United States Government Accountability Office

GAO

Report to Congressional Committees

May 2007

HOMELAND SECURITY

DHS Enterprise Architecture Continues to Evolve but Improvements Needed

GAO-07-564

May 2007

HOMELAND SECURITY

DHS Enterprise Architecture Continues to Evolve but Improvements Needed

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-564, a report to congressional committees

Why GAO Did This Study

GAO designated the transformation of the Department of Homeland Security (DHS) as high risk in 2003, and it continues to do so today. One essential tool for facilitating organizational transformation is an enterprise architecture (EA)—a corporate blueprint that serves as an authoritative frame of reference for information technology investment decision making. The Congress required DHS to submit a report that includes its EA and a capital investment plan for implementing it. The Congress also required that GAO review the report. In June 2006, DHS submitted this report to the Congress. GAO's objective was to assess the status of the EA, referred to as DHS EA 2006, and the plan for implementing it. To meet this objective, GAO analyzed architectural documents relative to its prior recommendations; evaluated stakeholder comments and the process used to obtain them; and analyzed the implementation plan against relevant guidance.

What GAO Recommends

GAO is making recommendations to DHS for tracing the implementation of prior GAO recommendations to EA content, and for more effectively soliciting and addressing EA stakeholder comments. DHS agreed to trace GAO's recommendations, but stated that it already adequately deals with stakeholder comments. GAO does not agree for reasons cited in this report, and thus stands by its recommendation.

www.gao.gov/cgi-bin/getrpt?GAO-07-564.

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

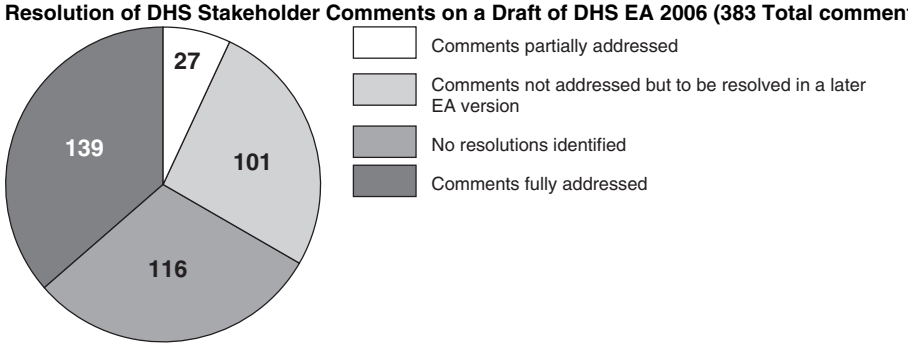
DHS EA 2006 has evolved beyond prior versions, but missing architecture content and limited stakeholder input constrain its usability. While the architecture partially addresses each of the prior GAO recommendations concerning the content of DHS's architecture, the full depth and breadth of EA content that the recommendations solicited is still missing. For example, GAO recommended that DHS use, among other things, an analysis of the gaps between the current ("as-is") and future ("to-be") states of the architecture to define missing and needed capabilities and form the basis for its transition plan. However, DHS EA 2006 does not include a transition plan and it does not include any evidence of a gap analysis.

In addition, department stakeholders, including component organizations and the department's EA support contractor, provided a range of comments relative to the completeness, internal consistency, and understandability of a draft of DHS EA 2006, but the majority of the comments were not addressed (see fig.). Moreover, key stakeholders, such as the Coast Guard and the Transportation Security Administration, did not comment on the draft. GAO found that the extent of stakeholder participation was limited because the approach EA officials used to solicit input did not clearly define the type of information being requested and did not provide sufficient time for responding.

Furthermore, DHS's capital investment plan for implementing its architecture is not based on a transition plan and is missing key information technology (IT) investments. Thus, the plan does not provide a comprehensive roadmap for transitioning the department to a target architectural state. Also, the plan does not account for all of DHS's planned investments in IT (excluding about $2.5 billion in planned IT investments).

Without an architecture that is complete, internally consistent, and understandable, the usability of the DHS's EA is diminished, which in turn limits the department's ability to guide and constrain IT investments in a way that promotes interoperability, reduces overlap and duplication, and optimizes overall mission performance.

Resolution of DHS Stakeholder Comments on a Draft of DHS EA 2006 (383 Total comments)



Source: GAO analysis of DHS data.

Contents

Abbreviations

CBP	Customs and Border Protection
CIO	chief information officer
CURE	create, update, reference, and eliminate
DHS	Department of Homeland Security
EA	enterprise architecture
EAMMF	Enterprise Architecture Management Maturity Framework
FEMA	Federal Emergency Management Agency
ICE	Immigration and Customs Enforcement
IT	information technology
OMB	Office of Management and Budget
TRM	technical reference model
TSA	Transportation Security Administration
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
USSS	United States Secret Service

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 9, 2007

The Honorable Robert C. Byrd
Chairman
The Honorable Thad Cochran
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable David E. Price
Chairman
The Honorable Harold Rogers
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

Information technology (IT) is a critical tool in the Department of Homeland Security's (DHS) quest to transform 22 diverse and distinct agencies into one cohesive, high-performing department. Because of the importance of this transformation and the magnitude of the associated challenges, we designated the department's implementation and transformation as a high-risk undertaking in 2003.[1] In 2003 and in 2004, we reported that DHS needed to, among other things, develop and implement an enterprise architecture (EA)—a corporate blueprint that serves as an authoritative frame of reference to guide and constrain IT investment decision making, promoting interoperability, minimizing wasteful duplication and redundancy, and optimizing departmentwide mission performance.[2]

[1]GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003); *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

[2]GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: Aug. 27, 2003) and *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*, GAO-04-702 (Washington, D.C.: Aug. 27, 2004).

Recognizing the importance that an EA plays in effectively leveraging IT for organizational transformation, DHS issued an initial version of its architecture in September 2003. Following our review of this EA and recommendations for its improvement,[3] the department issued a second version in October 2004. The DHS Appropriations Act of 2006 required the department's chief information officer (CIO) to submit to Congress a report that includes, among other things, an EA and a capital investment plan for implementing the architecture.[4] It also required GAO to review the report. On June 16, 2006, the CIO submitted its report, which included the third version of the department's EA and a plan for implementing it, which DHS referred to as DHS EA 2006 and *Capital Investment Plan for Implementing the DHS Enterprise Architecture*.

Our objective was to assess the status of DHS EA 2006, including the capital investment plan for implementing it. On February 28, 2007, we briefed your staffs on the results of our review, which included sensitive information. This report transmits the slides from that briefing, with sensitive information removed. These slides, along with our scope and methodology, are included as appendix I.

DHS EA 2006 Has Evolved beyond Prior Versions, but Missing Architecture Content and Limited Stakeholder Input Constrain Its Usability

DHS EA 2006 partially addresses the content shortcomings in earlier versions of the department's architecture, which we had reported on and made recommendations to correct. However, the full depth and breadth of EA content that our 41 recommendations provided for is not reflected in DHS EA 2006. For example, we recommended that the architecture include a data dictionary, which is a repository of standard definitions of key terms. In response, DHS EA 2006 provides a data dictionary, but it does not include definitions of all key terms (e.g., first responder). We also recommended that DHS base its EA transition plan on, among other things, an analysis of the gaps between the current ("as-is") and future ("to-be") states of the architecture to define missing and needed capabilities.[5] However, DHS EA 2006 does not include a transition plan,

[3]GAO, *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, GAO-04-777 (Washington, D.C.: Aug. 6, 2004).

[4]The act also required DHS's CIO report to include a description of the IT capital planning and investment control (CPIC) process and an IT human capital plan.

[5]An EA describes how an entity currently operates (the "as-is" architecture) and how it plans to operate in the future (the "to-be" architecture); it also includes a plan for making that transition (the transition plan).

and it does not include any evidence of a gap analysis—a comparison of the "as-is" and "to-be" architectures to identify capability differences.

Moreover, this version of the architecture does not address the majority of the 383 comments made on a draft of it by DHS stakeholders, including component organizations and the department's EA support contractor. For example, Immigration and Customs Enforcement commented that the inputs it provided had not been incorporated, represented, or otherwise accommodated in any way. Of the comments, 139 were categorized as fully addressed, 27 as partially addressed, 101 as not addressed but to be resolved in a later EA version. The remaining 116 had no resolutions specified. In general, comments were raised about the architecture's completeness, internal consistency, and understandability. In addition, concerns were raised about the architecture's usability as a departmental frame of reference for informing IT investment decisions.

In addition, the approach DHS used in soliciting comments did not clearly define the type of information requested and did not provide sufficient time for detailed responses. Also, the extent to which comments were obtained was limited. For example, key stakeholders, such as the Coast Guard and Transportation Security Administration, chose to not comment on a draft of DHS EA 2006.

