., cargo, incident, and weapon). As a result, this information glossary could be used to facilitate the creation of a data dictionary.

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A conceptual data model that describes the fundamental things/objects (e.g., business or tourist visas, shipping manifests) that make up the business, without regard for how they will be physically stored. A conceptual data model contains the content needed to derive facts about the business and to facilitate the creation of business rules. It represents the consolidated structure of business objects to be used by business applications.			X	The architecture does not provide a conceptual data model that contains the content needed to derive facts about the business and to facilitate the creation of business rules to build databases. The content is at such a high level (e.g., labels and terms) that it can be interpreted in numerous ways. However, the architecture does provide a high-level conceptual data model that identifies "super-classes" or groupings of objects without the required business context, such as (1) the complete definitions for information categories or classes and (2) concrete business objects. This information can be used to build the conceptual data model.
A logical database model that provides (1) a normalized (i.e., nonredundant) data structure that supports information flows and (2) the basis for developing the schemas for designing, building, and maintaining physical databases.		X		
A metadata[f] model that specifies the rules and standards for representing data (e.g., data formats) and accessing information (e.g., data protocols) according to a documented business context that is complete, consistent, and practical.		X		
A description of the information flows and relationships among organizational units, business operations, and system elements.		X		

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
Services/applications				
A description of the services and their relationships to key end-user services to be provided by the application systems.			X	The architecture does not specify all the end-user services to be provided by application systems (e.g., the use of e-mail as an end-user service for various applications), nor does it provide a rationale for this exclusion. It also does not specify the various relationships between the end-user services and the entities that will provide these services. The architecture also contains inconsistencies in the descriptions of the relationships between user services and application systems, which affect its utility. For example, in one instance, the architecture notes that correspondence management may involve "maintaining logs and references to pieces of correspondence that are of interest to the enterprise for tracking purposes and that these pieces of correspondence may be e-mails, paper letters, phone conversations, etc." In another instance, the architecture does not recognize the use of this e-mail service for managing correspondence. However, the architecture does contain high-level descriptions of the types of application systems that will be needed (e.g., a financial management application that can manage all financial aspects of general accounting, budgeting, capital assets, and investment control). It also notes that "To Be" applications will be derived and created based on how each user class uses data while performing business activities.

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A list of application systems (acquisition/development and production portfolio) and their relative importance to achieving the department's vision, based on business value and technical performance.			X	The architecture does not identify the applications' relative importance to the overall vision. For example, it does not explicitly identify and describe application systems that support functionality across organizational boundaries (e.g., local, state, and federal agencies). In addition, priorities are not explicitly defined for the target applications. However, the architecture provides a list of the types of candidate applications (e.g., financial, grant, and property management) and links these application types to business functions by providing an application-to-function cross-reference matrix. In addition, it identifies conceptual projects that may provide target capabilities or applications and it prioritizes these projects according to scheduled completion times. For example, some conceptual projects are placed within a category labeled "Rationalize," which means they are scheduled for completion within 6 months.
A description of the policies, procedures, processes, and tools for selecting, controlling, and evaluating application systems to enable effective IT investment management.		X		
A description of the enterprise application systems and system components and their interfaces.			X	The architecture does not describe applications in terms of the business process flows that each application will support (e.g., how to identify and report threats and vulnerabilities), nor does the architecture describe the business process flows. The architecture also does not reflect how application selection decisions can or will be made without this information. Further, it does not identify human/machine boundaries, inputs, outputs, controls, and standard application programming interfaces. However, the architecture contains a list and graphic depictions of the types of application systems that would satisfy the department's business needs, including a brief description of the functionality to be provided by these systems. For example, it describes a generic "financial management" application that could be satisfied by many application packages or development components.

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A description of the system development life cycle process for application development or acquisition and the integration of the process with the architecture, including policies, procedures, and architectural techniques and methods for acquiring systems throughout their life cycles. The common technical approach should also describe the process for integrating legacy systems with the systems to be developed/acquired.		X		
Technical				
A list of infrastructure systems and a description of the systems' hardware and software infrastructure components. The description should also reflect the system's relative importance to achieving the department's vision based on constraints, business value, and technical performance.			X	The architecture does not provide a complete list of the "To Be" infrastructure systems, nor does it describe the functional characteristics, capabilities, and interconnections for the infrastructure projects listed. It also does not reflect the systems' relative importance to achieving DHS's vision. For example, the relationship between the department's vision for infrastructure projects and their value in preventing terrorist attacks has not been defined. However, it does identify a conceptual project (i.e., OneDHS) that may be used to consolidate the infrastructure. It also identifies a list of conceptual applications (e.g., a communications management application to manage connectivity between networks) that may provide certain infrastructure capabilities and functions for OneDHS. Further, it identifies associated subprojects, such as a secure network, server and storage consolidation, and a standard desktop environment, and it associates them with the business areas. The architecture also lists several existing infrastructure systems, such as the Department of Defense's (DOD) Secure Internet Protocol Routing Network, which may be used by the department and its homeland security partners. The architecture outlines an approach for establishing a framework to enable DHS to sequence the delivery of capabilities over time based on homeland security priorities.
A description of the policies, procedures, processes, and tools for selecting, controlling, and evaluating infrastructure systems to enable effective IT investment management.		X		

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A description of the technical reference model (TRM[g]) that describes the enterprise infrastructure services,[h] including specific details regarding the functionality and capabilities that these services will provide to enable the development of application systems.			X	The architecture does not contain a TRM that describes all enterprise infrastructure services. The list of technical services is likely incomplete because the architecture does not identify all DHS organizations and its homeland security partners that supply and consume technical services. For example, the architecture indicates the use of DOD's Secure Internet Protocol Routing Network, which is a Global Information Grid (GIG)[i] enterprise service, to exchange information among homeland security organizations. However, it does not list the technical services that are provided by this network. The architecture also does not show whether these TRM services are common or reusable. In addition, the architecture does not describe the functionality and capabilities that will be provided by the services that are identified. However, it does contain a high-level TRM that provides a structure and vocabulary that can be used to describe DHS's enterprise infrastructure services. It also contains application principles (e.g., there will be only one enterprise application for each function area, to be used by all departmental organizations) and technology patterns (e.g., use of commercial-off-the-shelf software for implementing relational databases) that can be used to guide technology development and acquisition decisions.

