United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees

For Release on Delivery
Expected at 3:00 p.m. EST
Wednesday, March 29, 2006

HOMELAND SECURITY

Progress Continues, but Challenges Remain on Department's Management of Information Technology

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

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-598T, a testimony before congressional subcommittees

March 29, 2006

HOMELAND SECURITY

Progress Continues, but Challenges Remain on Department's Management of Information Technology

Why GAO Did This Study

Information technology (IT) is a critical tool for the Department of Homeland Security (DHS), not only in performing its mission today, but also in transforming how it will do so in the future. In light of the importance of this transformation and the magnitude of the associated challenges, GAO has designated the implementation of the department and its transformation as high risk.

GAO has reported that in order to effectively leverage IT as a transformation tool, DHS needs to establish certain institutional management controls and capabilities, such as having an enterprise architecture and making informed portfolio-based decisions across competing IT investments. GAO has also reported that it is critical for the department to implement these controls and associated best practices on its many IT investments.

In its past work, GAO has made numerous recommendations on DHS institutional controls and on individual IT investment projects. The testimony is based on GAO's body of work in these areas, covering the state of DHS IT management both on the institutional level and the individual program level.

www.gao.gov/cgi-bin/getrpt?GAO-06-598T.

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 continues to work to institutionalize IT management controls and capabilities (disciplines) across the department. Among these are

- having and using an enterprise architecture, or corporate blueprint, as an authoritative frame of reference to guide and constrain IT investments;
- defining and following a corporate process for informed decision making by senior leadership about competing IT investment options;
- applying system and software development and acquisition discipline and rigor when defining, designing, developing, testing, deploying, and maintaining systems;
- establishing a comprehensive information security program to protect its information and systems;
- having sufficient people with the right knowledge, skills, and abilities to execute each of these areas now and in the future; and
- centralizing leadership for extending these disciplines throughout the organization with an empowered Chief Information Officer.

Over the last 3 years, the department has made efforts to establish and implement these IT management disciplines, but it has more to do. Despite progress, for instance, in developing its enterprise architecture and its investment management processes, much work remains before these and the other disciplines are fully mature and institutionalized. For example, although the department recently completed a comprehensive inventory of its major information systems—a prerequisite for effective security management—it has not fully implemented a comprehensive information security program, and its other institutional IT disciplines are still evolving. The department also has more to do in deploying and operating IT systems and infrastructure in support of core mission operations, such as border and aviation security. For example, a system to identify and screen visitors entering the country has been deployed and is operating, but a related exit capability largely is not. Also, a government-run system to prescreen domestic airline passengers is not yet in place. Similarly, some infrastructure has been delivered, but goals related to consolidating networks and e-mail systems, for example, remain to be fully accomplished.

Similarly, GAO's review of key nonfinancial systems show that DHS has more to do before the IT disciplines discussed above are consistently employed. For example, these programs have not consistently employed reliable cost estimating practices, effective requirements development and test management, meaningful performance measurement, strategic workforce management, and proactive risk management, among other recognized program management best practices.

Until the department fully establishes and consistently implements the full range of IT management disciplines embodied in best practices and federal guidance, it will be challenged in its ability to manage and deliver programs.

Mr. Chairmen and Members of the Subcommittees,

I appreciate the opportunity to participate in today's joint oversight hearing on Department of Homeland Security (DHS) efforts to effectively manage information technology (IT). As you know, IT is a critical tool in DHS's quest to transform 22 diverse and distinct agencies—some with longstanding management weaknesses—into a single, integrated, high-performing department. In light of the importance of this transformation and the magnitude of the associated challenges, in 2003 we designated the implementation of the department and its transformation as a high-risk undertaking.[1]

For DHS to effectively leverage IT as a transformation enabler, we reported in 2004 that it needed to put firmly in place certain institutional management controls and capabilities, such as having an enterprise architecture and a process for making informed portfolio-based decisions across competing IT investments.[2] These controls and capabilities are interrelated management disciplines that collectively help an organization to deliver IT systems and infrastructure on time and on budget, and to do so in a way that minimizes risk and maximizes value to the organization as a whole.

My testimony today addresses the state of DHS IT management on two levels: the institutional level and the individual program level. At the department level, it addresses efforts to establish corporate management controls, such as enterprise architecture, IT investment management, and the empowerment of the Chief Information Officer (CIO) to lead the department's IT activities. At the program level, it addresses the extent to which the institutional management controls are actually being implemented on key nonfinancial systems (such as those related to border and aviation security), pointing out the pitfalls to avoid and best practices to employ in managing these IT investments.

[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, *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*, GAO-04-702 (Washington, D.C.: Aug. 27, 2004).

In summary, DHS continues to work to institutionalize the range of IT management controls and capabilities that our research and past work have shown are fundamental to any organization’s ability to use technology effectively to transform itself and accomplish mission goals.[3] Among these IT management controls and capabilities are

- having and using an enterprise architecture, or corporate blueprint, as an authoritative frame of reference to guide and constrain system investments;
- defining and following a corporate process for informed decision making by senior leadership about competing IT investment options;
- applying system and software development and acquisition discipline and rigor when defining, designing, developing, testing, deploying, and maintaining systems;
- establishing a comprehensive, departmentwide information security program to protect information and systems;
- having sufficient people with the right knowledge, skills, and abilities to execute each of these areas now and in the future; and
- centralizing leadership for extending these disciplines throughout the organization with an empowered Chief Information Officer.

Despite its efforts over the last 3 years, the department has more to do before each of these management controls and capabilities is fully in place and is integral to how each system investment is managed. In this regard, our reviews of key nonfinancial systems show that, for example, DHS IT programs have not consistently employed reliable cost estimating practices, effective requirements development and test management, meaningful performance measurement, strategic workforce management, and proactive management of risks, among other recognized program management best practices.

[3] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001); *Architect of the Capitol: Management and Accountability Framework Needed for Organizational Transformation*, GAO-03-231 (Washington, D.C.: Jan. 17, 2003).

The department also has more to do with respect to deploying and operating the mix of IT systems and infrastructure that are needed to support core mission operations, such as border and aviation security. For example, although a system to identify and screen visitors entering the country has been deployed and is operating, a related exit capability largely is not. Also, a government-run capability to prescreen domestic airline passengers is not yet in place. Similarly, while certain system and infrastructure capabilities have been delivered, goals related to consolidating data centers and networks and employing a common e-mail system, for example, remain to be fully accomplished.

To assist the department in addressing its IT needs and management challenges, we have made a series of recommendations for both institutional and program-specific improvements. Spanning these recommendations is one for ensuring that the CIO is sufficiently empowered to extend management discipline and implement common IT solutions across the department. We look forward to working with DHS leadership as it implements these recommendations.

In preparing this testimony, we drew extensively from our previous work on DHS's IT management controls and capabilities and their application on key department programs and projects. In addition, we reviewed documentation and interviewed responsible DHS officials, including the CIO. All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Background

DHS's mission is to lead the unified national effort to secure America by preventing and deterring terrorist attacks and protecting against and responding to threats and hazards to the nation. DHS also is to ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce.