Lastly, DHS's capital investment plan for implementing its architecture is not based on an EA transition plan and is missing key IT investments. For example, the plan does not account for all of DHS's planned investments in IT nor does it include information on certain major IT capital investments.

Conclusions

DHS's approach to developing its EA through incremental releases or versions is reasonable, given the size and complexity of the department and the volumes of information needed to produce a complete, understandable, and usable architecture. As the department's third version of its EA, DHS EA 2006 is an improvement over prior versions, as evidenced by it at least partially addressing our prior recommendations. Moreover, DHS EA 2006 is partially responsive to stakeholder comments on a draft of it.

Nevertheless, DHS EA 2006 is still not sufficiently complete and usable, given those aspects of our recommendations that it did not fully address the range of stakeholder comments that have not been resolved and the limitations of the capital investment plan. Given the critical role that DHS's

EA should play in the department's transformation efforts, which we have identified as a high-risk undertaking, it is important for DHS to fully address both our existing recommendations and stakeholder comments on incremental versions of its architecture.

Finally, with regard to stakeholder comments, it is also important for DHS to ensure that it devotes sufficient time and adopts an effective approach to obtaining stakeholder comments on future versions. If it does not, the chances of developing a well-defined EA that is accepted and usable will be diminished.

Recommendations for Executive Action

To ensure that DHS fully implements our prior EA recommendations and effectively solicits and addresses stakeholder comments on incremental versions of its EA, we recommend that the Secretary of Homeland Security direct the department's CIO to take the following two actions:

- Include in future versions of the department's EA a traceability matrix that explicitly maps EA content to our recommendations in sufficient detail to demonstrate their implementation, and
- Ensure that future efforts to solicit stakeholder comments on the department's EA employ an effective approach that includes clearly defining the type of information requested and allowing sufficient time for obtaining and responding to these comments.

We are not making recommendations for addressing limitations in the department's capital investment plan for implementing its EA because our existing recommendations for an EA transition plan address such limitations.

Agency Comments and Our Evaluation

In DHS's written comments on a draft of this report, signed by the Director, Departmental GAO/OIG Liaison Office, and reprinted in appendix II, the department stated that the fourth release of its EA (referred to as HLS EA 2007) addresses many of the issues that our report identifies. In addition, DHS agreed to include in future EA releases a traceability matrix that explicitly maps its EA content to our recommendations, adding that this recommended tool will allow DHS to better track progress.

However, DHS commented that its current approach to soliciting architecture stakeholders' input is adequate, noting that this approach

provides stakeholders with unlimited opportunity to comment and observing that its receipt of nearly 400 comments on DHS EA 2006 demonstrates this opportunity. Moreover, the department stated that we had an incorrect perception of how it treated stakeholder comments, adding that all comments that require resolution will be addressed in future EA releases.

We do not agree with DHS's comments about the adequacy of its approach to obtaining and incorporating stakeholder comments for several reasons, each of which are cited in our report. For example, the approach did not adequately define the type and nature of the comments being solicited, and it did not provide sufficient time for stakeholders to comment, as evidenced by some stakeholders stating that the time was too limited. Also, most DHS component organizations, including large ones like the Transportation Security Agency and the Coast Guard, did not provide comments. Moreover, about 60 percent of the comments that were received on DHS EA 2006 were not to be addressed in the next version (HLS EA 2007), and it was not specified when they would be addressed. Given that comments were directed at the architecture's completeness, internal consistency, understandability, and usability, which are all fundamental characteristics of an EA, we believe that our recommendation aimed at employing a more effective approach to soliciting and responding to comments is warranted.

We are sending copies of this report to the Chairmen and Ranking Minority Members of other Senate and House committees that have authorization and oversight responsibilities for homeland security. We are also sending a copy of this report to the Secretary of Homeland Security and the Director of OMB. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

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

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

Appendix I: Briefing to the Staffs of the Subcommittees on Homeland Security Senate and House Committees on Appropriations

Homeland Security: DHS Enterprise Architecture Continues to Evolve but Improvements Needed

Briefing to the Staffs of the
Subcommittees on Homeland Security
Senate and House Committees on Appropriations

February 28, 2007

1

GAO
Accountability * Integrity * Reliability

Table of Contents

2

GAO
Accountability * Integrity * Reliability

Introduction

Information technology (IT) is a critical tool in the Department of Homeland Security's (DHS) quest to transform 22 diverse and distinct agencies into one cohesive, high-performing department. In light of the importance of this transformation and the magnitude of the associated challenges, in 2003 we designated the department's implementation and transformation as a high-risk undertaking.[1]

In 2003 and in 2004, we reported that DHS needed to, among other things, develop and implement an enterprise architecture (EA)—a corporate blueprint—as an authoritative frame of reference to guide and constrain IT investment decision-making in a way that promoted interoperability, minimized wasteful duplication and redundancy, and optimized departmentwide mission performance.[2]

[1]GAO-03-119 and GAO-05-207.
[2]GAO-03-760 and GAO-04-702.

3

GAO
Accountability * Integrity * Reliability

Introduction

Recognizing the importance that an EA plays in effectively leveraging IT for organizational transformation, DHS issued an initial version of its architecture in September 2003. Following our review and recommendations for improvement of this version,[3] the department issued a second version in October 2004.

The DHS Appropriations Act of 2006 required the department's chief information officer (CIO) to submit to Congress a report that includes, among other things, an EA and a capital investment plan for implementing the architecture. It also required GAO to review the report.[4] On June 16, 2006, the CIO submitted its report, which included the third version of the department's EA and a plan for implementing it, which DHS referred to as DHS EA 2006 and Capital Investment Plan for Implementing the DHS EA.

[3]GAO-04-777.
[4]The act also requires DHS's CIO to submit a report that includes a description of the information technology (IT) capital planning and investment control (CPIC) process and an IT human capital plan, which will also be reviewed by GAO.

4

Objective, Scope, and Methodology

As agreed with staff for the Chairmen and Ranking Minority Members of the House and Senate Appropriations Committees' respective homeland security subcommittees, our objective was to assess the status of DHS EA 2006, including the capital investment plan for implementing it.

In order to meet this objective, we

- analyzed DHS EA 2006 and supporting documentation against our 41 prior recommendations regarding DHS EA content;
- evaluated the nature, substance, and disposition of stakeholder comments, including documentation produced by DHS's EA support contractor on DHS EA 2006;
- assessed DHS's process for soliciting stakeholder comments relative to applicable survey and data collection practices; analyzed DHS's capital investment plan against relevant guidance, including Office of Management and Budget's (OMB) capital planning guidance and applicable EA guidance; and
- interviewed DHS and contractor officials about their efforts to address our recommendations and resolve stakeholder comments, process for soliciting and responding to stakeholder comments, and basis for the capital investment plan.

5

Objective, Scope, and Methodology

We conducted our work at DHS and contractor facilities in the Washington, D.C., metropolitan area from June 2006 to February 2007 in accordance with generally accepted government auditing standards. For DHS data that we did not substantiate, we made appropriate attribution indicating the data source.

6

Results in Brief

DHS EA 2006 has evolved beyond prior versions, but missing architecture content and limited stakeholder input constrain its usability. While the architecture partially addresses prior GAO recommendations and stakeholder comments, the full depth and breadth of EA content that our recommendations provided for is still missing. Additionally, the majority of stakeholder comments, including concerns about architecture completeness, consistency, and understanding remain to be addressed. Stakeholder commentary on draft DHS EA 2006 products was limited by the approach used to solicit comments and the extent to which stakeholders provided comments. Further, DHS's capital investment plan for implementing its architecture is not based on an EA transition plan and is missing key IT investments. Without an EA that is complete, internally consistent, and understandable, DHS's ability to guide and constrain IT investments in a way that promotes interoperability, reduces overlap and duplication, and optimizes mission performance will be significantly diminished.

We are making recommendations to ensure that DHS fully implements our prior EA recommendations and effectively solicits stakeholder comments on future versions of its EA.

7

Results in Brief

In commenting on a draft of this briefing, DHS officials, including the DHS Chief Information Officer (CIO) and the Chief Architect, acknowledged that DHS EA 2006 is missing important content and stated that future versions will add content and improve usability. Additionally, the Chief Architect generally agreed with our recommendations for mapping our prior recommendations to specific EA content and for effectively soliciting stakeholder comments on future EA versions.

8

GAO
Accountability * Integrity * Reliability

Background

Created in March 2003, DHS has assumed operational control of about 209,000 civilian and military positions from 22 agencies and offices that specialize in one or more aspects of homeland security.[5] A major purpose of DHS's establishment was to improve coordination, communication, and information sharing among the multiple federal agencies responsible for protecting the homeland.

As we previously reported, the creation of DHS[6] is critically important and poses significant management and leadership challenges. For these reasons, we designated the implementation of the department and its transformation as high risk; we also pointed out that failure to effectively address DHS's management challenges and program risks could have serious consequences for our national security.