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A description in the TRM that identifies and describes (1) the technical standards[j] to be implemented for each enterprise service and (2) the anticipated life cycle of each standard.			X	The architecture does not contain a complete standards profile (i.e., it excludes technical standards that support a number of the services reflected in the TRM). For example, the profile does not identify standards that support "narrowband wireless access," even though there are applicable homeland security applications that require this service (e.g., Land Mobile Radio, Air to Ground Communications, Mobile Operations IT). It also does not list the actual life cycles (e.g., "sunset" dates for current products and standards, and dates for when new developments will use target technologies) of many of the standards and products identified in the architecture. However, it does contain a list of technical standards that the department and/or its partners may implement.
A description of the physical IT infrastructure needed to design and acquire systems, including the relationships among hardware, software, and communications devices.			X	The architecture does not provide a description of the physical IT infrastructure that will be needed to support future operations. Specifically, it does not fully describe networks and their topologies and configurations for the department's internal and/or shared spaces. For example, the architecture does not identify the component parts of the DHS consolidated network. It also does not relate the technology platforms to applications and business functions. However, the architecture does provide a vision for the technology environment, such as a high-level diagram that depicts information sharing among user groups. It also identifies telecommunications backbone options for exchanging data, such as use of the Internet for sensitive but unclassified data. The architecture also identifies types of technology platforms, including computing, storage, and communication devices and software.
Common policies and procedures for developing infrastructure systems throughout their life cycles, including requirements management, design, implementation, testing, deployment, operations, and maintenance. These policies and procedures should also address how the applications will be integrated, including legacy systems.		X		

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
Security				
A description of the policies, procedures, goals, strategies, principles, and requirements relevant to information assurance and security and how they (the policies, procedures, goals, strategies, and requirements) align and integrate with other elements of the architecture (e.g., security services).			X	The architecture does not describe the policies, procedures, goals, strategies, principles, and requirements that are relevant to information assurance and security, nor their alignment and integration with other architecture elements. However, it does contain (1) a high-level diagram that depicts a data classification schema to facilitate information sharing (e.g., sensitive but unclassified or top secret); (2) a security pattern that can be used to provide capabilities to secure and protect IT resources (e.g., confidentiality via encryption, authorization and access control via single sign-on, and intrusion detection and prevention using firewalls); and (3) a security principle that reflects the requirement for sharing information contained within nonclassified systems. This information could be used to develop a strategy.
Definitions of terms related to security and information assurance.			X	The architecture does not define all key terms that are listed (e.g., "information assurance" and "security services"). In addition, there are discrepancies between DHS's security terms and others involved in homeland security, such as DOD. For example, DOD's definitions for authentication, availability, confidentiality, and integrity differ from DHS's definitions for the same terms. However, the architecture does contain definitions for some security-related terms (e.g., "identification and authorization" and "audit trail").
A listing of accountable organizations and their respective responsibilities for implementing enterprise security services. It is important to show organizational relationships in an operational view because they illustrate fundamental roles (e.g., who conducts operational activities) and management relationships (e.g., what is the command structure or relationship to other key players) and how these influence the operational nodes.		X		
A description of operational security rules that are derived from security policies.		X		

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
A description of enterprise security infrastructure services (e.g., identification and authentication) that will be needed to protect the department's assets and the relationship of these services to protective mechanisms.			X	The architecture's TRM does not explicitly identify the security services, making it difficult to ensure that there are no redundant services, nor does it clearly define what constitutes a technical security service. In addition, the architecture identifies DOD's Secure Internet Protocol Routing Network, thereby implying the use of a GIG enterprise service, but it does not reconcile how or whether these services will be used by DHS and other homeland security entities. However, the architecture does provide some guidance on security services, and it lists several services to be used to secure and protect resources, such as confidentiality, data integrity, authentication, and policy enforcement.
A description of the security standards to be implemented for each enterprise service. These standards should be derived from security requirements. This description should also address how these services will align and integrate with other elements of the architecture (e.g., security policies and requirements).			X	The architecture does not contain a complete list of standards. For example, it does not include standards for several security services (e.g., network security/intrusion detection systems and single sign-on) nor does it provide a rationale for excluding them. Further, the architecture does not explain how DHS will communicate with other extended architecture systems (e.g., DOD and Department of State) if those systems require certain standards to support DHS systems. However, the architecture does contain a list of several security standards that may be associated with security services.
A description of the protection mechanisms (e.g., firewalls and intrusion detection software) that will be implemented to secure the department's assets, including a description of the interrelationships among these protection mechanisms.			X	The architecture does not contain a complete list of the protection mechanisms needed, nor does it describe all these mechanisms and the interrelationships among them. For example, protection mechanisms have not been identified for monitoring and auditing activities, biometrics, control and protection, computer forensics tools, and computer intrusion and alarm. Moreover, the architecture indicates that security requirements have not been analyzed, thereby bringing into question the validity of the protection mechanisms identified. However, the architecture does contain a list of protection mechanisms, such as firewalls.

Source: GAO analysis of DHS data.

[a]A business assessment is a comprehensive analysis of the business, from both an internal and an external perspective, to reach conclusions on what requires strategic management focus and action.

[b]A gap analysis is the process of comparing an existing state with a desired state and determining what changes must be made to achieve the desired state.

[c]DHS defines a conceptual project as a project that is "derived from business activities and their associated applications and components. Conceptual projects are the highest level of categorization for a set of capabilities that can be combined and developed to satisfy a set of business requirements."

[d]A CURE (create, update, reference, and eliminate) matrix shows the business functions and applications that create, update, reference, and/or eliminate specific data elements, enabling the organization to develop applications.

[e]Business and operational rules define specific constraints for the data, such as security needs (e.g., confidentiality and accessibility of data) and actions that should or should not occur, such as updating or deleting data.

[f]Metadata are "data about data" that enable automation and consistent management and use of information, such as rules and standards.

[g]The technical reference model (TRM) describes (1) how technology is supporting the delivery of service components and (2) the relevant standards for implementing the technology. The TRM is a generally accepted representation of the generic components of an information system. It allows designers, developers, and users to agree on definitions, have a common understanding of the services to be provided, and identify and resolve issues affecting such requirements as interoperability, portability, reliability, scalability, and serviceability.

[h]Examples of enterprise services include application services, such as Web services, and collaboration services, such as instant messaging and video conferencing.

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

[j]Technical standards are strict rules and protocols governing how a given enterprise service is to be implemented.