Created in March 2003, DHS has assumed operational control of about 209,000 civilian and military positions from 22 agencies and offices specializing in one or more aspects of homeland security.[4] The intent behind DHS's merger and transformation was to improve coordination, communication, and information sharing among the multiple federal agencies responsible for protecting the homeland. Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. As we reported before the department was created,[5] such a transformation 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.

Among DHS's transformation challenges, we highlighted the formidable hurdle of integrating numerous mission-critical and mission support systems and associated IT infrastructure. For the department to overcome this hurdle, we emphasized the need for DHS to establish an effective IT governance framework, including controls aimed at effectively managing IT-related people, processes, and tools.

DHS Components and IT Spending

To accomplish its mission, the department 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 external entities. Table 1 shows DHS's principal organizations and their missions. An organizational structure is shown in figure 1.

[4] Some of those specialties are intelligence analysis, law enforcement, border security, transportation security, biological research, critical infrastructure protection, and disaster recovery.

[5] 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).

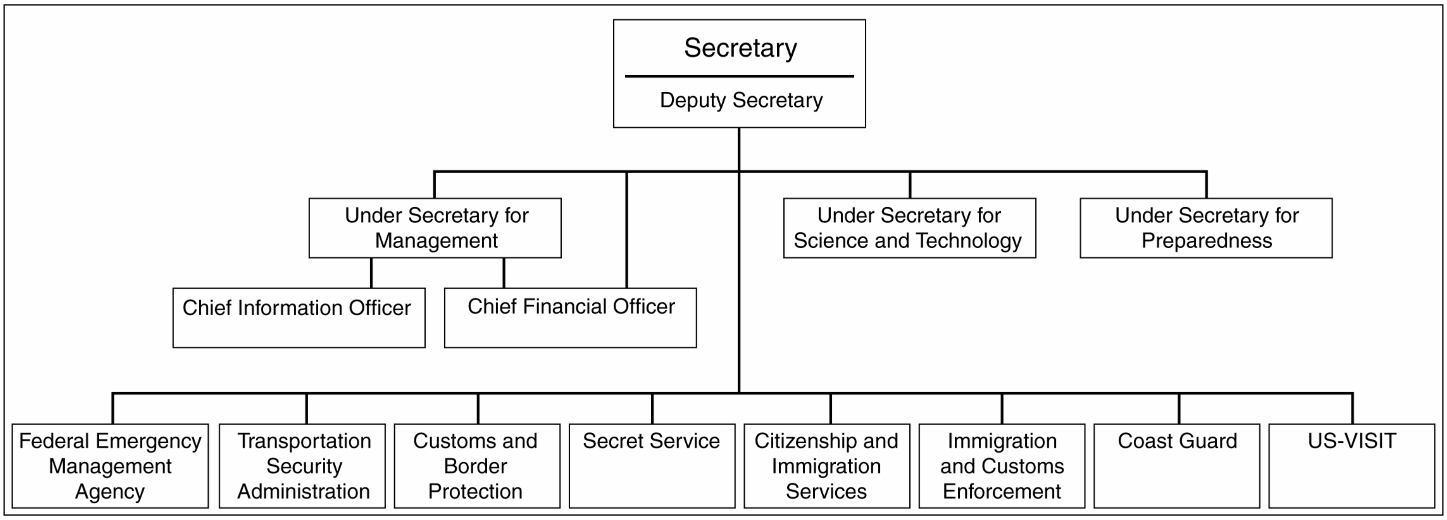
Table 1: DHS's Principal Organizations and Their Missions

Principal organizations[a]	Missions
Citizenship and Immigration Services	Responsible for the administration of immigration and naturalization adjudication functions and establishing 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	Responsible for protecting 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	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	The largest investigative arm of the department, responsible for identifying and shutting down vulnerabilities in the nation's border, economic, transportation, and infrastructure security.
Management Directorate	Responsible for department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. This directorate includes the offices of the Chief Financial Officer and the Chief Information Officer.
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 and capabilities to protect the homeland.
Secret Service	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	Protects the nation's transportation systems to ensure freedom of movement for people and commerce.
US-VISIT	Responsible for developing and implementing 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.

Sources: DHS (data); GAO (analysis).

[a] This table does not show the organizations that fall under each of the directorates. This table also does not show all organizations that report directly to the DHS Secretary and Deputy Secretary, such as executive secretary, legislative and intergovernmental affairs, public affairs, chief of staff, inspector general, and general counsel.

Figure 1: DHS Organizational Structure (Simplified and Partial)


Secretary
Deputy Secretary
Under Secretary for Management
Under Secretary for Science and Technology
Under Secretary for Preparedness
Chief Information Officer
Chief Financial Officer
Federal Emergency Management Agency
Transportation Security Administration
Customs and Border Protection
Secret Service
Citizenship and Immigration Services
Immigration and Customs Enforcement
Coast Guard
US-VISIT

Source: GAO analysis of DHS data.

Within the Management Directorate is the Office of the CIO, which is expected to leverage best available technologies and IT management practices, provide shared services, coordinate acquisition strategies, maintain an enterprise architecture that is fully integrated with other management processes, and advocate and enable business transformation. Other DHS entities also are responsible or share responsibility for critical IT management activities. For example, DHS's major organizational components (e.g., directorates, offices, and agencies) have their own CIOs and IT organizations. Control over the department's IT funding is vested primarily with the components' CIOs, who are accountable to the heads of their respective components.[6]

To promote IT coordination across DHS component boundaries, the DHS CIO established a CIO Council, chaired by the CIO and composed of component-level CIOs. According to its charter, the specific functions of the council include establishing a strategic

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

plan, setting priorities for departmentwide IT, identifying opportunities for sharing resources, coordinating multibureau projects and programs, and consolidating activities.

To accomplish their respective missions, DHS and its component organizations rely extensively on IT. For example, in fiscal year 2006 DHS IT funding totaled about $3.64 billion, and in fiscal year 2007 DHS has requested about $4.16 billion. For fiscal year 2006, DHS reported that this funding supported 279 major IT programs. Table 2 shows the fiscal year 2006 IT funding that was provided to key DHS components.

Table 2: IT Funding for Fiscal Year 2006

Dollars in millions

DHS components and investments	Funding
Citizenship and Immigration Services	388.8
Coast Guard	201.3
Customs and Border Protection	$423.7
Federal Emergency and Management Agency	93.5
Immigration and Customs Enforcement	166.8
Management Directorate	
eMerge2[a]	17.8
Enterprise Application Delivery[b]	20.3
Enterprise Architecture and Investment Management Program[c]	34.6
Enterprise-Geospatial System[d]	13.1
Homeland Secure Data Network[e]	32.7
Human Resources IT[f]	20.8
Information Security Program[g]	54.1
Integrated Wireless Network[i]	261.7
Watch List and Technical Integration[j]	9.9
OCIO salaries and expenses	15.5
Other IT infrastructure[h]	887.2
Other	31.6
Preparedness Directorate	215.4
Science and Technology Directorate	33.2
Secret Service	3.8
Transportation Security Administration	333.2
US-VISIT	341.0
Other DHS components	40.2
Total	**$3,640.2**

Source: GAO analysis of DHS data.