[5]These specialties include intelligence analysis, law enforcement, border security, transportation security, biological research, critical infrastructure protection, and disaster recovery.
[6]For example, see GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003) and *Homeland Security: Proposal for Cabinet Agency Has Merit, but Implementation Will be Pivotal to Success*, GAO-02-886T (Washington, D.C.: June 25, 2002).

9

GAO
Accountability * Integrity * Reliability

Background
Mission and Organization

DHS's mission is to lead the unified national effort to secure the United States by preventing and deterring terrorist attacks and protecting against and responding to national threats. Among other things, DHS is charged with ensuring safe and secure borders, and promoting the free flow of commerce.

To accomplish its mission, DHS is organized into various components, each of which is responsible for specific homeland security missions and for coordinating related efforts with its sibling components as well as with external entities. Table 1 shows DHS's principal organizations and their missions. Figure 1 shows a simplified view of the DHS organizational structure.

10

GAO
Accountability * Integrity * Reliability

Background
Mission and Organization

Table 1: Principal DHS Organizations and Their Missions

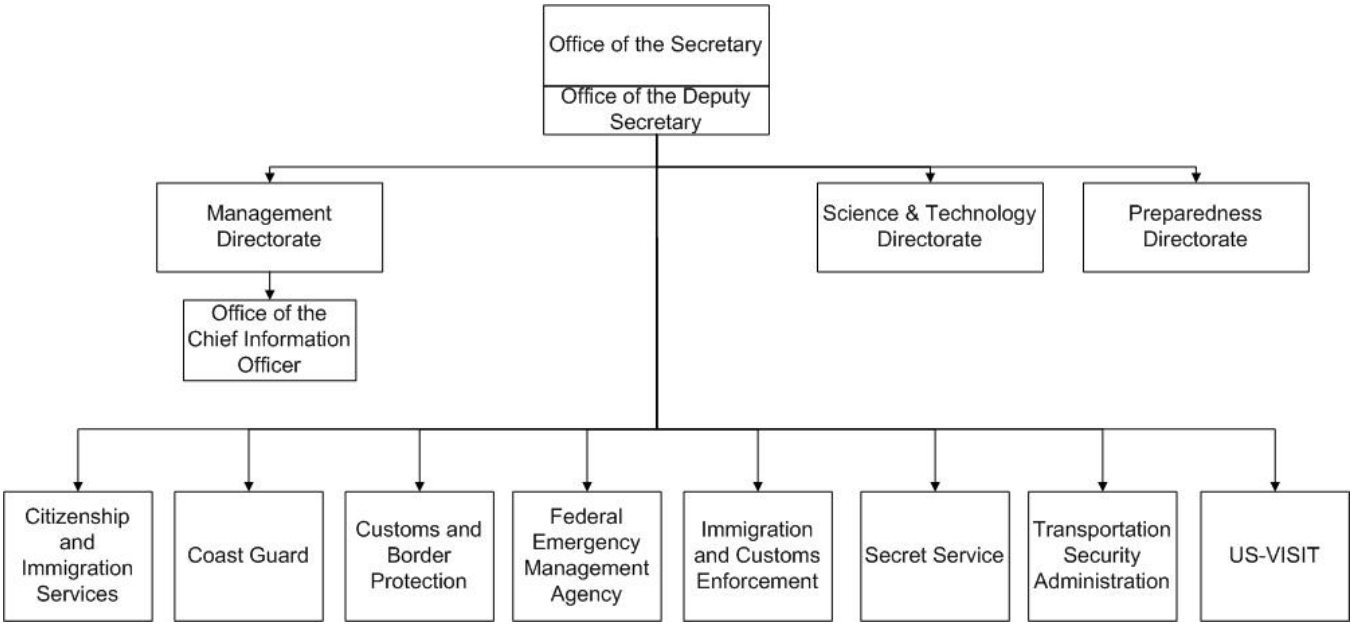
Principal organizations[a]	Missions
Citizenship and Immigration Services	Administers immigration and naturalization adjudication functions and establishes immigration services policies and priorities.
Coast Guard	Protects the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, and in any maritime region as required to support national security.
Customs and Border Protection (CBP)	Protects the nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.
Federal Emergency Management Agency (FEMA)	Prepares the nation for hazards, manages federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.
Immigration and Customs Enforcement (ICE)	Identifies and addresses vulnerabilities in the nation's border, economic, transportation, and infrastructure security.
Management Directorate	Manages department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, IT systems, facilities and equipment, and performance measurements.
Preparedness Directorate	Works with state, local, and private sector partners to identify threats, determine vulnerabilities, and target resources where risk is greatest, thereby safeguarding borders, seaports, bridges and highways, and critical information systems.
Science and Technology Directorate	Serves as the primary research and development arm of the department, responsible for providing federal, state, and local officials with the technology to protect the homeland.
Secret Service (USSS)	Protects the President and other high-level officials and investigates counterfeiting and other financial crimes (including financial institution fraud, identity theft, and computer fraud) and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.
Transportation Security Administration (TSA)	Protects the nation's transportation systems to ensure freedom of movement for people and commerce.
U.S. Visitor and Immigrations Status Indicator Technology (US-VISIT)	Develops and implements a governmentwide program to record the entry into and exit from the United States of selected individuals, verify their identity, and confirm their compliance with the terms of their admission into and stay in this country.

Source: GAO analysis based on DHS data.
[a]Does not show all the organizations under each of the directorates or all organizations that report directly to the DHS Secretary and Deputy Secretary.

GAO
Accountability * Integrity * Reliability

Background
Mission and Organization

Figure 1: Simplified and Partial DHS Organizational Structure



Source: GAO analysis based on DHS data.

12

GAO
Accountability * Integrity * Reliability

Background
EA: A Brief Description

An EA provides systematic structural descriptions—in useful models, diagrams, tables, and narrative—of how an entity currently operates (the "as-is" architecture) and how it plans to operate in the future (the "to-be" architecture), and it includes a plan for making that transition (the transition plan). In the federal arena, the transition plan provides the basis for informed capital investment planning. Agency capital investment plans are the basis for budget exhibits that are submitted annually to the OMB. Those plans identify, among other things, ongoing and planned IT investments.

Our experience with federal agencies has shown that investing in IT programs without having an EA to guide the process often results in systems that are duplicative, not well integrated, unnecessarily costly to maintain, and limited in terms of meeting mission needs and optimizing mission performance.[7]

[7]See GAO, *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).

13

GAO
Accountability * Integrity * Reliability

Background
GAO EA Guidance

To assist DHS and other federal agencies in effectively developing, maintaining, and implementing an enterprise architecture, we published a framework for architecture management that is grounded in federal guidance and recognized best practices.[8] The framework is a five-stage maturity framework that outlines 31 practices that contribute to effective architecture management.

In addition, we published a set of architecture content criteria that define the attributes of well-defined EA artifacts. These criteria are associated with the major components of the current and target architectures, namely the business, performance, information/data, services/applications, technical, and security descriptions, as well as the sequencing plan for transitioning from the current to the target architectures.[9]

[8]GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management* (Version 1.1), GAO-03-584G (Washington, D.C.: April 2003).
[9]GAO-04-777.

14

GAO
Accountability * Integrity * Reliability

Background
DHS EA Players

The DHS Office of the CIO has primary responsibility for departmentwide IT. According to the CIO, this includes among other things, developing and facilitating the implementation of the department's EA. To satisfy this responsibility, the CIO established various entities with specific roles and responsibilities. (See table 2 below.)

Table 2: DHS EA Players

Player	Roles and responsibilities
Enterprise Architecture Board (EAB)	Evaluates and approves IT investments for EA alignment and ensures that the EA is updated and maintained. Chair is the DHS CIO; Vice-Chair is the DHS Deputy CIO. Members include Chief Financial Officer Designee, Chief Procurement Officer Designee, Designated CIO's from DHS Directorates/Components, and a Business Process Support Group Designee.
Enterprise Architecture Center of Excellence (EACOE)	Reviews the information provided by the Submitter and provides recommendations to the EAB. Members include representatives from the components and departmental specialists.
Chief Architect	Serves as the EA program manager and is responsible for developing the EA and associated processes.
Submitter	Initiates a request to the EACOE and EAB for a decision about a particular IT investment. Represents a DHS component, focus group, or other DHS stakeholder.
Reviewer	Provides the research, supporting analysis, and to support the EACOE and EAB decision process.
EA team	Supports DHS Chief Architect in developing and managing the EA.
Facilitator team	Supports, manages, and facilitates the EACOE.

Source: GAO analysis of DHS data.

15

Background
DHS EA Players

Additionally, major stakeholders consisting of DHS component organizations (e.g., CBP and FEMA), internal stakeholders (e.g., Chief Information Security Office and the Wireless Management Office), and the department's EA support contractor are asked to support development of the architecture by providing input and responding to solicitations for comments on draft versions.

