United States Government Accountability Office

GAO

Report to Congressional Committees

August 2004

DEPARTMENT OF HOMELAND SECURITY

Formidable Information and Technology Management Challenge Requires Institutional Approach

GAO-04-702

August 2004

DEPARTMENT OF HOMELAND SECURITY

Formidable Information and Technology Management Challenge Requires Institutional Approach

GAO Highlights

Highlights of GAO-04-702, a report to the Chairman, Senate Committee on Governmental Affairs, and the Chairman, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

Why GAO Did This Study

In 2003 GAO designated the merger of 22 separate federal entities into the Department of Homeland Security (DHS) as a high risk area because of the criticality of the department's mission and the enormous transformation challenges that the department faced. Given that the effective use of information technology (IT) is a critical enabler of this merger, GAO has previously reported on a number of DHS efforts aimed at institutionalizing an effective information and technology governance structure and investing in new IT systems that are intended to better support mission operations.

Now that DHS has been operating for over a year, GAO was asked to, based largely on its prior work, describe DHS's progress in meeting its information and technology management challenge.

What GAO Recommends

To strengthen DHS's IT strategic planning, GAO recommends that the department establish IT goals, performance measures, and milestones, and analyze whether its IT staffing adequately supports those goals. In commenting on a draft of this report, DHS generally concurred with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-702.

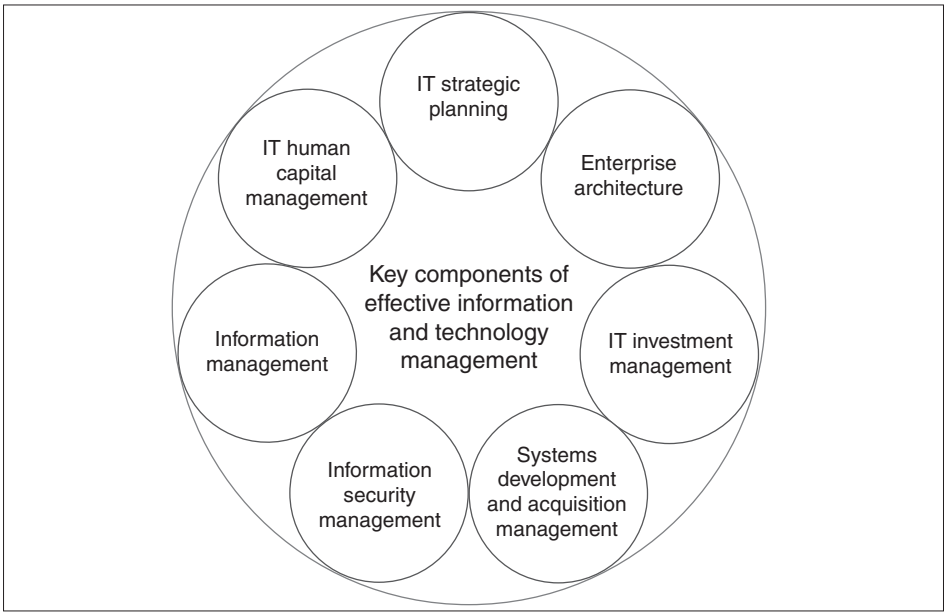
To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

DHS's overall IT challenge is to standardize and integrate the legacy system environments and management approaches that it inherited from its predecessor agencies, while concurrently attempting to ensure that present levels of IT support for critical homeland security operations are not only maintained but improved in the near term. To accomplish this, the department is in the process of instituting seven information and technology management disciplines that are key elements of an effective information and technology management structure (see chart).

DHS's progress in institutionalizing these key information and technology management elements has been mixed, and overall remains a work in progress. Such progress is not unexpected, given the diversity of the inherited agencies and the size and complexity of the department's mission operations. Nevertheless, because DHS has not yet fully institutionalized these governance elements, its pursuit of new and enhanced IT investments are at risk of not optimally supporting corporate mission needs and not meeting cost, schedule, capability, and benefit commitments. Accordingly, GAO has previously made recommendations relative to most of these areas to the department's chief information officer and other responsible DHS entities. Lastly, DHS has developed a draft IT strategic plan, which GAO finds lacking in explicit goals, performance measures, milestones, and knowledge of whether it has properly positioned IT staff with the right skills to accomplish these things.