Detailed Results of GAO's Analyses of Version 1.0 of DHS's Transition Plan

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
Analysis of the gaps between the baseline and the target architecture for business processes, information/data, and services/application systems to define missing and needed capabilities.		X		
A high-level strategy[a] for implementing the enterprise architecture. This strategy should include:				
• Specific time-phased milestones for acquiring and deploying systems.			X	The architecture does not have specific milestones for any actual projects that will deploy systems. However, the architecture does identify specific time-phased milestones for conceptual projects. For example, it notes that projects categorized as "Quick Hits" will be completed within 6 months, projects to consolidate duplicate systems within less than 2 years, and projects that optimize systems after 2 years.
• Performance metrics for determining whether business value is being achieved.			X	The architecture does not contain explicit metrics that can be implemented or assessed, but it recognizes the need for such metrics. However, the architecture does contain high-level metrics, such as "the percent of data/information shared across organizational units" that may be used to establish detailed metrics.
• Financial and nonfinancial resources needed to achieve the business transformation.		X		
• A listing of the legacy systems that will not be part of the "To Be" environment and the schedule for terminating these systems.		X		
• A description of the training strategy/approach that will be implemented to address the changes made to the business operations (processes and systems) to promote operational efficiency and effectiveness. This plan should also address any changes to existing policies and procedures that affect day-to-day operations, as well as resource needs (staffing and funding).		X		

(Continued From Previous Page)

Key architectural element	Element satisfied? Yes	No	Partially	Explanation of partially satisfied
• A list of the systems to be developed, acquired, or modified to achieve business needs and a description of the relationship between the system and the business need(s).		X		
A strategy for employing enterprise application integration (EAI) plans, methods, and tools to, for example, provide for efficiently reusing applications that already exist, concurrent with adding new applications and databases.			X	The architecture does not contain a strategy for employing EAI plans, methods, and tools, nor does it describe how EAI will be used to integrate legacy and future systems. However, it does list technologies, products, and standards for EAI. It also contains a vision for a service-oriented architecture [b] that may be developed into an EAI strategy.
A technical (systems, infrastructure, and data) migration plan that shows				
• the transition from legacy to replacement systems, including explicit sunset dates and intermediate systems that may be temporarily needed to sustain existing functionality during the transition period.		X		
• an analysis of system interdependencies, including the level of effort required to implement related systems in a sequenced portfolio of projects that includes milestones, time lines, costs, and capabilities.		X		
• a cost estimate for the initial phase(s) of the transition and a high-level cost projection for the transition to the target architecture.		X		
• A strategy that describes the architecture's governance and control structure and the integrated procedures, processes, and criteria (e.g., investment management and security) to be followed to ensure that the department's business transformation effort remains compliant with the architecture.			X	The architecture does not include an architecture governance and control structure and the integrated procedures, processes, and criteria to be followed. However, the architecture recognizes the need for a governance structure and contains a high-level discussion of governance that focuses on identifying the most critical governance issues and challenges, making general recommendations for dealing with these, and establishing the context in which appropriate managers, process owners, and subject matter experts will develop process details.

Source: GAO analysis of DHS data.

[a]Acquisition/business strategy is a plan or action for achieving a specific goal or result through contracting for software products and services.

[b]A service-oriented architecture is a collection of services that must communicate with each other. The communication might involve only simple data passing, or it could involve two or more services coordinating some activity. It requires a means for connecting the services to each other.

Comments from the Department of Homeland Security

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

JUL 23 2004

Mr. Randolph Hite
Director, Architecture and Systems Issues
Government Accountability Office
Washington, DC 20548

Re: GAO-04-777; Homeland Security: Efforts Underway to Develop Enterprise Architecture, But Much Work Remains, GAO Engagement Number 310272

Dear Mr. Hite:

Thank you for the opportunity to review the findings referenced in the draft report, GAO 04-777, Homeland Security: Efforts Underway to Develop Enterprise Architecture, But Much Work Remains.

GAO Recommendations

To assist DHS in developing a well defined architecture, GAO is making recommendations to the Secretary of Homeland Security that are aimed at improving the department's architecture development approach and the content of its architecture. GAO is also making a recommendation to the Director of OMB to clarify the expected relationship between agencies' enterprise architectures and the Federal Enterprise Architecture.

Response

The Department of Homeland Security (DHS) acknowledges that much work does remain to create a target enterprise architecture (EA) and transition plan to support business and information technology transformation; however, we take exception to several aspects of the report and its recommendations.

The DHS EA was evaluated against an unrealistic expectation that the first version would comprehensively address the full national scope of the homeland security enterprise. While this full scope is one of the highest priorities of the EA effort, the scope is long term and collaborative in nature. The report does not fully recognize the "blank sheet of paper" DHS had on March 2003 and the need with limited resources to guide DHS transformation and to engage our business community in this transformation.

It is important to recognize that the DHS EA was evaluated against criteria that has not yet been provided to the federal community, and was not available when Version 1.0 was being developed.

One of the most significant outcomes of Version 1.0 was the positioning of the Department to more actively engage with our business representatives from a strategic perspective; and thereby gain a greater appreciation of the need for and value of EA generally on the part of our senior and executive management. We accomplished this goal with Version 1.0, and intend to continuously improve the content and processes of our EA program over time.

The recommendations do not take into consideration limited resources. The report explicitly expects that DHS would have fully decomposed all aspects of all elements of an EA when in fact (given time, resources and the maturity of the department), we selectively focused on those areas of the EA that were most transformational in nature. It would also have been helpful to have received the recommendations in a prioritized framework so that the most cost-effective impact on transforming DHS as mandated by the establishment of the Department can be realized. Notwithstanding the absence of prioritization, the DHS EA program will ensure that the criteria are addressed to the extent possible (given resources and time) in Version 2. Aspects of the criteria that are not incorporated into Version 2 will be integrated into subsequent versions in the most cost effective and technically disciplined manner possible. Our response to each key architectural element under Appendix II, Detailed Results of GAO's Analyses of DHS's "To Be" Architecture and Appendix III, Detailed Results of GAO's Analyses of Version 1.0 of DHS's Transition Plan are enclosed.

We again thank you for the opportunity to provide comments on this report.

Sincerely,

Anna Dixon
Director, Bankcard Programs and GAO/OIG Liaison
Office of the Chief Financial Officer
U.S. Department of Homeland Security

Enclosure

See comment 2.

See comment 3.