16

Background
History of DHS EA Versions

In September 2003, DHS issued the first version of its EA, called HLS EA (Homeland Security Enterprise Architecture). In October 2004, it issued the second version, known as EA version 2.

Subsequently, DHS decided to issue annual architecture updates. The first of these, DHS EA 2006, was issued in February 2006, and was included in the DHS CIO's June 2006 report to the Congress as mandated by the DHS Appropriations Act of 2006. According to DHS, this version was to create a better frame of reference to support departmental planning for the "to-be" environment, and to better coordinate cross-departmental initiatives. The department reports that the focus of DHS EA 2007 will be on issuing an enterprisewide transition plan and improving the target architecture.

17

Background
Summary of DHS EA 2006

DHS EA 2006 is organized as follows

- Overview Documents
- Business Architecture
- Data/Information Architecture
- Information Sharing Architecture
- "As-is" Inventory
- Target Technical Architecture
- EA Analysis Reports
- Create, Update, Reference, and Eliminate (CURE) Matrix
- HLS EA Strategic Drivers
- Other EA Related Artifacts

Attachment 1 depicts the structure of DHS EA 2006.

18

GAO
Accountability * Integrity * Reliability

Background
Summary of GAO Reviews of DHS's EA

Since 2003, we have evaluated and reported on DHS's efforts to develop, maintain, and implement its enterprise architecture from three EA perspectives: management, content, and investment alignment.

EA Management

We reported in 2003[10] and again in 2006,[11] on the department's institutional capability to manage its architecture program, including management practices associated with architecture governance, content, use, and measurement.

- In 2003 we reported that the department had implemented many of the practices described in our Enterprise Architecture Management Maturity Framework (EAMMF version 1.1).[12] For example, the department had, among other things, assigned architecture development, maintenance, program management, and approval responsibilities; and created policies governing architecture development and maintenance.

[10]GAO, *Information Technology: Leadership Remains Key to Agencies Making Progress on Enterprise Architecture Efforts*, GAO-04-40 (Washington, D.C.: Nov. 17, 2003).
[11]GAO, *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation*, GAO-06-831 (Washington, D.C.: Aug. 14, 2006).
[12]GAO-03-584G.

19

Background
Summary of GAO Reviews of DHS's EA

However, we also reported that the department's EA products did not describe its "as-is" and "to-be" environments, nor did they include a sequencing plan. Furthermore, the EA business, performance, information/data, application/service, and technology descriptions did not address security.

- In August 2006, we reported that DHS had satisfied a number of key elements within our EA framework (version 1.1). For example, we reported that DHS EA 2006 included products describing its "as-is" and "to-be" environments. However, we also reported that the sequencing plan was in draft and not approved, and DHS had not, for example, subjected its EA products and management processes to independent verification and validation, and it was not measuring and reporting on EA use and return on investment.

20

GAO
Accountability * Integrity * Reliability

Background
Summary of GAO Reviews of DHS's EA

EA Content

In 2004, we reported on the completeness and usability of the initial version of DHS's enterprise architecture.[13] In summary, we found that while the initial version provided a foundation on which to build, it was missing important content (i.e., was not sufficiently complete), which limited its usability. Moreover, we found that this version was not systematically derived from a DHS or national homeland security business strategy, but rather was an amalgamation of the existing architectures that several of DHS's predecessor agencies already had, along with their respective portfolios of system investments. Accordingly, we made 41 recommendations aimed at ensuring that future versions of the architecture

- are based on a methodology that provides for identifying the appropriate scope and are effectively planned;
- include the key elements business, performance, information, services/applications, technical, and security descriptions of a "to-be" architecture; and
- include the key elements of a transition plan.

Attachment 2 lists the 41 recommendations.

[13]GAO-04-777.

21

GAO
Accountability * Integrity * Reliability

Background
Summary of GAO Reviews of DHS's EA

EA Investment Alignment

Between 2003 and 2006, we have reported on the extent to which the department has ensured that major IT investments, such as US-VISIT,[14] CBP's Automated Commercial Environment (ACE) system,[15] and ICE's Atlas program,[16] are aligned with its EA. For example,

- We reported in September 2003 that US-VISIT was making assumptions and decisions about the program's operational technological context because DHS did not yet have a well-defined EA. We concluded that if program decisions were not consistent with DHS's EA, program rework would be required.[17]

[14]US-VISIT is a governmentwide program to collect, maintain, and share information on foreign nationals for enhancing national security and facilitating legitimate trade and travel, while adhering to U.S. privacy laws and policies.
[15]ACE is a new import and export processing system to facilitate the movement of legitimate trade through more effective trade account management and strengthen border security by identifying import and export transactions that could pose a threat to the United States.
[16]Atlas is a program to modernize ICE's IT infrastructure to improve information sharing, strengthen information security, and improve productivity.
[17]GAO, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed,* GAO-03-1083 (Washington, D.C.: Sept. 19, 2003).

22

GAO
Accountability * Integrity * Reliability

Background
Summary of GAO Reviews of DHS's EA

In February 2005, we reported that DHS had assessed US-VISIT for alignment with its architecture and found it to be in compliance. However, DHS could not provide us with sufficient documentation to understand its architecture compliance methodology and criteria, or verifiable analysis to justify its determination.[18]

- We similarly reported in March 2005 that DHS's determination that ACE was aligned with DHS's EA was not supported by sufficient documentation to allow us to understand its architecture compliance methodology and criteria (e.g., definition of alignment and compliance) or with verifiable analysis demonstrating alignment.[19] In May 2006, we again reported that DHS evaluated and approved ACE alignment. However, DHS again did not have a documented methodology for evaluating programs for compliance, and no analysis or documentation was produced that could be used to verify ACE's degree of alignment. Moreover, the alignment assessment again did not cover all architectural views.[20]

[18]GAO, *Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program,* GAO-05-202 (Washington, D.C.: Feb. 23, 2005).
[19]GAO, *Information Technology: Customs Automated Commercial Environment Program Progressing, but Need for Management Improvements Continues,* GAO-05-267 (Washington, D.C.: Mar. 14, 2005).
[20]GAO, *Information Technology: Customs Has Made Progress on Automated Commercial Environment System, but It Faces Long-Standing Management Challenges and New Risks*, GAO-06-580 (Washington, D.C.: May 31, 2006).

23

Background
Summary of GAO Reviews of DHS's EA

- We reported in September 2005 that DHS had determined that Atlas was in compliance with the EA but that this determination was also not based on a documented analysis that is necessary to make such a determination.[21] In July 2006, we reported that DHS had again determined that Atlas was in compliance. However, the determination was not based on a documented analysis mapping Atlas's infrastructure architecture to the EA or a documented methodology for evaluating compliance.[22]

[21]GAO, *Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program,* GAO-05-805 (Washington, D.C.: Sept. 7, 2005).
[22]GAO, *Information Technology: Immigration and Customs Enforcement Is Beginning to Address Infrastructure Modernization Program Weaknesses but Key Improvements Still Needed*, GAO-06-823 (Washington, D.C.: July 27, 2006).

24

DHS EA 2006 Has Evolved beyond Prior Versions, but Missing Architecture Content and Limited Stakeholder Input Constrain Its Usability

DHS EA 2006 partially addresses the content shortcomings that we previously reported about prior versions of the department's architecture and made recommendations to correct. Moreover, this latest version of the architecture either partially or fully addresses about 36 percent of the comments made by DHS component organizations and stakeholders and its EA support contractor on a draft of it.

Nevertheless, the full depth and breadth of EA content that our recommendations provided for adding is still missing. Moreover, not only do the majority of stakeholder comments remain to be addressed, but key stakeholders, such as the Coast Guard and TSA, chose to not comment on a draft of DHS EA 2006, and the approach used to solicit input from those DHS organizations and stakeholders that chose to comment was limited.

Results
DHS EA 2006 Evolution and Limitations

As a result, concerns about the usability of DHS EA 2006 as a departmental frame of reference for informing IT investment decisions were raised by certain DHS component organizations and stakeholders, and the EA support contractor, and as noted earlier, was observed as part of our prior work on major IT investments. Without an EA that is complete, internally consistent, and understandable, DHS's ability to guide and constrain IT investments in a way that promotes interoperability, reduces overlap and duplication, and optimizes overall mission performance will be greatly diminished.

26

DHS EA 2006 Partially Addresses Prior GAO Recommendations, but Important Content Still Are Missing

DHS EA 2006 partially satisfies each of our 41 prior recommendations aimed at adding important content to the architecture's "to-be" business, performance, information, services/applications, technical, and security views.[23] The following are summaries of selected recommendations that are illustrative of the extent to which DHS EA 2006 addresses them.

[23]Partially satisfied means that DHS addressed at least one but not all elements of the recommendation.

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "business" view of the "to-be" architecture, among other things, the enterprise's purpose, scope (e.g., organizations, business areas, and internal and external stakeholders' concerns), and associated limitations or assumptions.