[a] eMerge2 is an initiative planned to integrate the business and financial management policies, processes and systems of DHS into a single solution with the goal of meeting the department's financial management, acquisition, and asset management needs.

[b] Enterprise Application Delivery is intended to consolidate existing and planned Web pages and platforms of the DHS component organizations.

[c] Enterprise Architecture and Investment Management Program is intended to develop the department's enterprise architecture and implement the transition strategy through the department's investment management process.

[d] Enterprise-Geospatial System is planned to establish a framework, organizational structure, and requisite resources to enable departmentwide use of geographic information systems.

[e] Homeland Secure Data Network is an effort to merge disparate classified networks into a single, integrated network to enable, among other things, the secure sharing of intelligence and other information.

[f] HR IT includes the set of DHS enterprisewide systems to support the personnel regulations such as Max^{HR}.

[g] Information Security Program is intended to establish information security policies and procedures throughout the department to protect the confidentiality, integrity, and availability of information.

[h] Other infrastructure includes initiatives with the goal of creating a single, consolidated, and secure infrastructure to ensure connectivity among the department's 22 component organizations.

[i] The Integrated Wireless Network is to deliver the wireless communications services required by agents and officers of DHS, Justice, and Treasury.

[j] Watch List and Technical Integration is to increase effective information sharing by consolidating, re-using, and retiring applications that develop multiple terrorist watch lists being used by multiple operating entities within the government.

GAO Has Reviewed Several of DHS's Mission-Critical IT Programs

In view of the importance of major IT programs to the department's mission, the Congress has taken a close interest in certain mission-critical programs, often directing us to review and evaluate program management, progress, and spending. Among the programs that we have reviewed are the following:

- US-VISIT (the United States Visitor and Immigrant Status Indicator Technology) has several major goals: to enhance the security of our citizens and visitors and ensure the integrity of the U.S. immigration system, and at the same time to facilitate legitimate trade and travel and protect privacy. To achieve these goals, US-VISIT is to record the entry into and exit from the United States of selected travelers, verify their identity, and determine their compliance with the terms of their admission and stay. As of October 2005, US-VISIT officials reported that about $1.4 billion had been appropriated for the program.

- The Automated Commercial Environment (ACE) is a Customs and Border Protection (CBP) program to modernize trade processing systems and support border security. Its goals include enhancing analysis and information sharing with other government agencies; providing an integrated, fully automated information system for commercial import and export data; and reducing costs for the government and the trade community though streamlining. To date, CBP reports that the program has received almost $1.7 billion in funding.
- The America's Shield Initiative (ASI) program (now cancelled) was to enhance DHS's ability to provide surveillance and protection of the U.S. northern and southern borders through a system of sensors, databases, and cameras. The program was also to address known limitations of the current Integrated Surveillance Intelligence System (ISIS) and to support DHS's antiterrorism mission, including its need to exchange information with state, local, and federal law enforcement organizations. As of September 2005, ASI officials reported that about $340.3 million had been spent on the program. As of December 2005, the program was subsumed within the Secure Border Initiative, the department's broader border and interior enforcement strategy.
- The Secure Flight program is developing a system to perform passenger prescreening for domestic flights: that is, the matching of passenger information against terrorist watch lists to identify persons who should undergo additional security scrutiny. The goal is to prevent people suspected of posing a threat to aviation from boarding commercial aircraft in the United States, while protecting passengers' privacy and civil liberties. The program also aims to reduce the number of people unnecessarily selected for secondary screening. To date, TSA officials report that about $144 million has been spent on the program.
- The Atlas program is intended to modernize the IT infrastructure of Immigration and Customs Enforcement (ICE). The goals of the program are to, among other things, improve information sharing, strengthen information security, and improve workforce productivity. ICE estimates the life cycle cost of Atlas to be roughly $1 billion.
- The Student and Exchange Visitor Information System (SEVIS) is an Internet-based system that is to collect and record information on foreign students, exchange visitors, and their dependents—before

they enter the United States, when they enter, and during their stay. Through fiscal year 2006, the department expects to have spent, in total, about $133.5 million on this program.

- The Rescue 21 program is to replace and modernize the Coast Guard's 30-year-old search and rescue communication system, the National Distress and Response System. The modernization is to, among other things, increase the Coast Guard's communication coverage area in the United States; allow electronic tracking of department vessels and other mobile assets; enable better communication with other federal and state systems; and provide for secure communication of sensitive information. The Coast Guard reports that it plans to spend about $373.1 million on the program by the end of fiscal year 2006. It also estimates program's life cycle cost to be $710 million.

IT Management Controls and Capabilities Are Important

Our research on leading private and public sector organizations, as well as our past work at federal departments and agencies, shows that successful organizations embrace the central role of IT as an enabler for enterprisewide transformation.[7] These leading organizations develop and implement institutional or agencywide IT management controls and capabilities (people, processes, and tools) that help ensure that the vast potential of technology is applied effectively to achieve desired mission outcomes. Among these IT management controls and capabilities are

- enterprise architecture development and use,
- IT investment management,
- system development and acquisition process discipline,
- information security management, and
- IT human capital management.[8]

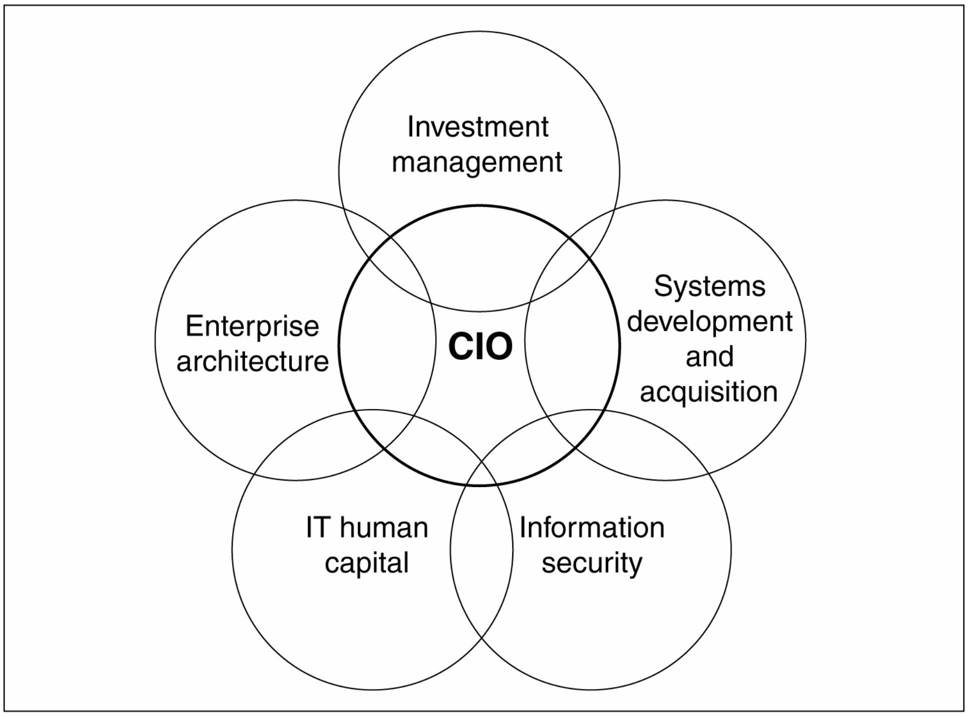
[7] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001); *Architect of the Capitol: Management and Accountability Framework Needed for Organizational Transformation*, GAO-03-231 (Washington, D.C.: Jan. 17, 2003).