APPNDX II	RECOMMENDATION	ISSUE	COMMENT
	BUSINESS		
1	A business assessment that includes the enterprise's purpose, scope (e.g., organizations, business areas, and internal and external stakeholders' concerns), limitations or assumptions, and methods.	Business Assessment	A high-level business assessment was included as the Business Model Overview document which describes and characterizes of the business model in terms of scope and methods.
2	A gap analysis that describes the target outcomes and shortfalls including strategic business issues, conclusions reached as a result of the analysis (e.g., missing capabilities), causal information, and rationales.	Gap Analysis	Concur, as additional information is collected for version 2.0 a more detailed gap analysis can be conducted. The primary intent of the EA version 1 was to describe the target business environment in terms of functions and data. A high-level assessment was conducted in order to develop the sequence diagram for the transition strategy which draws relationships between current investments and target functions/activities. If anything, rather than gaps there are/is a lot of redundancy in terms of investments.
3	A business strategy that describes the desired future state of the business, the specific objectives to be achieved, and the strategic direction that will be followed by the enterprise tot realize the desired future state.	Business Strategy:	The intent of the EA version 1.0 was to describe the business in terms of the top to rows of the Zachman framework. The EA Business strategy that describes the EA Program scope, objectives and strategic directions was not within the scope of the initial architecture description. In regards to the business strategy (mission, goals and objectives) for the Department that is defined in the DHS strategic plan. EA planning and implementation does not dictate the DHS strategic direction, mission and goals but rather is complementary to the strategic plan and brings that plan into life.

See comment 3.

See comment 4.

See comment 5.

3a	A vision statement that describes the business areas required strategic attention based on the gap analysis.	Vision Statement	See response to 3.
3b	A description of the business priorities and constraints, including their relationships to, at a minimum, applicable laws and regulations, executive orders, departmental policy, procedures, guidance, and audit reports.	Business Priorities & Constraints	Concur with comment. Version 2.0 will better define the business priorities and constraints, however mapping to applicable laws and regulations, executive orders, departmental policy, procedures, guidance, and audit reports will be a huge resource intensive exercise and will not be completed until a later date.
3c	A description of the scope of business change that is to occur to address identified gaps and realize the future desired business state. The scope of change, at a minimum, should identify expected changes to strategic goals, customers, suppliers, services, locations, and capabilities.	Scope of Business Change	The intent of the EA version 1.0 was to describe the business in terms of the top two rows of the Zachman framework. Once information is collected and vetted then the true analysis can begin. This is a critical step in understanding the long term changes that will need to be managed across the Department. Preliminary analysis will begin in the Summer of 2004.
3d	A description of the measurable strategic business objectives to be met to achieve the desired change.	Measurable Strategic Business Objectives	The intent of the EA version 1.0 was to describe the business terms in of the top two rows of the Zachman framework. The measurable business objectives are defined in the DHS strategic plan. The relationship between the EA business view and the strategic objectives is described in terms of related business activities to strategic objectives. In terms of the business objectives of the EA program, those are described in the Governance strategy and DHS EA Governance Plan, which is being implemented incrementally.

2

See comment 5.

See comment 4.

See comment 5.

See comment 6.

3e	A description of the measurable tactical business goals to be met to achieve the strategic objectives..	Measurable Tactical Business Goals	The intent of the EA version 1.0 was to describe the business terms in of the top two rows of the Zachman framework. The measurable business goals are defined in the DHS strategic plan. The relationship between the EA business view and the strategic goals is described in terms of related business activities to strategic objectives (associated with the strategic goal). In terms of the business goals of the EA program, those are described in the Governance strategy and DHS EA Governance Plan, which is being implemented incrementally.
3f	A listing of opportunities to unify and simplify systems or processes across the department, including their relationships to solutions that align with the strategic initiatives to be implemented to achieve strategic objectives and tactical goals.	Listing - Unify / Simplify Systems or Processes	The intent of the EA version 1.0 was to describe the business in terms of the top two rows of the Zachman framework. Once information is collected and vetted then the true analysis can begin. This is a critical step in understanding the long term changes that will need to be managed across the Department. More detailed analysis will be part of the transition plan analysis to be conducted during the Summer of 2004 and be delivered along with the EA V2 materials.
4	Common (standard and department wide) policies, procedures, and business and operational rules for consistent implementation of the architecture.	Standard Business Policies, Procedures, Rules	In terms of the business goals of the EA program, those are described in the Governance strategy and DHS EA Governance Plan, which is being implemented incrementally - to include EA policy, procedures and rules.
5	A description of key business processes and how they support the department's mission, including the organizational units responsible for performing the business processes and the locations where the business processes will be performed.	Key Business Processes	This statement is false. Key business processes are described in terms of the business function/activity descriptions contained in the business model. These functions/activities were derived from the Homeland Security Act of 2002 and the National Strategy for Homeland Security.

3

See comment 6.

See comments 4 and 5.

See comment 6.

See comment 6.

5a	this description should provide for the consistent alignment of : a) applicable federal laws, regulations, and guidance	Applicable Federal Laws, Regulations & Guidance	The functions/activities were derived from the National Strategy for Homeland Security and the Homeland Security Act of 2002. While these is not a specific mapping of the activities to each requirement additional resources are required to conduct more detailed analysis. See response to 3b.
5b	b) departmental policies, procedures, and guidance	Department Policies, Procedures & Guidance	The intent of the EA version 1.0 was to describe the business in terms of the top to rows of the Zachman framework. Alignment to department policy, procedures and guidance is described in the governance strategy and DHS EA Governance Plan, which is being implemented incrementally.
5c	c) operational activities	Operational Activities	This statement is false. Operational activities are described in terms of the business function/activity descriptions contained in the business model. These functions/activities were derived from the Homeland Security Act of 2002 and the National Strategy for Homeland Security.
5d	d) organizational roles	Organizational Roles	DHS organizations are attributed to each of the business activities as appropriate. While the specific roles are not defined, the information collected provides a starting point to understanding the relationship between the organizational elements and the functions they perform. This will be further analyzed to better define the organizational roles within the Department. Version 2.0 provides an organizational description in terms of mission and function. This information will be used in that analysis.

4

See comment 6.

See comments 4 and 5.

See comments 4, 5, and 7.

See comments 4, 5, and 7.