  In response, the DHS EA 2006 business view describes DHS's purpose, including strategic goals, and it describes aspects of DHS's scope, such as organizational entities and their business area responsibilities. Further, it describes the need to interact with external stakeholders, and it identifies the limitations of its current environment (e.g., information sharing). However, some of the entities described no longer exist (e.g., Border and Transportation Security Directorate). Moreover, it does not clearly describe DHS's scope within the larger context of homeland security, which is important because other departments are involved in homeland security, and thus where DHS's business areas stop and other departments' start needs to be clear. In addition, it does not identify any assumptions associated with the "to-be" business model, such as cultural changes needed for information sharing.

28

GAO
Accountability * Integrity * Reliability

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "business" view of the "to-be" architecture a description of key business processes and the locations where the processes will be performed, including the alignment among (1) applicable federal laws, regulations, and guidance, (2) department policies, procedures, (3) operational activities, (4) organizational roles, and (5) operational events and information.

  In response, the DHS EA 2006 identifies functions (e.g., "Implement and Test Countermeasures") and services (e.g., "Person-Centric Information Services") for achieving mission and strategic business goals (e.g., "Prevention"). However, the functions are not decomposed into business processes, which is important because functions are logical groupings of business activities, whereas a process is an executable series of triggered events that produces a desired outcome. Moreover, not all functions are assigned to a location/organization (e.g., "Discover Threat Trends" or "Assess Preparedness Capabilities"). In addition, while functions are based on applicable laws, regulations, and guidance (e.g., the National Strategy for Homeland Security), the architecture does not describe alignment with department policies, procedures, and guidance, and it does not address operational activities, all organizational roles, and operational events.

29

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "performance" view of the "to-be" architecture a description of measurable goals and outcomes for (1) technology products and services and (2) business applications and services that help enable achievement of business goals and outcomes.

  In response, DHS EA 2006 describes certain technical performance goals/measures, (e.g., 99.5 percent availability for IT infrastructure). However, goals/measures for other items are not specified, such as network throughputs. According to EA Team officials, specification of all technical goals/measures are pending execution of IT and business unit service level agreements. Also, the EA provides a vision for business services to develop an integrated system or system of systems that provide a comprehensive set of business services. In addition, while the architecture specifies measurable goals and outcomes for some applications and services, it does not describe such goals and services for all specified services (e.g., "Managing Grants, Procurements, and Acquisitions") and all systems (e.g., the Automated Export System).

30

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "information/data" view of the "to-be" architecture a description of data management policies, procedures, processes, and tools for analyzing, designing, building, and maintaining databases in an enterprise architected environment.

  In response, DHS EA 2006 outlines data management strategies and database management activities, including ensuring that the design, development, deployment, operation, and maintenance of an enterprise data environment support enterprisewide management of data. For example, activities are identified for establishing procedures for coordinating data maintenance activities. Also, data management objectives are defined, such as ensuring that data storage is not centralized but rather available via federated query. Further, the need to identify and adopt tools for meeting data management objectives, such as modeling and organizing data is recognized. However, DHS EA 2006 does not describe data management processes and procedures, such as ones for identifying and standardizing core data elements to be used across DHS and with external stakeholders.

31

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "information/data" view of the "to-be" architecture a data dictionary, which is a repository of standard definitions for key terms.

  In response, DHS EA 2006 provides a data dictionary that includes definitions of subject areas (e.g., event) and data objects (e.g., incident). However, definitions of all key terms (e.g., first responder) are not included in the dictionary.

32

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "information/data" view of the "to-be" architecture a (1) conceptual data model (i.e., a description of the objects or things that comprise the business without regard to how they will be physically stored); (2) a logical database model (i.e., the normalized basis for developing the schemas that support design of physical databases), and (3) a metadata model (i.e., the rules and standards for representing data (data formats) and accessing data (data protocols), according to a documented business context).

  In response, DHS EA 2006 provides definitions of subject areas or high-level categories of business things/information types (e.g., "Conveyances") and data objects (e.g., "Manifest") that are fundamental to DHS's business. It also identifies the relationships between data objects.

  Also, DHS EA 2006 provides a logical database model for its "Integrated Flow of Persons Through Existing Screening Processes" business function. However, logical database models are not included for all business functions. DHS EA Team officials told us that a project team has been established to develop a metadata model.

33

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "services/applications" view of the "to-be" architecture a description of the enterprise application systems and system components and their interfaces.

  In response, DHS EA 2006 defines capabilities (e.g., Maintain Threat Notification) for target application and application components. In addition, it identifies business functions (e.g., "Communicate Risks" and "Threats to the Public") that are enabled by application components. However, the architecture does not describe the interfaces between enterprise applications and application components. For example, it does not depict the interconnection involved between the "Communicate Risks" and "Threats to the Public" business functions.

34

GAO
Accountability * Integrity * Reliability

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "technical" view of the "to-be" architecture a description of the technical reference model (TRM)[24] that describes enterprise infrastructure services, including specific details regarding the services' functionality and capabilities that will be available in developing application systems, as well as the technical standards to be implemented for each service and the life cycle of each service.

  In response, DHS EA 2006 lists TRM services, such as data discovery services and Web services, and identifies the technical standards that support the services. However, since the listed services are from DHS components, the services that will and will not be enterprise services are not identified. In addition, the functionality and capabilities of these services are not specified, and the anticipated life cycles of many services (e.g., "Message Middleware") are not described.

[24]Describes technology that is to support the delivery of service components, including relevant standards for implementing the technology.

35

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Include in the "security" view of the "to-be" architecture a description of the policies, procedures, goals, strategies, principles, and requirements relevant to information assurance and security, including how they align and integrate with other elements of the architecture (e.g., security services).

  In response, DHS EA 2006 contains policies, procedures, goals, strategies, principles, and requirements for managing information assurance and security. For example, it includes DHS IT Security Architecture Guidance, which outlines security principles related to identity and access management, as well as the DHS Sensitive Systems Policy and DHS Sensitive Systems Handbook, which describe a range of security policies and procedures. However, the architecture does not clearly show how these documents are aligned with each other, and how they are aligned with products in the other architecture views (e.g., the "technical" view's TRM identifies component organizations firewalls, but it is unclear whether these are part of the "security" view of the "to-be" architecture). Moreover, none of the security related documents have been updated from those in the prior version of the EA.

36

Results
DHS EA 2006 Evolution and Limitations

- Recommendation: Base the EA transition plan on, among other things, an analysis of the gaps between the "as-is" and "to-be" architectures' business, information/data, and services/application systems to define missing and needed capabilities.

  In response, DHS EA 2006 does not include a transition plan, and it does not include any evidence of a gap analysis—a comparison of the current and target architectures to identify capability differences.

37

DHS EA 2006 Partially Addresses Stakeholder Comments, but Concerns Remain

A total of 383 stakeholder comments were submitted on a draft of DHS EA 2006. Of these comments, DHS reported that 139 were fully addressed, 27 were partially addressed, and 101 were not addressed but are to be resolved in a later EA version, while 116 had no resolutions reported. Thus, the majority of stakeholder comments, including expressions of concern about the usability of DHS EA 2006, were not addressed.

Of the 139 stakeholder comments that were reported as fully addressed,

- 131 were reportedly addressed by adding or correcting previously missing or erroneous information in the draft materials, such as omitted systems, misspellings, and incorrect business owner contact information and
- 8 were reportedly addressed by providing additional descriptive information.

GAO
Accountability * Integrity * Reliability

Results
DHS EA 2006 Evolution and Limitations

According to DHS's comment tracking documentation, 27 of the remaining 244 comments were partially addressed. For example,

- The EA support contractor stated that the IT standards profile[25] in the TRM did not identify important time frames for TRM categories. These categories are hold,[26] contain,[27] divest,[28] or move-to.[29] Without time frames for each standard, programs cannot effectively plan for the appropriate use of new and existing standards, thus increasing the chances of later program rework.

  In response, the EA Team stated that time frames for 30 percent of the standards in the move-to category were established by the January 31, 2006, target, and the remainder of the time frames are scheduled to be identified by September 30, 2007.

[25]The TRM identifies and describes the IT services (e.g., a data interchange service) used throughout the agency. The standards profile defines the set of IT standards that support the services. The profile may also specify the technology products that implement a specific IT standard.
[26]The hold category identifies the IT standards (or technology products) that are currently in use.
[27]The contain category identifies the IT standards (or technology products) that are currently in use but cannot be further deployed.
[28]The divest category identifies the IT standards (or technology products) that are to be retired.
[29]The move-to category identifies the IT standards (or technology products) that are to be in the target state.

39

Results
DHS EA 2006 Evolution and Limitations

- Multiple comments criticized the usability of EA 2006. CBP stated that the collection of Access tables and Excel spreadsheets was very hard to understand, navigate, and cross-reference. IAIP commented that data were spread over too many documents, making it hard for nonarchitects to understand and utilize. US-VISIT noted that appropriate architecture access tools were not provided. The EA support contractor stated that the architecture's usability was poor and suggested adopting a proper EA repository tool to improve usability.