[8] Other important IT management controls and capabilities are not addressed in this testimony, such as IT strategic planning and information management.

In addition, these organizations establish these controls and capabilities within a governance structure that centralizes leadership in an empowered CIO.

These controls and capabilities are interdependent and interrelated IT management disciplines, as shown in figure 2. If effectively established and implemented, they can go a long way in determining how successfully an organization leverages IT to achieve mission goals and outcomes.

Figure 2: Interrelated Keys to Successful IT Management



Source: GAO.

Note: Figure shows topics addressed in this testimony; other key IT management areas include IT strategic planning and information management.

DHS Is Making Progress but Has Yet to Fully Institutionalize IT Management Controls and Capabilities

Over the last 3 years, our work has shown that the department has continued to work to establish effective corporate governance and associated IT management controls and capabilities, but progress in each of the key areas has been uneven, and more remains to be accomplished. Until it fully institutionalizes effective governance controls and capabilities, it will be challenged in its ability to leverage IT to support transformation and mission results.

Enterprise Architecture

Leading organizations recognize the importance of having and using an enterprise architecture, or corporate blueprint, as an authoritative operational and technical frame of reference to guide and constrain IT investments. In brief, an enterprise architecture provides systematic structural descriptions—in useful models, diagrams, tables, and narrative—of how a given entity operates today and how it plans to operate in the future, and it includes a road map for transitioning from today to tomorrow. Our experience with federal agencies has shown that attempting to modernize systems without having an enterprise architecture often results in systems that are duplicative, not well integrated, unnecessarily costly to maintain, and limited in terms of optimizing mission performance.[9]

To assist agencies in effectively developing, maintaining, and implementing an enterprise architecture, we published a framework for architecture management, grounded in federal guidance and

[9] See for example, 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).

recognized best practices.[10] The underpinning of this framework is a five-stage maturity framework outlining steps toward achieving a stable and mature enterprise architecture program. The framework describes 31 practices or conditions, referred to as core elements, that are needed for effective architecture management.

We have previously reported on DHS's effort to develop its enterprise architecture from two perspectives. First, in November 2003, we reported on DHS's architecture management program relative to the framework described above.[11] At that time, we found that the department had implemented many of the practices described in our framework. For example, the department had, among other things, assigned architecture development, maintenance, program management, and approval responsibilities; created policies governing architecture development and maintenance; and formulated plans to develop architecture products and begun developing them. Second, in August 2004, we reported on DHS's effort to develop enterprise architecture products, relative to well-established, publicly available criteria on the content of enterprise architectures.[12] At that time, we concluded that the department's initial enterprise architecture provided a foundation upon which to build, but that it was nevertheless missing important content that limited its utility. Thus, it could not be considered a well-defined architecture. In particular, the content of this initial version was not systematically derived from a DHS or national corporate business strategy; rather, it was more the result of an amalgamation of the existing architectures that several of DHS's predecessor agencies already had, along with their respective portfolios of system investment projects. To its credit, the department recognized the limitations of the initial architecture and has developed a new version. To assist DHS in evolving its architecture, we recommended 41 actions aimed at having DHS add

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

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

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

needed architecture content and ensure that architecture development best practices are employed.

Since then, DHS reported that it had taken steps in response to our recommendations. For example, the department issued version 2 of its enterprise architecture in October 2004. According to DHS, this version contained additional business/mission, service, and technical descriptions. Also, this version was submitted to a group of CIOs of major corporations and an enterprise architecture consulting firm, both of which found the architecture meritorious. Earlier this month (March 2006), the department issued another new version of its enterprise architecture, which it calls HLS EA 2006.

Our analysis of version 2 of the department's architecture indicates that DHS has made progress toward development of its architecture products, particularly descriptions of both the "as-is" and "to-be" environments. Specifically, the scope of the "as-is" and "to-be" environments extends to descriptions of business operations, information and data needs and definitions, application and service delivery vehicles, and technology profiles and standards. With respect to the depth and detail of these descriptions (which are the focus of most of our 41 prior recommendations), the department has reported progress, such as (1) completing its first inventory of information technology systems, a key input to its description of the "as-is" environment; (2) establishing departmentwide technology standards; (3) developing and beginning to implement a plan for introducing a shared services orientation to the architecture, particularly with regard to information services (e.g., network, data center, e-mail, help desk, and video operations); and (4) finalizing content for the portion of its architecture that relates to certain border security functions (e.g., the alien detention and removal process that is a major facet of the department's new Strategic Border Initiative).

IT Investment Management

Through IT investment management, organizations define and follow a corporate process to help senior leadership make informed decisions on competing options for investing in IT. Such investments, if managed effectively, can have a dramatic impact on performance and accountability. If mismanaged, they can result in wasteful spending and lost opportunities for improving delivery of services.

Based on our research, we have issued an IT investment management framework[13] that encompasses the best practices of successful public and private sector organizations, including investment selection and control policies and procedures. Our framework identifies, among other things, effective policies and procedures for developing and using an enterprisewide collection—or portfolio—of investments; using such portfolios enables an organization to determine priorities and make decisions among competing options across investment categories based on analyses of the relative organizational value and risks of all investments.[14]

A central tenet of the federal approach to IT investment management is the select/control/evaluate model. During the select phase, the organization (1) identifies and analyzes each project's risks and returns before committing significant funds and (2) selects those projects that will best support its mission needs. In the control phase, the organization ensures that the project continues to meet mission needs at the expected levels of cost and risks. If the project is not meeting expectations or if problems have arisen, steps are quickly taken to address the deficiencies. During the evaluate phase, actual versus expected results are compared after a project has been fully implemented.

[13] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity, Exposure Draft*, GAO/AIMD-10.1.23 (Washington, D.C.: May 2000); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

[14] Our ITIM framework is also consistent with the Clinger-Cohen Act of 1996 (40 U.S.C. §§ 11101-11703), in which Congress enacted provisions requiring federal agencies to focus on results achieved through IT investments and to improve their IT acquisition processes. The act also introduces more rigor and structure into how agencies select and manage IT projects.

In August 2004, we reported[15] that DHS had established an investment management process that included departmental oversight of major IT programs. However, this process was not yet institutionalized: for example, most programs (about 75 percent) had not undergone the departmental oversight process, and resources were limited for completing control reviews in a timely manner. At that time, the CIO and other DHS officials attributed these shortfalls, in part, to the fact that the department's process was maturing and needed to improve. Based on our findings, we made recommendations aimed at strengthening the process.

In March 2005,[16] we again reported on this investment review process, noting that it incorporated many best practices and provided its senior leaders with the information required to make well-informed investment decisions at key points in the investment life cycle. However, we also concluded that at some key investment decision points, DHS's process did not require senior management attention and oversight. For example, management reviews are not required at key system and subsystem decision points, although such reviews (especially with complex systems that incorporate new technology like US-VISIT) are critical to ensuring that risk is reduced before the organization commits to the next phase of investment. Accordingly, we made further recommendations to improve the process.