5e	e) operational events and information	Operational Events	The intent of the EA version 1.0 was to describe the business in terms of the top two rows of the Zachman framework. Part of that information is indeed key business events. Future work is planned involving key DHS internal stakeholders in defining and describing key events and the relationship of those events to the business functions/activities.
6	A description of the operational management processes to ensure that the department's business transformation effort remains compliant with the business rules for fault, performance, security, configuration, and account management.	Operational Management Processes	The intent of the EA version 1.0 was to describe the business in terms of the top to rows of the Zachman framework. Alignment to organizational management processes is described in the governance strategy and DHS EA Governance Plan, which is being implemented incrementally.
7	A description of the organizational approach (processes and organizational structure) for communications and interactions among business lines and program areas for:	Organizational Communications Processes and Structure:	The intent of the EA version 1.0 was to describe the business in terms of the top to rows of the Zachman framework. The organizational approach to the EA processes and organizational structure for communications and interactions among business lines and program areas is described in the governance strategy, DHS EA Governance Plan, and DHS EA Communications Plan - which is being implemented incrementally.
7a	a) management reporting	Management Reporting	See response to 7. If the proper information is collected during the EA Planning phase analysis can be conducted inform management of the most effective methods of management reporting. The EA Planning team has only considered management reporting in terms of the EA program.

5

See comments 4, 6, and 8.

See comment 5.

7b	b) operational functions	Operational Functions	The intent of the EA version 1.0 was to describe the business in terms of the top to rows of the Zachman framework. In terms of the management structure of the Department, that information was provided and used from the DHS organizational chart provided to the EA team. Business functions/activities were attributed by organizations that perform those functions. This information (once more detailed information can be collected) can be used to allow management to make informed decisions and understand the impact to the organization of those decisions.
7c	c) architectural development and use (i.e., how to develop the architecture description, implement the architecture, and govern/manage the development and implementation of the architecture.)	Architectural Development & Use	Architecture development and use is described in the Governance strategy and DHS EA Governance Plan, which is being implemented incrementally.
	PERFORMANCE		

6

8	A description of the processes for establishing, measuring, tracking, evaluating, and predicting business performance regarding business functions, baseline data, and service levels.	Process - Business Performance Metrics	Version 2.0 of the EA will provide an enhanced business model that will be a solid foundation for establishing performance measures. The individual business activities identified in Version 2.0 should each have performance measures and metrics, baseline data, and service levels associated with them. The overall process for developing this performance information needs to be defined by the business area and performance measurement staff of DHS. This is a substantial process that must involve a wide range of DHS components working together. To the extent these processes are developed, they will be referenced and/or included in Version 2.0. The conceptual project and business activity related to this area in Version 1.0 will be expanded upon in Version 2.0 by the DHS EA Project team.
9	A description of measurable business goals and outcomes for business products and services, including strategic and tactical objectives.	Goals & Outcomes - Business Products & Services	Version 2 of the EA will provide an enhanced business model that will be a solid foundation for establishing business goals and outcomes. The individual business activities or value chain areas identified in Version 2 can each have measurable goals and outcomes associated with them. The development of the specific quantitative goals and outcomes needs to be done by each business area and performance measurement staff of DHS. To the extent these goals and outcomes are developed, they will be referenced or included in Version 2. The description of customer focused, measurable business goals included in Version 1 will be expanded upon in Version 2.

7

10	A description of measurable technical goals and outcomes for managing technology products and services for the "To Be" architecture that enable the achievement of business goals and outcomes.	Goals & Outcomes - Technology Products	Version 2.0 of the EA will provide an improved foundation for describing technical goals and outcomes. The technology-related quantitative goals and outcomes need to be defined by the CIO and performance measurement staff of DHS. To the extent these goals and outcomes are developed, they will be referenced and/or included in Version 2.0. The performance measures for measuring technology and the technology management conceptual projects included in Version 1.0 will be expanded upon in Version 2.0.
	INFORMATION / DATA		
11	A description of data management policies, procedures, processes, and tools (e.g., CURE matrix) for analyzing, designing, building, and maintaining databases in an enterprise architected environment.	Data Management Policies, Procedures, Processes & Tools	The intent and scope of the version 1.0 effort was to collect the terms and facts that represent the common nouns (data objects) of the business. The data management policy, practices, processes and tools will be defined in the data management governance documents at a later date. The CURE matrix is a data usage planning tool, in that is provides high-level relationships between the business functions/activities and how those functions/activities may act on a particular data object. This tool is instrumental in the application/component architecture definition phase. This version of DHS EA data architecture represents conceptual data model and it was not intended to define data mgmt policies, procedures, processes and tools at this level. Acceptance criteria did not identify this as a requirement.

8

See comment 9.

12	A description of the business and operational rules for data standardization to ensure data consistency, integrity, and accuracy, such as business and security rules that govern address to, maintenance of, and use of data.	Data Standardization - Business & Operational Rules	The intent and scope of the version 1.0 effort was to collect the terms and facts that represent the common nouns (data objects) of the business. The data management policy, practices (including business and security rules), processes and tools will be defined at a later date as the EA plan is refined and the architecture matures.
13	A data dictionary, which is a repository of standard data definitions for applications.	Data Dictionary	
14	A conceptual data model that describes the fundamental things/objects (e.g., business or tourist visas, shipping manifests) that make up the business, without regard for how they will be physically stored A conceptual data model contains the content needed to derive facts about the business and to facilitate the creation of business rules. It represents the consolidated structure of business objects to be used by business applications.	Conceptual Data Model	This is not accurate. A conceptual data model was delivered consisting of a list of primary data object definitions and characteristics, associated business subject areas and even some high-level subject area diagrams. Conceptual data models are usually abstract, however necessary to begin to form the underlying structure of the business needs. The intent and scope of the version 1 effort was to collect the terms and facts that represent the common nouns (data objects) of the business to understand the types of information of which the department has a need to collect and store. The purpose of conceptual data model is to provide common vocabulary for the enterprise and to depict fundamental structure of the enterprise in terms of data. It was not intended to provide rules for building databases.