  In response, an html embedded table of contents with hyperlinks to EA products was added. However, plans to make the EA repository available in a commercial tool, which was at one time scheduled for December 1, 2005, have been suspended. Additionally, the repository requirements working group has been disbanded. Notwithstanding this, EA Team officials stated that they are looking at opportunities for improved presentation of the EA.

40

Results
DHS EA 2006 Evolution and Limitations

According to DHS's comment tracking documentation, 101 comments were not addressed in DHS EA 2006 but are to be resolved in a later version of the EA.

- The Chief Information Security Office stated that the security architecture was not fully integrated, citing for example that the "as-is" inventory lacked security classifications-sensitivity levels for 4,118 out of 4,260 systems listed. According to DHS documentation, work is ongoing to address this comment and continued planning, collaboration, and resources are required to further integrate the security architecture into the EA.
- ICE stated that the inputs it provided had not been incorporated, represented, or otherwise accommodated in anyway, and that the draft DHS EA 2006 business model was an unchanged repackaging of the prior version of the EA. DHS documentation acknowledged that the scope of the business model included only limited changes, and the ICE business model and mapping would be incorporated in a later version of the architecture.
- CBP stated that the draft DHS EA 2006 lacked a framework or other organizational structure. According to DHS documentation, a framework is to be used for the next version of the architecture.

41

Results
DHS EA 2006 Evolution and Limitations

- The United States Secret Service (USSS) stated that the draft architecture described a “snap shot in time” and did not provide any organized way of updating and maintaining data. The EA Team stated that in developing the draft it had tried to minimize the number of “data calls” to component organizations and that it would make further efforts to initiate more component collaboration and input in the future.
- The EA support contractor stated that
  - The business model was not complete and should have been updated to reflect missing data. According to DHS documentation, a business model review was under way at the time to collect additional information where possible and include it in EA 2007, but some business model updates may be carried to the DHS EA 2008 version.
  - The process flows, and use cases—which are essential for driving out information sharing and interoperability issues—were missing. According to DHS documentation, work on this had started for business areas based on Office of the Chief Information Officer (OCIO) priorities and where artifacts and content were available.
  - The transition strategy had weaknesses, such as a lack of vision for incremental transformation. According to DHS documentation, work was under way for creating a transition plan.

42

Results
DHS EA 2006 Evolution and Limitations

- Security and privacy considerations were notably weak. According to DHS documentation, some related work is on-going but that further efforts will be planned to address security and privacy information in a future release of the EA as opportunity and information is available.

DHS's comment tracking documentation did not provide resolution actions for the remaining 116 comments. Although some of these unresolved comments did not require that action be taken, others were substantive. For example,

- CBP stated that the draft EA suffered the same incompleteness that we identified with the first version of DHS's EA and that it did not demonstrate an integrated understanding of the current DHS environment. According to DHS documentation, no change was required to address this comment because our recommendations were addressed in the second version of DHS's EA. However, as previously discussed, our analysis of the extent to which DHS EA 2006 addresses our prior recommendations showed that they were only partially addressed, and that important content remained to be added.
- Science and Technology (S&T) stated that performance measures were not comprehensive and not always measurable. According to DHS documentation, no change was required because the source for the performance measures was the department's fiscal year 2006 budget.

43

Stakeholder Commentary on Draft DHS EA 2006 Products Was Limited

Soliciting and obtaining comments from all departmental stakeholders is an important way to ensure that draft architectural products are well defined. To their credit, the DHS Chief Architect and EA Team recognized the importance of such commentary.

However, the approach they used in soliciting comments did not clearly define the type of information requested and did not provide sufficient time for detailed responses. Also, the extent to which they actually obtained comments was limited. Of 33 EA stakeholders, only 12 submitted comments. Without ensuring that meaningful comments from all key DHS organizational components were obtained, the department has missed a valuable opportunity to better ensure the completeness, internal consistency, and understandability of DHS EA 2006.

Approach to Soliciting Stakeholder Comments Was Limited

When soliciting comments from stakeholders, it is important that the approach used, among other things, (1) clearly define the type of information being solicited, including what key terms mean, and (2) permit adequate time for stakeholders to provide comments. The approach to soliciting comments on DHS EA 2006 did not do these things.

First, the type of information being solicited from stakeholders on a draft of DHS EA 2006 was not clearly defined. For example,

- Stakeholders were asked to use a scale of 1 to 5 to score the quality of four characteristics of DHS EA 2006. However, only the extremes of the scale were labeled, with 1 being designated as poor and 5 being designated as excellent. Scores of 2, 3, and 4 were not labeled. Moreover, the intended meaning of poor and excellent, much less a score of 2, 3, or 4, were not defined. As a result, stakeholders had to assign their own unique meanings to the scoring system.

Results
DHS EA 2006 Evolution and Limitations

- The characteristics that stakeholders were asked to score the quality of were completeness, consistency, understanding, and usability. Associated with each of the four architecture characteristics were between 2 to 4 questions. However, these questions did not clarify what was meant by each characteristic. For example, stakeholders were asked to score completeness based on the following questions without further explanation or guidance.
    - How complete do you feel EA 2006 is from a DHS perspective?
    - How complete do you feel EA 2006 is from your component or organization perspective?
    - How complete do you feel EA 2006 is from an OMB or oversight perspective?

46

Results
DHS EA 2006 Evolution and Limitations

Second, stakeholders had to review the draft and provide their comments in only 2 weeks. According to the EA support contractor, this was not sufficient time to respond. Similarly, CBP stated in its comments that this was too short a period of time to permit a detailed review. Our review of DHS EA 2006 confirmed this, as we found that considerably more time was needed for us to examine the number of complex artifacts in the architecture (e.g., 200 Access tables and 6 Excel workbooks (each of with multiple worksheets).

47

Results
DHS EA 2006 Evolution and Limitations

Extent to Which Stakeholders Provided Comments Was Limited

To the credit of the Chief Architect and the EA Team, they solicited stakeholder comments on a draft of DHS EA 2006. The stakeholders included 14 component organizations, 18 internal stakeholders, and 1 support contractor.

Of these 33 stakeholders, comments were received from only 12. Among those major DHS organizations that did not comment were Transportation Security Administration (TSA), the Coast Guard, and FEMA. This means that DHS EA 2006 does not reflect the reactions and perspectives of major organizational parts of the department. The tables on the next slide identifies the 33 stakeholders as well as which ones provided comments.

48

GAO
Accountability * Integrity * Reliability

Results
DHS EA 2006 Evolution and Limitations

Table 4: Stakeholders That Did and Did Not Provide Comments

Provided comments	
Components	
✓	Customs and Border Protection (CBP)
✓	Immigration and Customs Enforcement (ICE)
✓	Science and Technology (S&T)
✓	US-VISIT
✓	Intelligence Analysis and Operations (IAIP)
✓	Federal Law Enforcement Training Center (FLETC)
✓	Secret Service (USSS)
Internal stakeholders	
✓	EA Program Management Office (PMO)
✓	Chief Information Security Office (CISO)
✓	Enterprise Data Management Office
✓	Wireless Management Office (WMO)
Contractor	
✓	Contractor/Independent Review Team

Did not provide comments	
Components	
×	OPS Coordination
×	Citizenship and Immigration Services (USCIS)
×	Federal Emergency Management Agency (FEMA)
×	Office of Intelligence and Analysis (OI&A)
×	Preparedness Division (PD)
×	Transportation Security Administration (TSA)
×	Coast Guard (USCG)
Internal stakeholders	
×	Geospatial Management Office
×	Infrastructure Transformation Office
×	Continuity of Operations/Critical Infrastructure Protection
×	Homeland Secure Data Network
×	Section 508 Compliance
×	Enterprise Business Management Office (EBMO)
×	Enterprise Application Delivery Office (EADO)
×	Privacy Office
×	Chief Medical Officer (CMO)
×	Chief Financial Office (CFO)
×	Chief Procurement Officer (CPO)
×	Chief Human Capital Officer (CHCO)
×	Screening Coordination Officer
×	Grants and Training

Source: GAO Analysis of DHS data.

49

Results
DHS EA 2006 Evolution and Limitations

DHS Capital Investment Plan Is Not Based on EA Transition Plan and Is Not Complete

According to OMB guidance, capital planning helps to ensure that investments are timed and economically justified to fill identified gaps in mission capabilities and to support strategic mission goals and outcomes. Capital investment plans are intended to capture the results of such planning. Our EA guidance states that a complete EA includes a plan for investing in capital assets and transitioning from the "as-is" architectural environment to the "to-be" environment. It further states that this transition plan is to be based on an analysis of the mission capability gaps that exists between these two environments, as well as such factors as technology opportunities, marketplace trends, fiscal and budgetary constraints, institutional system development and acquisition capabilities, new and legacy system dependencies and life expectancies, and the relative value of competing investments.