Further, the CIO recently reported additional steps being taken to strengthen IT investment management. According to the CIO, DHS has

- established an acquisition project performance reporting system, which requires periodic reporting of cost, schedule, and performance measures as well as earned value metrics, as means to monitor and control major acquisitions;

[15] GAO, *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*, GAO-04-702 (Washington, D.C.: Aug. 27, 2004).

[16] GAO, *Homeland Security: Successes and Challenges in DHS's Efforts to Create an Effective Acquisition Organization*, GAO-05-179 (Washington, D.C.: Mar. 29, 2005).

- aligned the investment management cycle and associated milestones with the department's annual budget preparation process to allow business cases for major investments to be submitted to department headquarters at the same time as the budget, rather than as a follow-on;
- linked investment management systems to standardize and make consistent the financial data used to make investment decisions;
- verified alignment of approximately $2 billion worth of investments via the department's portfolio management framework; and
- completed investment oversight reviews (by total dollar value) of over 75 percent of the department's major investments.

The department has also developed a standard template for capturing information about a given IT program to be used in determining the investment's alignment with the enterprise architecture. Such alignment is important because it ensures that programs will be defined, designed, and developed in a way that avoids duplication and promotes interoperability and integration. However, the department has yet to document a methodology, with explicit criteria, for making its judgments about the degree of alignment. Instead, it relies on the undocumented and subjective determinations of individuals in its Enterprise Architecture Center of Excellence.

Systems Development and Acquisition Management

Managing systems development and acquisition effectively requires applying engineering and acquisition discipline and rigor when defining, designing, developing and acquiring, testing, deploying, and maintaining IT systems and services. Our work and other best practice research have shown that applying such rigorous management practices improves the likelihood of delivering expected capabilities on time and within budget. In other words, the quality of IT systems and services is largely governed by the quality of the management processes involved in developing and acquiring them.

Best practices in systems development and acquisition include following a disciplined life cycle management process, in which key activities and phases of the project are conducted in a logical and orderly process and are fully documented. Such a life cycle process begins with initial concept definition and continues through requirements determination to design, development, various phases of testing, implementation, and maintenance. For example, expected system capabilities should be defined in terms of requirements for functionality (what the system is to do), performance (how well the system is to execute functions), data (what data are needed by what functions, when, and in what form), interface (what interactions with related and dependent systems are needed), and security. Further, system requirements should be unambiguous, consistent with one another, linked (that is, traceable from one source level to another),[17] verifiable, understood by stakeholders, and fully documented.

The steps in the life cycle process each have important purposes, and they have inherent dependencies among themselves. Thus, if earlier steps are omitted or deficient, later steps will be affected, resulting in costly and time-consuming rework. For example, a system can be effectively tested to determine whether it meets requirements only if these requirements have already been completely and correctly defined. Concurrent, incomplete, and omitted activities in life cycle management exacerbate the program risks. Life cycle management weaknesses become even more critical as the program continues, because the size and complexity of the program will likely only increase, and the later problems are found, the harder and more costly they will likely be to fix.

These steps, practices, and processes are embedded in an effective systems development life cycle (SDLC) methodology, which sets forth the multistep process of developing information systems from investigation of initial requirements through analysis, design, implementation, maintenance, and disposal. Organizations generally

[17] Examples of higher order sources include legislation, which may dictate certain requirements, and other system documentation, such as the operational concept. When requirements are managed well, traceability can be established from the source requirements to lower level requirements and from the lower level back to their source. Such bidirectional traceability helps determine that all source requirements have been addressed completely and that all lower level requirements can be verified as derived from a valid source.

formalize their SDLC in policies, procedures, and guidance. Currently, many of the major DHS components are following the processes established under their predecessor organizations. For example, both the Transportation Security Administration and CBP have their own SDLCs. As part of our reviews of DHS IT management and specific IT programs, we have not raised any issues or identified any shortcomings with these SDLCs.

DHS is currently drafting policies and procedures to establish a departmentwide SDLC methodology and thus provide a common management approach to systems development and acquisition. According to DHS, the goals of the SDLC are to help

- align projects to mission and business needs and requirements;
- incorporate accepted industry and government standards, best practices, and disciplined engineering methods, including IT maturity model concepts;
- ensure that formal reviews and approvals required by the process are consistent with DHS's investment management process; and
- institute disciplined life cycle management practices, including planning and evaluation in each phase of the information system life cycle.

The department's SDLC, currently in draft form, is to apply to DHS's IT portfolio as well as other capital asset acquisitions. Under the SDLC, each program will be expected to, among other things,

- follow disciplined project planning and management processes balanced by effective management controls;
- have a comprehensive project management plan;
- base project plans on user requirements that are clearly articulated, testable, and traceable to the work products produced; and
- integrate information security activities throughout the SDLC.

Information Security Management

Effective information security management depends on establishing a comprehensive program to protect the information and information systems that support an organization's operations and assets. The overall framework for ensuring the effectiveness of federal information security controls is provided by the Federal Information Security Management Act of 2002.[18] In addition, OMB Circular No. A-130 requires agencies to provide information and systems with protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to these assets or their loss, misuse, or modification.

Because of continuing evidence indicating significant, pervasive weaknesses in the controls over computerized federal operations, we have designated information security as a governmentwide high-risk issue since 1997.[19] Moreover, related risks continue to escalate, in part because the government is increasingly relying on the Internet and on commercially available IT products. Concerns are increasing regarding attacks for the purpose of crime, terrorism, foreign intelligence gathering, and acts of war, as well as by the disgruntled insider, who may not need particular expertise to gain unrestricted access and inflict damage or steal assets. Without an effective security management program, an organization has no assurance that it can withstand these and other threats.

Since it was established, both we and the department's inspector general (IG) have reported that although the department continues to improve its IT security, it remains a major management challenge. For example, within its first year the department had appointed a chief information security officer and developed and disseminated information system security policies and procedures, but it had not completed a comprehensive inventory of its major IT systems—a prerequisite for effective security management.

In June 2005, we reported that DHS had yet to effectively implement a comprehensive, departmentwide information security program to protect the information and information systems that support its

[18] Pub. L. No. 107-347, tit. III, § 301, 116 Stat. 2946, 2946-55 (Dec. 17, 2002) (codified at 44 U.S.C. §§ 3541-3549).

[19] See GAO, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

operations and assets.[20] In particular, although it had developed and documented departmental policies and procedures that could provide a framework for implementing such a program, certain departmental components had not yet fully implemented key information security practices and controls. Examples of weaknesses in components' implementation included incomplete or missing elements in risk assessments, security plans, and remedial action plans, as well as incomplete, nonexistent, or untested continuity of operations plans. To address these weaknesses, we made recommendations aimed at ensuring that DHS fully implement the key information security practices and controls.