9

15	A logical database model that provides (1) a normalized (I/e/, non-redundant) data structure that supports information flows and (2) the basis for developing the schemes for designing, building, and maintaining physical databases.	Logical Database Model	The main focus of the EA version 1.0 effort was to describe the DHS enterprise in terms of the top two rows of the Zachman framework. Clearly, a logical data model does not fall within that scope, but rather a logical data model would be defined by a "solution" architecture using the structure provided and defined by the conceptual data model. That is ensuring that information and data used by a solution is reflective within the enterprise conceptual data model. There was not our objective to develop logical data model at this point .
16	A metadata model that specifies the rules and standards for representing data (e.g., data formats) and accessing information (e.g., data protocols) according to a documented business context that is complete, consistent, and practical.	Metadata Model	The intent and scope of the version 1 effort was to collect the terms and facts that represent the common nouns (data objects) of the business. The data management policy, practices, processes (including rules and standards for representing data) and tools will be defined in the data management governance documents at a later date.
17	A description of the information flows and relationships among organizational units, business operations, and system elements.	Information Flows & Relationships	The main focus of the EA version 1.0 effort was to describe the DHS enterprise in terms of the top two rows of the Zachman framework. As the EA Plan continues to evolve information flows will created to describe the information flow among organizational entities as well as with external entities.
	SERVICES / APPLICATIONS		
18	A description of the services and their relationships to key end-user services to be provided by the application systems.	Services - Key End Users	The description of the Notional Application Architecture describes applications in terms of the user workflows they enable.
18a		Specify End-User Services by Application Systems	While it is not specifically mentioned, these applications were derived from the usage of business functions by user classes, as mapped in the business model. This relationship of user to business function to application will be much more apparent in version 2.

10

18b		Inconsistency User Services / Application Systems	The consumption diagram for the Communication Management Application specifically calls out the consumption of Email services for managing some of the correspondence.
19	A list of application systems (acquisition/development and production portfolio) and their relative importance to achieving the department's vision, based on business value and technical performance.	Application Systems - Relevance to DHS Vision	The Application and Component Architectures indirectly link to the Value Chain, via the business functions. Relative importance should be noted via this linkage. However, Applications will cross both value chain and organizational boundaries. This is the basis of reuse that has been built into the architecture. Version 2.0 of the Application and Component Architecture should have more detail available to specify which organizations will be able to use each component. This will be based on the mapping of Components to the Business Functions they enable. Business Functions are then mapped to the organizations (both internal and external) that perform them.
20	A description of the policies, procedures, processes, and tools for selecting, controlling, and evaluating application systems to enable effective IT investment management.	Application Systems - IT Investment Management	The notional application and component architecture describes the categories of information systems required to execute the enterprise mission. The GAO report is correct in that it does not describe the governance for selecting, controlling, and evaluating systems to enable investment management. This is an issue that should be addressed with governance.
21	A description of the enterprise application systems and system components and their interfaces.	Application Systems, System Components and Interfaces	

See comment 10.

22	A description of the system development lifecycle process for application development or acquisition and the integration of the process with the architecture, including policies, procedures, and architectural techniques and methods for acquiring systems throughout their lifecycles. The common technical approach should also describe the process for integrating legacy systems with the systems to be developed/acquired.	System Development Life Cycle Process - App. Dev.	The business functions and their interaction with data and user roles requires much further decomposition before we can begin to describe all of the system development life cycle processes, policies, procedures, and architectural techniques. At this stage of the architecture, we have defined the need for types of software to be required by the enterprise. Once the models are decomposed into specifications, then it would be more appropriate to define how the software will be provisioned.
	TECHNICAL		
23	A list of infrastructure systems and a description of the systems' hardware and software infrastructure components. The description should also reflect the system's relative importance to achieving the department's vision based on constraints, business value, and technical performance.	Infrastructure Systems, Hardware & Software Components	"One DHS" has become a real initiative sponsored by the Infrastructure Services section of the Office of the CIO. "One DHS" is creating the Roadmap to One DHS Infrastructure which will detail out the list of infrastructure systems (including descriptions, hardware and software components, and value characteristics) which will support DHS moving forward. The DHS EA effort is coordinating with "One DHS" in order to incorporate this information into the architecture. We require timely response from the Infrastructure Services unit for this information as it is surfaced through the "One DHS" activities. Resource constraints within Infrastructure Services has negatively affected this timely response.
24	A description of the policies, procedures, processes, and tools for selecting, controlling, and evaluating infrastructure systems to enable effective IT investment management..	Policies, Procedures, Processes, Tools - Infrastructure Systems Evaluation	Governance processes, procedures and policies have been adopted to guide decision making as to architectural alignment of proposed technology investments. These are being described within V2.0 of the DHS EA.

12

25	A description of the technical reference model (TRM) that describes the enterprise infrastructure services, including specific details regarding the functionality and capabilities that these services will provide to enable the development of application systems.	TRM - Description Infrastructure Services	Governance processes, procedures and policies have been adopted to guide the evolution and maturation of the DHS EA TRM. Focus is rapidly moving from as-is descriptions to to-be targets. These are being described within V2.0 of the DHS EA.
26	A description in the TRM that identifies and describes (a) the technical standards to be implemented for each enterprise service and	TRM - Technical Standards for Enterprise Service	The V2.0 DHS EA TRM contains both structure and content which support the to-be target infrastructure services. These items are under governance processes, procedures and policies at a DHS enterprise level. These are being described within V2.0 of the DHS EA.
26a	(b) the anticipated life cycle of each standard.	TRM - Life Cycle of each Standard	The anticipated lifecycle of the above referenced technical standards is incorporated into v2.0 of the DHS EA TRM. The content of the lifecycle information is under governance and will be described within the V2.0 DHS EA.
27	A description of the physical IT infrastructure needed to design and acquire systems, including the relationships among hardware, software, and communications devices.	Physical IT Infrastructure Description	The "One DHS" initiative is defining the physical infrastructure components required to support a DHS to-be target. DHS EA is coordinating with "One DHS" in order to incorporate these definitions, descriptions and requirements into the DHS EA. DHS Infrastructure Services resource constraints limit the effectiveness of our coordination. Information Sharing requirements and solution concepts are included within V2.0 of the DHS EA.

See comment 10.

13

See comment 10.

28	Common policies and procedures for developing infrastructure systems throughout their life cycles, including requirements management, design, implementation, testing, deployment, operations, and maintenance. These policies and procedures should also address how the applications will be integrated, including legacy systems.	Policies & Procedures - Developing Infrastructure Systems	Common policies and procedures for life cycle development of infrastructure capabilities are being developed through "One DHS". DHS EA is coordinating with "One DHS" in order to incorporate these items within the DHS EA. Applications integration (including legacy) is addressed in the DHS EA through a combination of Services/Applications, Technical and the DHS EA Transition Plan. These perspectives come to bear on every investment guided by the DHS EA. Concepts of how this would work are described within V2.0 of the DHS EA.
	SECURITY		Currently developing a draft security document that addresses these issues.
29	A description or the policies, procedures, goals, strategies, principals, and requirements relevant to information assurance and security and how they (the policies, procedures, goals, strategies, and requirements) align and integrate with other elements of the architecture (e.g., security services).	Policies & Procedures - Information Assurance	Concur. Policies and procedures for information assurance and security are not contained in the EA. The Department (CISO) is developing policies and procedures for information assurance and security. Currently developing security goals, underlying principles, strategies, implementation approaches, and standards. Policies and procedures will be referenced as part of the requirements.
30	Definitions of terms related to security and information assurance.	Definitions of Terms - Information Assurance	Concur. The conceptual EA (V1.0) presented the outline of a security architecture approach and indicated some of the components from which it will be constructed. The Security Architecture under development will define all terms included. The Definitions of Terms for Information Assurance will be developed and will align with commonly accepted terminology.