50

Results
DHS EA 2006 Evolution and Limitations

In January 2006, DHS produced *Capital Investment Plan for Implementing the DHS Enterprise Architecture,* which was prepared to respond to the DHS Appropriations Act of 2006. According to the plan, it focuses on the near-term and represents the first phase of a transition plan for getting from the "as-is" to the "to-be" EA. The plan refers to this focus as building the foundation for effective transition, and states that it includes the following four areas:

- establishing the IT infrastructure (e.g., communications security, network/e-mail/data center services, application portals) to support eventual provision of enterprisewide shared services and efficient information sharing;
- planning and implementing more efficient provision enterprise business services (e.g., financial services, human resource services);
- consolidating duplicative legacy systems (e.g., watch lists); and
- supporting OMB eGov initiatives and lines of business.

51

Results
DHS EA 2006 Evolution and Limitations

For each of these areas, the capital investment plan incorporates information from the department's fiscal year 2007 budget submissions to OMB (Exhibit 53 and Exhibit 300s) to identify prior year, current year (fiscal year 2006), and future year (fiscal year 2007 to 2011) funding and personnel levels for a number of investments, including descriptions of these investments. Examples of investments in each category are as follows.

- IT Infrastructure: *Network services* to move toward a consolidated, reliable, and secure communications network.
- Enterprise Business Services: *Electronic records management* to integrate and replace multiple applications and manual processes.
- Consolidating Legacy Systems: *Watch list technical integration* to, among other things, streamline the flow of terrorist screening data to and among DHS agencies and the National Counterterrorism Center.
- OMB eGOV and Lines of Business: *Geospatial information one-stop* to promote coordination and alignment of geospatial data collection and maintenance among all levels of government.

Results
DHS EA 2006 Evolution and Limitations

Notwithstanding the wide range of investment-related information in DHS's capital investment plan, it is not complete with respect to providing a comprehensive roadmap for transitioning from the "as-is" to the "to-be" DHS architecture. For example,

- DHS EA 2006 did not include an EA transition plan, and thus the capital investment plan is not based on this integral part of a complete EA—namely the temporal roadmap transitioning to the "to-be" architecture that is grounded in, among other things, analyses of gaps in mission area capabilities and proposed investments to fill the gaps that are sequenced over time in light of, for example, the investments' mutual dependencies and return on investment, and the department's ability to afford and manage them. Rather, the capital investment plan is the compilation of a number of ongoing and planned investments as contained in the department's budget submissions, logically organized by investment categories or portfolios. According to the DHS Chief Architect, the capital investment plan is in an "initial plan" and a more complete version will exist once the DHS EA 2007 transition plan is developed.

53

Results
DHS EA 2006 Evolution and Limitations

- The capital investment plan does not account for all of DHS's planned investment in IT. For example,
  - For fiscal year 2007, it includes $527 million in IT development, modernization, and enhancement funding, while DHS's budget submission to OMB for IT totaled $1.845 billion. Thus, it excludes about $1.318 billion or about 71 percent of this planned IT funding.
  - For fiscal year 2007, it includes $1.078 billion in IT operations and maintenance funding, while DHS's budget submission to OMB for IT totaled $2.260 billion. Thus, it excludes $1.182 billion or about 52 percent of this planned IT funding.
- The capital investment plan does not include information on certain major IT capital investments, such as Secure Flight, which is a system to prescreen passengers (i.e., match passenger information against terrorist watch lists) for domestic flights, or the Secure Border Initiative (SBI), which is a multiyear program to secure U.S. borders and reduce illegal immigration. According to the capital investment plan, investments like SBI were not included in the plan because they require an enormous amount of planning and did not have investment dollars associated with them.

54

Results
DHS EA 2006 Evolution and Limitations

- In March 2006, DHS announced that eMerge2, a departmentwide program to consolidate financial management systems and which was included within the capital investment plan, was being terminated.

55

GAO
Accountability * Integrity * Reliability

Conclusions

DHS's approach to developing its EA through incremental releases or versions is reasonable, given the size and complexity of the department and the volumes of information needed to produce a complete, understandable, and usable architecture. As the department's third version of its EA, DHS EA 2006 is an improvement over prior versions, as evidenced by it at least partially addressing our prior recommendations. Moreover, DHS EA 2006 is partially responsive to stakeholder comments on a draft of it.

Nevertheless, DHS EA 2006 is still not sufficiently complete and usable, given those aspects of our recommendations that it did not fully address, the range of stakeholder comments that have not been resolved, and the limitations of the capital investment plan. Given the critical role that DHS's EA should play in the department's transformation efforts, which we have identified as a high-risk undertaking, it is important for DHS to fully address both our existing recommendations and stakeholder comments on incremental versions of its architecture.

Conclusions

Finally, with regard to stakeholder comments, it is also important for the department to ensure that it devotes sufficient time and adopts an effective approach to obtaining stakeholder comments on future versions. If it does not, the chances of developing a well-defined EA that is accepted and usable will be diminished.

57

GAO
Accountability * Integrity * Reliability

Recommendations For Executive Action

To ensure that DHS fully implements our prior EA recommendations and effectively solicits and addresses stakeholder comments on incremental versions of its EA, we recommend that the Secretary of Homeland Security direct the department's CIO to

(1) include in future versions of the department's EA a traceability matrix that explicitly maps EA content to our recommendations in sufficient detail to demonstrate their implementation, and

(2) ensure that future efforts to solicit stakeholder comments on the department's EA employ an effective approach that includes clearly defining the type of information requested and allowing sufficient time for obtaining and responding to these comments.

We are not making recommendations for addressing limitations in the department's capital investment plan for implementing its EA because our existing recommendations for an EA transition plan address such limitations.

58

GAO
Accountability * Integrity * Reliability

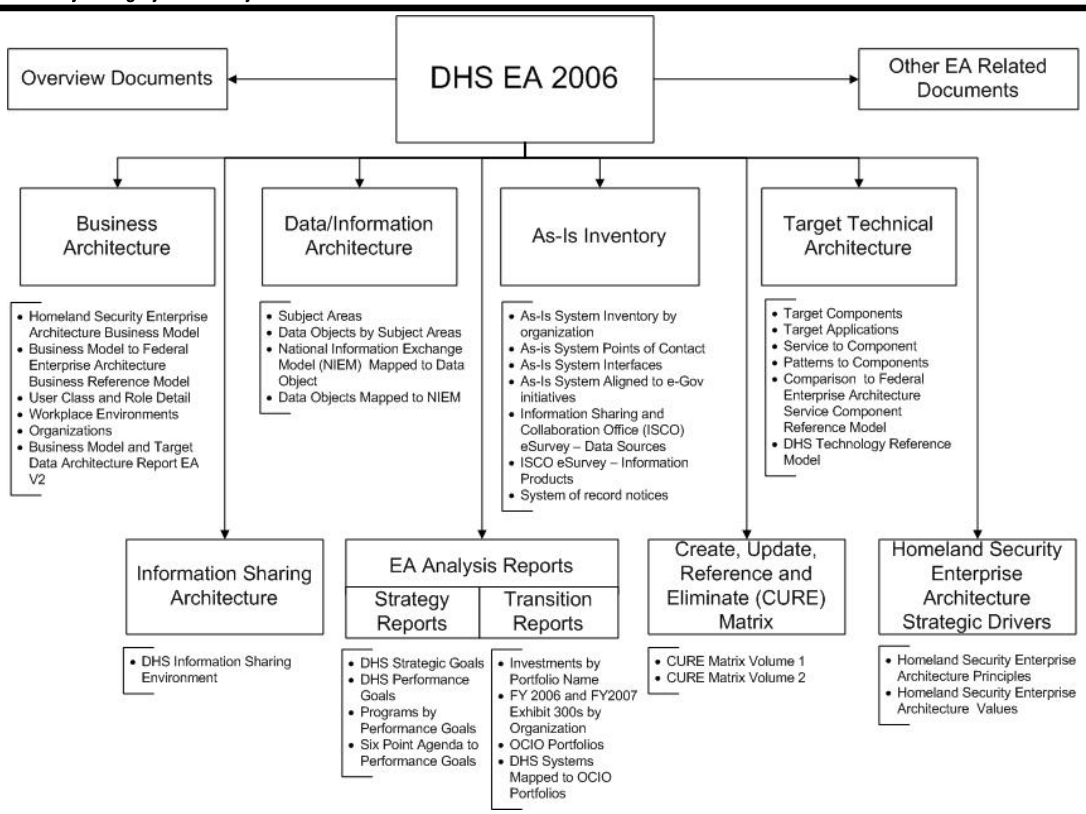
Agency Comments

In written comments on a draft of this briefing, the DHS CIO acknowledged that DHS EA 2006 is missing important content. He also stated that the department is addressing our prior recommendations and valid stakeholder comments, and that future versions of the architecture will add recommended content and improve usability. Further, the CIO stated that the department is currently using its EA as a means to improve mission effectiveness and efficiency, and that completeness is not required for an EA to be useful. We agree that there is value in each incremental version of an evolving architecture to help inform system investment decision making. However, the more complete and understandable an EA is, the greater its utility. Our prior recommendations are aimed at advancing the utility of DHS's EA.