More recently, the DHS IG reported that DHS's components have not completely aligned their respective information security programs with DHS's overall policies, procedures, and practices.[21] However, the IG also reported progress. According to the IG, DHS completed actions to eliminate two obstacles that had significantly impeded the department in establishing its security program: First, it completed the comprehensive system inventory mentioned earlier, including major applications and general support systems for all DHS components. Second, it implemented a departmentwide tool that incorporates the guidance required to adequately complete security certification and accreditation for all systems. The IG also reported that the CIO had developed a plan to accredit all systems by September 2006.

The DHS CIO testified earlier this month (March 2006) on progress in implementing the department's certification and accreditation plan, stating that the department is well on its way to achieving its September 2006 target for full system accreditation.[22] The CIO also stated that by the end of February 2006, more than 60 percent of the

[20] GAO, *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program*, GAO-05-700 (Washington, D.C.: June 17, 2005).

[21] DHS Office of Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, OIG-06-14 (Washington, D.C.: December 2005).

[22] Statement by Scott Charbo, DHS CIO, before the House Committee on Government Reform (Washington, D.C.: Mar. 16, 2006).

over 700 systems in its inventory were fully accredited, up from about 26 percent 5 months earlier.

IT Human Capital Management

A strategic approach to human capital management includes viewing people as assets whose value to an organization can be enhanced by investing in them,[23] and thus increasing both their value and the performance capacity of the organization. Based on our experience with leading organizations, we issued a model[24] encompassing strategic human capital management, in which strategic human capital planning was one cornerstone.[25] Strategic human capital planning enables organizations to remain aware of and be prepared for current and future needs as an organization, ensuring that they have the knowledge, skills, and abilities needed to pursue their missions. We have also issued a set of key practices for effective strategic human capital planning.[26] These practices are generic, applying to any organization or component, such as an agency's IT organization. They include

- involving top management, employees, and other stakeholders in developing, communicating, and implementing a strategic workforce plan;
- determining the critical skills and competencies needed to achieve current and future programmatic results;
- developing strategies tailored to address gaps between the current workforce and future needs;
- building the capability to support workforce strategies; and

[23] See GAO, *Human Capital: Attracting and Retaining a High-Quality Information Technology Workforce*, GAO-02-113T (Washington, D.C.: Oct. 4, 2001); *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002); *Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[24] GAO-02-373SP.

[25] The other three are leadership; acquiring, developing, and retaining talent; and results-oriented organizational culture.

[26] GAO-04-39.

- monitoring and evaluating an agency's progress toward its human capital goals and the contribution that human capital results have made to achieving programmatic goals.

In June 2004, we reported that DHS had begun strategic planning for IT human capital at the headquarters level, but it had not yet systematically gathered baseline data about its existing workforce. Moreover, the DHS CIO expressed concern over staffing and acknowledged that progress in this area had been slow.[27] In our report, we recommended that the department analyze whether it had appropriately allocated and deployed IT staff with the relevant skills to obtain its institutional and program-related goals. In response, DHS stated that on July 30, 2004, the CIO approved funding for an IT human capital Center of Excellence. This center was tasked with delivering plans, processes, and procedures to execute an IT human capital strategy and to conduct an analysis of the skill sets of DHS IT professionals.

Since that time, DHS has undertaken a departmentwide human capital initiative, MAX^{HR}, which is to provide greater flexibility and accountability in the way employees are paid, developed, evaluated, afforded due process, and represented by labor organizations. Part of this initiative involves the development of departmentwide workforce competencies. According to the DHS IG, the department intended to implement MAX^{HR} in the summer of 2005, but federal district court decisions have delayed the department's plans. However, the IG stated that the classification, pay, and performance management provisions of the new program are moving forward, with implementation of the new performance management system beginning in October 2005. According to the IG, the new pay system is planned for implementation by January 2007 for some DHS components.

[27] GAO, *Human Capital: DHS Faces Challenges In Implementing Its New Personnel System*, GAO-04-790 (Washington, D.C.: June 18, 2004).

CIO Leadership

According to our research on leading private and public sector organizations and experience at federal agencies, leading organizations adopt and use an enterprisewide approach to IT governance under the leadership of a CIO or comparable senior executive, who has responsibility and authority, including budgetary and spending control, for IT across the entity.[28]

In May 2004, we reported that the DHS CIO did not have authority and control over departmentwide IT spending.[29] Control over the department's IT budget was vested primarily with the CIO organizations within each DHS component, and the components' CIO organizations were accountable to the heads of the components. As a result, DHS's CIO did not have authority to manage IT assets across the department. Accordingly, we recommended that the Secretary examine the sufficiency of spending authority vested in the CIO and take appropriate steps to correct any limitations in authority that constrain the CIO's ability to effectively integrate IT investments in support of departmentwide mission goals.

Since then, the DHS IG has reported that the DHS CIO is not well positioned to accomplish IT integration objectives.[30] According to the IG, despite federal laws and requirements, the CIO is not a member of the senior management team with authority to strategically manage departmentwide technology assets and programs. The IG reported that steps were taken to formalize reporting relationships between the DHS CIO and the CIOs of major component organizations, but that the CIO still does not have

[28] For example, see GAO, *Architect of the Capitol: Management and Accountability Framework Needed for Organizational Transformation*, GAO-03-231 (Washington, D.C.: Jan. 17, 2003) and *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001).

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

[30] DHS Office of Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, OIG-06-14 (Washington, D.C.: December 2005).

sufficient staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support departmental units. The IG expressed the view that although the CIO currently participates as an integral member at each level of the investment review process, the department would benefit from following the successful examples of other federal agencies in positioning their CIOs with the authority and influence needed to guide executive decisions on departmentwide IT investments and strategies.

In response to the IG's comments, the DHS CIO stated that his office is properly positioned and has the authority it needs to accomplish its mission. According to the CIO, the office is the principal IT authority to the Secretary and Deputy Secretary, and it will continue to hold that leadership role within the department.

DHS Is Making Some Progress in Implementing IT Systems and Infrastructure

A gauge of DHS's progress in managing its IT investments is the extent to which it has deployed and is currently operating more modern IT systems and infrastructure. To the department's credit, our reviews have shown progress in these areas, and DHS has reported other progress. However, our reviews have also shown that IT programs have not met stated goals for deployed capabilities, and DHS's own reporting shows that infrastructure goals have yet to be fully met.

To expedite the implementation of IT systems, the department has developed and deployed system capabilities incrementally, which we support, as this is a best practice and consistent with our recommendations.[31] For example, the department has successfully delivered visitor entry identification and screening capabilities with the first three increments of its US-VISIT program, and it is currently

[31] Clinger-Cohen Act of 1996, Pub. L. 104-106; OMB, *Management of Federal Information Resources*, Circular A-130 (Nov. 28, 2000).

implementing release four of its ACE program. At the same time, however, US-VISIT exit capabilities are not in place, and release four of ACE does not include needed functionality. Further, some IT programs that either were or have been under way for years have not delivered any functionality, such as the canceled ASI program and the Secure Flight program.