14

31	A listing of accountable organizations and their respective responsibilities for implementing enterprise security services It is important to show organizational relationships in an operational view because they illustrate fundamental roles (e.g., who conducts operational activities) and management relationships (e.g., what is the command structure or relationship to other key players) and how these influence the operational nodes.	List Organizations - Enterprise Security Services	Concur. A listing of organizations and roles and responsibilities will be provided in the Security Architecture under development. Currently developing the security organization and a high level diagram will be completed for V2.0.
32	A description of operational security rules that are derived from security policies.	Operational Security Rules	Concur. A listing of operational security rules derived from security policies will be provided in the Security Architecture under development. There is a need for clarification on requirements and specific details from the Department in order to complete this effort.
33	A description of enterprise security infrastructure services (e.g., identification and authentication) that will be needed to protect the department's assets, and the relationship of these services to protective mechanisms.	Enterprise Security Infrastructure Services	The purpose of the conceptual EA (V1.0) is to provide an outline of the elements of the EA that require further detail to be provided in subsequent versions. The EA V1.0 does indicate the security infrastructure services required, but does not indicate the mechanisms by which they will be implemented. These have been identified and will be incorporated in V2.0.
34	A description of the security standards to be implemented for each enterprise service. These standards should be derived from security requirements. This description should also address how these services will align and integrate with other elements of the architecture (e.g., security policies and requirements).	Security Standards for Each Service	Concur. The EA (V1.0) does not contain a complete list of standards (security and other). Development of standards is underway and will be reflected in subsequent versions. Will identify and incorporate general requirements (such as FIPS); there is a need to address the organization specific requirements (such as DoD etc) that will require cooperative work and input from the organizations.

15

See comment 11.

35	A description of the protection mechanisms (e.g., firewalls and intrusion detection software) that will be implemented to secure the department's assets, including a description of the interrelationships among these protection mechanisms.	Protection Mechanisms to Secure Assets	Concur. The EA (V1.0) does not contain a list and descriptions of protective mechanisms to be employed. The EA V1.0 is intended as an outline EA to indicate the areas where further detail is required and is under development. A high level analysis for assessment of Protection Mechanisms to Secure Assets is underway.
APPNDX III			
36	Analysis of the gaps between the baseline and the target architecture for business processes, information/data and services/application systems to define missing and needed capabilities.	Gap Analysis - Baseline and Target Architecture	Partial analysis provided. Version 1.0 provided legacy systems by mission area and provided a sequensing plan that could be corrolated to those same mission areas. Problems identified with the legacy systems are addressed by the target. Further Gap analysis was planned for during the Rationalize phase (first 6 months) of the Transition Plan. Each conceptual project contains a sub-project called As-Is/Target Gap analysis. This sub-project identifies target requirements and determines the gap between current capabilities and target requirements. Results from the Gap analysis plan indicate: - Existing applications or 300s that can be used to satisfy target requirements - Portions of an existing applications or 300 can be used to satisfy target requirements - No existing application or 300 can be used to satisfy a target requirement - A portion of an existing application or 300 can be used during an interim time period to satisfy a target requirement
37	A high-level strategy for implementing the enterprise architecture.	High Level Strategy - Implementing EA	

16

See comments 11 and 12.

See comments 11, 12, and 13.

See comment 14.

See comment 15.

37a	Specific time-phased milestones for acquiring and deploying systems.	Time-phased Milestones	Concur.
37b	Performance metrics for determining whether business value is being achieved	Performance Metrics	Concur.
37c	Financial and non-financial resources needed to achieve the business transformations.	Financial & Non-financial Resources	Partial analysis provided. Version 1.0 provided a correlation between conceptual projects and the associated already approved 300s. The Gap Analysis Projects (Within Each Conceptual Project) Will Determine The Extent To Which Current 300s Can Be Used
37d	A listing of the legacy systems that will not be part of the "To Be" environment and the schedule for terminating these systems.	Listing - legacy systems to be terminated	Partial analysis provided. The existing and planned systems can be correlated to a swim lane in version 1.0. All existing systems will be phased out eventually or built upon as part of the target architecture. The Gap analysis project in each swim lane will focus on reviewing 300s that might meet specific target requirements and determine a specific action plan.
37e	A description of the training strategy/approach that will be implemented to address the changes made to the business operations (processes and systems) to promote operational efficiency and effectiveness. This plan should also address any changes to existing policies and procedures that affect day-to-day operations, as well as resource needs (staffing and funding).	Training Strategy for changes - business operations and processes	Partial Analysis provided Changed management and training was planned for as a part of each conceptual project. Change Management (People) Activities: These Sub-projects Seek To Improve Organizational Collaboration And Cooperation. Some Of These Projects May Result In Organizational Changes, Some In New Training Programs, And Some In Improved Procedures.
37f	A list of the systems to be developed, acquired, or modified to achieve business needs and a description of the relationship between the system and the business need(s).	List of Systems to be developed, acquired, modified	Partial Analysis Provided. A list of Target applications was provided and the concept

17

See comment 16.