While the CIO's written comments did not explicitly address the recommendations in this briefing, the DHS Chief Architect said that the department generally agrees with our recommendations for mapping our prior recommendations to specific EA content and for effectively soliciting stakeholder comments on future EA versions.

GAO
Accountability * Integrity * Reliability

Attachment 1
DHS EA 2006 Structure



Source: GAO based on DHS EA 2006.

60

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

To ensure that DHS has a well-defined architecture to guide and constrain pressing transformation and modernization decisions, we recommended that the Secretary of Homeland Security direct the department's architecture executive steering committee, in collaboration with the CIO, to:

#	Recommendation
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.
2	Develop, approve, and fund a plan for incorporating into the architecture the content that is missing.

Source: GAO.

61

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

We recommended the following actions to ensure that future versions of the architecture included the six key elements governing the business view of the "to-be" architectural content that our previous report identified as not being fully developed:

#	Recommendation
3	A business assessment that includes the enterprise's purpose, scope (e.g., organizations, business areas, and internal and external stakeholders' concern(s), limitations or assumptions, and methods.
	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), casual information, and rationales.
4	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. The business strategy should include:
	(1) A vision statement that describes the business areas requiring strategic attention based on the gap analysis,
	(2) 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,
	(3) 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,
	(4) A description of the measurable strategic business objectives to be met to achieve the desired change,
	(5) A description of the measurable tactical business goals to be met to achieve the strategic objective, and
	(6) 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.
5	Common (standard and departmentwide) policies, procedures, and business and operational rules for consistent implementation of the architecture.
6	A description of key business processes and how they support the department's mission, including the business processes and the locations where the business process will be performed. This description should provide 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.
7	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.
8	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, and govern/manage the development and implementation of the architecture).

Source: GAO.

62

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

We recommended the following actions to ensure that future versions of the architecture included the three key elements governing the performance view of the "to-be" architectural content that our previous report identified as not being fully developed:

#	Recommendation
9	A description of the processes for establishing, measuring, tracking, evaluating, and predicting business performance regarding business functions, baseline data, and service levels.
10	A description of measurable business goals and outcomes for business products and services, including strategic and tactical objectives.
11	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.

Source: GAO.

63

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

We recommended the following actions to ensure that future versions of the architecture included the seven key elements governing the information view of the "to-be" architectural content that our previous report identified as not being fully developed:

#	Recommendation
12	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.
13	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 access to, maintenance of, and use of data.
14	A data dictionary, which is a repository of standard data definitions for applications.
15	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 to 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.
16	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.
17	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.
18	A description of the information flows and relationships among organizational units, business operations, and system elements.

Source: GAO.

64

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

We recommended the following actions to ensure that future versions of the architecture included the five key elements governing the services/applications view of the "to-be" architectural content that our previous report identified as not being fully developed:

#	Recommendation
19	A description of the services and their relationships to key end-user services to be provided by the application systems.
20	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.
21	A description of the policies, procedures, process, and tools for selecting, controlling, and evaluating application systems to enable effective IT investment management.
22	A description of the enterprise application systems and system components and their interfaces.
23	A description of the system development life-cycle process for application development or acquisition and the integration of the process with 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.

Source: GAO.

65

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

We recommended the following actions to ensure that future versions of the architecture included the six key elements governing the technical view of the "to-be" architectural content that our previous report identified as not being fully developed:

#	Recommendation
24	A list of infrastructure systems and a description of the systems' hardware and software infrastructure components. The description should also reflect the systems relative importance to achieving the department's vision based on constraints, business value, and technical performance.
25	A description of the policies, procedures, processes, and tools for selecting, controlling, and evaluating infrastructure systems to enable effective IT investment management.
26	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.
27	A description of the TRM that identifies and describes (1) the technical standards to be implemented for each enterprise service and (2) the anticipated life cycle of each standard.
28	A description of the physical IT infrastructure needed to design and acquire systems, including the relationships among hardware, software, and communications devices.
29	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.

Source: GAO.

66

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

We recommended the following actions to ensure that future versions of the architecture included the seven key elements governing the security view of the "to-be" architectural content that our previous report identified as not being fully developed:

#	Recommendation
30	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).
31	Definitions of terms related to security and information assurance.
32	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.
33	A description of operational security rules that are derived from security policies.
34	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.
35	A description of the security standards to be implemented for each enterprise service. These standards should be derived form security requirements. This description should also address how the services will align and integrate with other elements of the architecture (e.g., security policies and requirements).
36	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.

Source: GAO.

67

GAO
Accountability * Integrity * Reliability

Attachment 2
GAO EA Content Recommendations

We recommended the following actions to ensure that future versions of the architecture included the five key elements governing the transition plan content that our previous report identified as not being fully developed:

#	Recommendation
37	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.
38	A high-level strategy for implementing the enterprise architecture. This strategy should include:
	(1) Specific time-phased milestones for acquiring and deploying systems;
	(2) Performance metrics for determining whether business value is being achieved;
	(3) Financial and nonfinancial resources needed to achieve the business transformation;
	(4) A listing of the legacy systems that will not be part of the "to-be" environment and the schedule for terminating these systems;
	(5) 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); and,
	(6) 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).
39	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.
40	A technical (systems, infrastructure, and data) migration plan that shows:
	(1) 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;
	(2) 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;
	(3) A cost estimate for the initial phase(s) of the transition and a high-level cost projection for the transition to the target architecture.
41	A strategy that describes the architecture's governance and control structure and the integrated procedures, processes, and criteria (e.g., inventory management and security) to be followed to ensure that the department's business transformation effort remains compliant with the architecture.

Source: GAO.

68

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

April 11, 2007

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

Dear Mr. Hite:

RE: Draft Report GAO-07-564, Homeland Security: DHS Enterprise Architecture Continues to Evolve but Improvements Needed (GAO Job Code 310641)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the draft report referenced above that addresses enterprise architecture and its role in facilitating organizational transformation. We are pleased that the Government Accountability Office (GAO) recognizes the progress made in the development of the DHS Enterprise Architecture (EA) since the Department was formed four years ago. We continue to make progress in EA development and the recent release of the Homeland Security Enterprise Architecture (HLS EA 2007) addresses many of the remaining issues GAO highlights.

The report recommends that the Department's Chief Information Officer (CIO) include a traceability matrix in future versions of the Department's Enterprise Architecture that explicitly maps EA content to GAO's recommendations in sufficient detail to demonstrate their implementation. We agree with this recommendation. Efforts are currently underway to develop a traceability matrix so that DHS can better track progress and explicitly map EA content to the recommendations.

GAO also recommends that the CIO ensure that future efforts to solicit stakeholder comments on the Department's EA employ an effective approach that includes clearly defining the type of information requested, and allowing sufficient time for obtaining and responding to these comments. We believe that the current process adequately allows for stakeholder input into the DHS EA. The DHS EA Program Management Office works closely with all stakeholders, including component agencies and major programs throughout the year. Stakeholders have unlimited opportunity to comment on and provide input to the EA. Stakeholders have visible insight into the contents of and changes to the EA through weekly EA review meetings of the EA Center of Excellence

www.dhs.gov

and the EA Board. The evolution of the EA is, in fact, guided largely by input from stakeholders. The annual review of the EA by stakeholders is merely a review of the final packaged deliverable content that is intended for review by OMB, which should already be familiar to stakeholders. Moreover, the fact that the GAO audit team counted nearly 400 comments from stakeholders suggests that there was ample opportunity for stakeholders to comment during this period.

We would like to correct the perception of the audit team on how the Department has treated stakeholder comments. Stakeholder input is crucial to the development of the DHS EA. In fact, the EA cannot exist as a useful tool for the Department without stakeholder participation. Many of the unresolved comments touch on areas that will be the focus of future releases of the DHS EA. Furthermore, although the draft report states that 116 comments from stakeholders had no resolution, many of these comments were merely observations about the EA not requiring a resolution.

Thank you again for the opportunity to comment on the draft report. DHS is committed to continuous progress and improvements to Enterprise Architecture to help support our very important mission of securing the homeland. As the Department continues to evolve, the EA will evolve and continue to show progress and improvements with each release.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

MMcP

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the person named above, Mark Bird, Assistant Director; Neil Doherty; Ashfaq Huda; Nancy Glover; Anh Le; Teresa Smith; Amos Tevelow; William Wadsworth; and Kim Zelonis made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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