In addition, the department has recently reported a number of accomplishments relative to IT infrastructure; however, what has been reported also shows that much remains to be accomplished before infrastructure-related efforts produce deployed and operational capabilities. For example, the department reports that it has begun its Infrastructure Transformation Program (ITP), which is its approach to moving to a consolidated, integrated, and services-oriented IT infrastructure. According to the department, the CIO developed and has begun implementing the ITP plan, which is to be centrally managed but executed in a distributed manner, with various DHS components taking the lead for different areas of infrastructure transformation.[32] The ITP is to create a highly secure and survivable communications network (OneNet) for Sensitive but Unclassified data across the department, and it is also to establish a common and reliable e-mail system across the department. The department reported that it had deployed the initial core of the DHS OneNet and built the primary Network Operation Center to monitor OneNet performance. Among the other goals of the program are consolidated data centers to reduce costs and provide a highly survivable and reliable computing environment. In this regard, the department reported that it has now established an interim data center.

In addition, the department stated that it has extended its classified networking capabilities by fielding 56 Secret sites on the department's Homeland Secure Data Network and by completing the connection of this network to SIPRNet (the Defense Department's Secret Internet Protocol Routed Network). DHS also

[32] For instance, CBP is the lead for network services and data centers; the Coast Guard is the lead for e-mail and help desk services; and the Federal Emergency Management Agency is the lead on video operations services.

reported that it has established an Integrated Wireless Program Plan, which provides a program management framework to ensure the on-time cost and schedule performance of wireless programs and projects.

Key IT Programs Reflect Mixed Use of Effective IT Management Practices

A key measure of how well an organization is managing IT is the degree to which its IT-dependent programs actually implement corporate management controls and employ associated best practices. In this regard, our reviews of several nonfinancial DHS IT programs provide examples of both strengths and weaknesses in program management. In summary, they show that DHS IT programs are not being managed consistently: some programs are at least partially implementing certain program management best practices, but others are largely disregarding most of the practices. Further, they show that most of the programs are considerably challenged in certain key areas, such as measuring progress and performance against program commitments and establishing human capital capabilities.

IT investment alignment with the enterprise architecture. An important element of enterprise architecture management is ensuring that IT investments comply with the architecture. However, in several of the programs that we have reviewed, investments have been approved without documented analysis to support these judgments and to permit the judgments to be independently verified. For example, DHS approved the ACE program's alignment with the department's architecture on the recommendation of its Enterprise Architecture Center of Excellence and Enterprise Architecture Board. However, the Center's evaluators did not provide a documented analysis that would allow independent verification. According to DHS officials, they do not have a documented methodology for evaluating programs' architecture compliance, and instead rely on the professional expertise of Center staff. In contrast, the ASI program provides an example of an instance in which the reviews required to ensure architecture alignment resulted in the discovery of a significant problem: the program had not adequately defined its relationships and dependencies with other department programs.[33] As a result, the program was reconsidered and later subsumed within the new Secure Border Initiative, the department's broader strategy for border and interior enforcement.

Reliable cost estimates. Reliable cost estimates are prerequisites both for developing an economic justification for a program and for establishing cost baselines against which to measure progress. DHS IT programs that we reviewed have demonstrated mixed results in this regard. For example, the ACE program has made considerable progress in implementing our recommendation to ensure that its development contractor's cost estimates are reconciled with independent cost estimates, and that the derivation of both estimates is consistent with published best practices. However, cost estimating remains a major challenge for other DHS IT programs. For example, Secure Flight did not have cost estimates for either initial or full operating capability, nor did it have a life-cycle cost estimate (estimated costs over the expected life of a program, including direct and indirect costs and costs of operation and maintenance). Also, for the US-VISIT program's analysis of proposed alternatives for monitoring the exit of travelers, cost estimates did not meet key criteria for reliable cost estimating as established in the published best practices mentioned above. For example, they did not include detailed work breakdown structures defining the work to be performed, so that associated costs could be identified and estimated. Such a work breakdown structure provides a reliable basis for ensuring that estimates include all relevant costs. Without reasonable cost estimates, it is not possible to produce an adequate economic justification for choosing among alternatives, and program performance cannot be adequately measured.

[33] In February 2006, we reported that the DHS Deputy Secretary had directed that the program be reevaluated within the department's broader border and interior enforcement strategy, now referred to as the Secure Border Initiative. See GAO, *Border Security: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program*, GAO-06-295 (Washington, D.C.: Feb. 22, 2006).

Earned value management. To help ensure that reliable processes are used to measure progress against cost and schedule commitments, OMB requires agencies to manage and measure major IT projects[34] through use of an earned value management (EVM) system that is compliant with specified standards.[35] On programs we reviewed, however, the use of EVM was as yet limited. For example, although the ACE program had instituted the use of EVM on recent releases, its use for one release was suspended in June 2005, because staff assigned to the release were unfamiliar with the technique. For another release, EVM was not used because, according to program officials, the release had not established the necessary cost and schedule baseline estimates against which earned value could be measured. ACE officials told us that they plan to establish baselines and use EVM for future work. With regard to the US-VISIT program, although EVM is to be used in managing the prime integration contract, it has not been used in a number of US-VISIT related contracts over the last 3 years. According to DHS, in fiscal year 2005, 30 percent of departmental programs were using EVM.

Performance management and accountability. To ensure that programs manage their performance effectively, it is important that they define and measure progress against program commitments and hold themselves accountable for results. These program commitments include expected or estimated (1) capabilities and associated use and quality; (2) benefits and mission value; (3) costs; and (4) milestones and schedules. To be accountable, projects need first to develop and maintain reliable and current expectations and then to define and select metrics to measure progress against these. However, in our reviews of DHS programs (such as those that are required to prepare expenditure plans for Senate and House appropriations subcommittees before obligating funding), we have

[34] Specifically, OMB requires agencies to use this method on all new major IT projects, ongoing major IT developmental projects, and high-risk projects.

[35] EVM is a project management tool that integrates the investment scope of work with schedule and cost elements for investment planning and control. This method compares the value of work accomplished during a given period with that of the work expected in the period. Differences in expectations are measured in both cost and schedule variances.

reported that program performance and accountability has been a challenge. For example, the fiscal year 2004 expenditure plan for the Atlas program did not provide sufficient information on program commitments to allow the Congress to perform effective oversight. On the other hand, although the ACE program office is still not where it needs to be in this regard, it has made progress in this area: it has now prepared an initial version of a program accountability framework that includes measuring progress against costs, milestones and schedules, and risks for select releases. However, ACE benefit commitments are still not well defined, and the performance targets being used were not always realistic. On other programs, such as SEVIS, we found that while some performance aspects of the system were being measured, others were not such as network usage.

Disciplined acquisition and development processes. Our reviews of DHS programs have disclosed numerous weaknesses in key process areas related to system acquisition and management, such as requirements development and management, test management, project planning, validation and verification, and contract management oversight. For example, we reported that the Atlas program office, which had been recently established, had not yet implemented any of these key process areas.[36] For the ACE program, weaknesses in requirements definition were a major reason for recent problems and delays, including the realization during pilot testing that key functionality had not been defined and built into the latest release. For US-VISIT, test plans were incomplete in that they did not, among other things, adequately demonstrate traceability between test cases and the requirement to be verified by testing. Also, both ASI and Secure Flight were proceeding without complete and up-to-date program management plans, and Secure Flight's requirements were not well developed. In addition, key ASI acquisition controls, such as contract management oversight, were not yet defined. This led to a number of problems in ASI deploying, operating, and maintaining ISIS technology. Further, ACE and US-

[36] GAO, *Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program*, GAO-05-805 (Washington, D.C.: Sept. 7, 2005).