38	A strategy for employing enterprise application integrations (EAI) plans, methods, and tools to, for example, provide for efficiently reusing applications that already exist, concurrent with adding new applications and databases.	Strategy - Enterprise Architecture Integration Plans	Concur with Partially Satisfied. There is a Enterprise Application Integration (EAI) component development that is planned as part of the Governance conceptual project.
39	A technical (systems, infrastructure, and data) migration plan that shows:	A Technical Migration Plan	
39a	a) the transition from legacy to replacement systems, including explicit sunset dates and intermediate systems that may be temporarily needed to sustain existing functionality during the transition period.	Transition from legacy to replacement systems	Version 2.0 will show the transition from legacy to replacement systems
39b	b) an analysis of system interdependencies, including the level of effort required to implement related systems in a sequenced portfolio of projects that includes milestones, timelines costs and capabilities.	Analysis - system Interdependencies	Partial Analysis provided - dependencies between components and conceptual projects are shown on the sequencing diagram.
39c	c) a cost estimate for the initial phase(s) of the transition and high-level cost projection for the transition to the target architecture.	Cost Estimate - Initial Phase	Version 2.0 will show the cost and schedule of projects
40	A strategy that describes the architecture's governance and control structure and the integrated procedures processes and criteria (e.g., investment management and security) to be followed to ensure that the department's business transformation effort remains compliant with the architecture.	Strategy - architecture's governance and control structure	Concur with the Partially Satisfied assessment.

18

The following are GAO's comments on the Department of Homeland Security's (DHS) letter dated July 23, 2004.

GAO Comments

1. See the "Agency Comments and Our Evaluation" section of this report.

2. We agree that Version 1.0 included a high-level (or overview) business model that offered some descriptive information on weaknesses, such as potential areas of inefficiencies or overlaps in current departmental business functions and technology. However, the underlying business assessment that would form the basis for a clear statement of the enterprise's purpose, scope, limitations, assumptions, and methods for successful business transformation was not present, and DHS provided no evidence that such an assessment had been performed. For example, for the areas that the business model overview identified as potential areas of inefficiency or overlap, the architecture did not provide the supporting analysis. The architecture also did not provide a time frame for completing such an assessment or state that one would be performed. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our finding.

3. We acknowledge the department's comment that the business strategy and vision statement were not within the scope of the initial architecture description. However, we note that this comment is inconsistent with DHS's intent to describe the top two rows of the Zachman framework, because these rows include this information. Moreover, as stated in our report, best practices require that the architecture be based on the business strategy and states that to do otherwise negatively affects the architecture's utility and makes it unlikely that changes to existing operations and systems will provide for optimum mission performance and satisfaction of stakeholders' needs. In addition, while we do not question that the business strategy and vision statement are included in DHS's strategic plan, we did not evaluate this plan because it was issued 5 months after the approval of Version 1.0. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

4. As stated in the report, we do not question the department's intent for Version 1.0 of the architecture or whether these goals have been achieved. However, our analysis shows that important architecture

artifacts that would be expected to be included in this version and that are associated with the top two rows of the Zachman framework were not included in the architecture description.

5. We acknowledge the department's comment that Version 1.0 of the architecture did not contain measurable strategic business objectives or tactical business goals, as evidenced by our finding that this information was missing. In addition, while we do not question that this information is included in DHS's strategic plan, we would note that we did not evaluate this plan because it was issued 5 months after the approval of Version 1.0. With respect to the governance strategy and plan, the former outlined the steps to be taken to develop such a strategy, and the latter was not contained within Version 1.0, nor was it provided separately. Further, as previously noted, we do not question the intent of Version 1.0. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

6. We disagree. While we acknowledge that there are high-level business functions and activities in the business model, the model did not define business processes. Business process descriptions have a definitive beginning and end and reflect the interrelationships among business functions and activities. The functions and activities described in Version 1.0 had not been decomposed to a sufficient level of operational detail to describe routine tasks (e.g., develop mitigation strategies to minimize the impact of the threat). Further, when we concluded our analysis and shared our findings with architecture officials and supporting contractor personnel, they agreed with the criteria and with our findings.

7. Version 1.0 of the architecture did not include a communications plan, nor was such a plan provided separately. However, we do agree that effective management reporting will depend on DHS's ability to collect the right information for the architecture program.

8. The organizational chart referred to in this comment was not provided to GAO.

9. We disagree. While we acknowledge that the architecture contains a high-level or abstract conceptual data model, we found that the model lacked the information for the business owner's view of data and for the creation of a conceptual data model that can be used to develop the

logical database model as required by the Zachman framework, which DHS has acknowledged that it is following to develop its architecture. Specifically, this would require that the conceptual data model (1) include concrete business objects, (2) enable facts about the business to be derived, and (3) facilitate the development and validation of business rules. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with the criteria and our findings.

10. The focus of our review was the content of Version 1.0 of the architecture. We did not evaluate the "OneDHS" initiative as part of this effort because it was identified in the architecture as a conceptual project.

11. We disagree. While we acknowledge that the architecture indicated the need to perform project-specific gap analyses, these analyses were not included in Version 1.0, and DHS did not provide any evidence that such analyses had been performed. In addition, the department did not provide a time frame for completing them. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

12. We disagree. While we acknowledge that conceptual projects were linked with proposed IT investments (i.e., exhibit 300s), the architecture did not show the correlation among the projects and the potential investments. To show this correlation, DHS would have needed to reflect the extent to which the identified business need—which should be based on a gap analysis—would be addressed by the proposed investment, and this explanation would be documented within the architecture. However, the architecture did not contain this information or a time frame for when it would be provided. The architecture also did not include information on the approval status of these proposed investments. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

13. We disagree. Version 1.0 of the DHS architecture does not provide sufficient information to differentiate between existing and new systems. In addition, the architecture did not include an analysis that identified existing systems that would be terminated. Further, when we

concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

14. We disagree. The architecture does not contain detailed training approaches, strategies, or plans. Instead, the architecture contains high-level briefings that refer to planned activities to determine the needs for training based on anticipated changes. These needs, once identified, may be used to develop a business-specific plan for change management and training. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

15. We disagree. While we acknowledge that the architecture listed the names of both existing systems and several systems under development, it did not identify which of these systems would be developed, modified, acquired, and/or used as intermediate systems until the target system has been deployed to meet specific future business needs. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

16. We disagree. We acknowledge that the architecture included a sequencing diagram that graphically associated the components and the conceptual projects. However, the architecture did not provide either an explanation of the graphically depicted relationships or an analysis of the interdependencies. DHS also did not provide evidence that such an analysis had been performed. Further, when we concluded our analysis and shared our findings with senior DHS architecture officials and supporting contractor personnel, they agreed with our findings.

GAO Contact and Staff Acknowledgments

GAO Contact

Cynthia Jackson, (202) 512-5086

Staff Acknowledgments

Staff who made key contributions to this report were Joseph Cruz, Joanne Fiorino, Anh Le, Randolph Tekeley, and William Wadsworth.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

PRINTED ON RECYCLED PAPER

United States
Government Accountability Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00