VISIT projects have not always effectively employed independent verification and validation.

Risk management. Effective risk management is vital to the success of any system acquisition. Accordingly, best practices[37] advocate establishing management structures and processes to proactively identify facts and circumstances that can increase the probability of an acquisition's failing to meet cost, schedule, and performance commitments and then taking steps to reduce the probability of their occurrence and impact. Our work on the ACE, US-VISIT, and ASI programs, for example, showed that risk management programs were in place, but not all risks were being effectively addressed. In particular, key risks on the ACE program were not being effectively addressed. Specifically, the ACE program schedule had introduced significant concurrency in the development and deployment of releases; as both prior experience on the ACE program and best practices show, such concurrency causes contention for common resources, which in turn produces schedule slips and cost overruns. Also, the ACE program was passing key milestones with known severe system defects—that is, allowing development to proceed to the next stage even though significant problems remained to be solved. This led to a recurring pattern of addressing quality problems with earlier releases by borrowing resources from future releases, which led to schedule delays and cost overruns. Moreover, it led the program to deploy one release prematurely with the intention of gaining user acceptance sooner. However, this premature deployment actually produced a groundswell of user complaints and poor user satisfaction scores with the release.

Similar risks were experienced on the Coast Guard's Rescue 21 program. For example, we reported that the Coast Guard's plan to compress and overlap key tests introduced risks, and subsequently the Coast Guard decided to postpone several tests.[38]

[37] Software Engineering Institute, Software Acquisition Capability Maturity Model® version 1.03, CMU/SEI-2002-TR-010 (Pittsburgh, PA: March 2002).

[38] GAO, *Coast Guard: New Communication System to Support Search and Rescue Faces Challenges*, GAO-03-1111 (Washington, D.C.: Sept. 30, 2003).

Security. The selection and employment of appropriate security and privacy controls for an information system are important tasks that can have major implications for the operations and assets and for the protection of personal information that is collected and maintained in the system. Security controls are the management, operational, and technical safeguards prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Privacy controls limit the collection, use, and disclosure of personal information.

For several IT programs, security and privacy has been a challenge. For example, we reported[39] in September 2003 and again in May 2004 that the US-VISIT program office had yet to develop a security plan as required by OMB and other federal guidance, although the program later developed a plan that was generally consistent with applicable guidance. However, the program office had not conducted a security risk assessment or included in the plan when such an assessment would be completed. OMB and other federal guidance specifies that security plans should describe the methodology that is used to identify system threats and vulnerabilities and to assess the risks, and include the date the assessment was completed.

In addition, we reported that the Atlas program was relying on a bureauwide security plan that did not address Atlas infrastructure requirements. Further, Atlas had yet to develop a privacy impact assessment to determine what effect, if any, the system would have on individual privacy, the privacy consequences of processing certain information, and alternatives considered to collect and handle the information.

On TSA's Secure Flight program, although the agency had taken steps to implement security to protect system information and assets, we recently reported that these steps were individually

[39] *Homeland Security: First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed*, GAO-04-586 (Washington, D.C.: May 11, 2004); and *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, GAO-03-1083 (Washington, D.C.: Sept. 19, 2003).

incomplete and collectively fell short of a comprehensive program consistent with federal guidance and associated best practices. More specifically, OMB and other federal guidance and relevant best practices call for agencies to, among other things, (1) conduct a systemwide risk assessment that is based on system threats and vulnerabilities and (2) then develop system security requirements and related policies and procedures that govern the operation and use of the system and address identified risks. Although TSA developed two system security plans—one for the underlying infrastructure (hardware and software) and another for the Secure Flight system application—neither was complete. Specifically, the infrastructure plan only partially defined the requirements to address the risks, and the application plan did not include any requirements addressing risks. Furthermore, we also recently reported[40] that TSA did not fully disclose to the public, as required by privacy guidance, its use of personal information during the testing phase of Secure Flight until after many of the tests had been completed.

Establishing and maintaining adequate staffing. Implementing the IT management processes that I have been describing requires that programs have the right people—not only people who have the right knowledge, skills, and abilities, but also enough of them to do the job. Generally, all the programs we reviewed were challenged, particularly in their initial stages, to assemble sufficient staff with the right skill mix and to treat workforce (human capital) planning as a management imperative. For example, we reported that both the Atlas and the ASI programs were initiated without being adequately staffed. In addition, in September 2003 we reported that the US-VISIT program office had assessed its staffing needs for acquisition management at 115 government and 117 contractor personnel, but that at the time the program had 10 staff within the program office and another 6 staff working closely with them.[41]

[40] GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

[41] GAO, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, GAO-03-1083 (Washington, D.C.: Sept. 19, 2003);

Since then, US-VISIT has filled 102 of its 115 planned government positions (with plans in place to fill the remaining positions) and all of its planned 117 contractor positions.[42]

However, to ensure that staffing needs continue to be met, organizations need to manage human capital strategically, which entails identifying the program functions that need to be performed and the associated numbers and skill sets (core competencies) needed to perform them, assessing the on-board workforce relative to these needs, identifying gaps, and developing and implementing strategies (i.e., hiring, retention, training, contracting) for filling these gaps over the long-term. In this regard, the US-VISIT program has made considerable progress. Specifically, we recently reported that it has analyzed the program office's workforce to determine diversity trends, retirement and attrition rates, and mission-critical and leadership competency gaps, and it has updated the program's core competency requirements to ensure alignment between the program's human capital and business needs. In contrast, although the ACE program has taken various informal steps to bolster its workforce (such as providing training), it has been slow to document and implement a human capital strategy that compares competency-based staffing needs to on-board capabilities and includes plans for closing shortfalls.

In closing, let me reiterate that we have made a series of recommendations to the department aimed at addressing both the department's institutional IT management challenges and its IT program-specific weaknesses. To the department's credit, it has largely agreed with these recommendations. Although some of these have been implemented, most are still works in process. In my view, these recommendations provide a comprehensive framework for strengthening DHS's management of IT and increasing the chances of delivering promised system capabilities and benefits on time and within budget. We look forward to working constructively with the

[42] GAO, *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented*, GAO-06-296 (Washington, D.C.: Feb. 14, 2006).

department in implementing these recommendations and thereby maximizing the role that IT can play in DHS's transformation efforts.

Mr. Chairmen, this concludes my statement. I would be happy to answer any questions at this time.

Contacts and Acknowledgments

For future information regarding this testimony, please contact Randy Hite, Director, Information Technology Architecture and Systems Issues, at (202) 512-3439, or hiter@gao.gov. Other individuals who made key contributions to this testimony were Mathew Bader, Mark Bird, Justin Booth, Barbara Collier, Deborah Davis, Michael Holland, Ash Huda, Gary Mountjoy, and Scott Pettis.

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

PRINTED ON RECYCLED PAPER