Key Elements of Effective Information and Technology Management Structure



Source: GAO.

Contents

Abbreviations

ACE	Automated Commercial Environment
CAPPS II	Computer-Assisted Passenger Prescreening System II
CIO	chief information officer
DHS	Department of Homeland Security
IRM	information resources management
IT	information technology
OMB	Office of Management and Budget
SEVIS	Student Exchange Visitor Information System
TSA	Transportation Security Administration
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

GAO
Accountability * Integrity * Reliability

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

August 27, 2004

The Honorable Susan M. Collins
Chairman, Committee on Governmental Affairs
United States Senate

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

Responding to real and potential threats to homeland security is one of the federal government's most significant challenges. To address this challenge, as you know, the Homeland Security Act of 2002 (P.L. 107-296) merged 22 federal agencies and organizations with homeland security-related missions into the Department of Homeland Security (DHS). Since becoming operational in March 2003, DHS has faced the considerable challenge of transforming these diverse organizations into a single new cabinet-level department. The information technology (IT) task related to DHS's transformation is complex and critical to the agency's success. According to DHS's Deputy Secretary, to help detect and deter future terrorist attacks, DHS must rationalize disparate technologies with conflicting business rules, consolidate data centers and networks, have a common e-mail system, get the right information to border agents, and prevent cyber attacks against the department's mission-critical systems.[1]

Critical to meeting DHS's challenge is establishing an effective corporate information and technology management governance process at the same time that the department is investing billions of dollars to develop, acquire, maintain, and operate mission-critical systems. Ideally, DHS's corporate governance structure would be in place prior to the department's making significant IT investments so that such investment decisions reflect departmentwide needs and priorities. Yet, the operational reality of starting a new organization such as DHS is that it must strike a balance between its pursuit of new and enhanced systems (that in some cases are being managed using legacy processes) and establishing the means for achieving

[1]Statement of Admiral James Loy, Deputy Secretary, Department of Homeland Security, before the House Select Committee on Homeland Security, May 6, 2004.

a family of systems that optimally support departmentwide operations and mission performance.

Since DHS has been operational for over a year, you requested that we describe the state of DHS's information and technology management. Accordingly, our objective is to describe DHS's progress in meeting its information and technology management challenge. To address this objective we reviewed and synthesized our prior reports and those of the DHS Office of Inspector General on the department's information and technology management and specific IT investments. (A list of related GAO products is included at the end of this report.) We also reviewed relevant documentation to obtain more up-to-date information on changes to the department's processes, particularly as it relates to IT strategic planning and IT investment management. This documentation included DHS's draft information resources management (IRM) strategic plan, draft road maps related to its eight IT priority areas, and the department's investment review management directive and related guidance documents. As part of reviewing these changed processes and to discuss steps that the department has taken to address certain of our open recommendations, we also interviewed appropriate DHS IT officials, including the chief information officer (CIO), chief technology officer, and the coordinator for its top level investment management boards. We performed our work at DHS in Washington, D.C., in accordance with generally accepted government auditing standards between April and July 2004.

Results in Brief

DHS is working to address the daunting challenge of standardizing and integrating the various legacy IT environments and management approaches it inherited from its predecessor agencies while it is concurrently attempting to ensure that existing levels of IT support for critical homeland security missions are not only maintained but improved in the near term. To do so, the department has, among other things, made progress in establishing seven key information and technology management disciplines. However, fully establishing and institutionalizing these disciplines remains a work in progress that has yet to be accomplished. While accomplishing them will understandably take considerable time given the diversity of the inherited agencies and the size and complexity of the department, DHS's progress to date on each has been mixed, both across and within the disciplines. In the interim, new and existing system investments continue to be pursued without a fully defined and implemented departmentwide IT governance structure. The status of

DHS's efforts relating to the seven disciplines that would create such a structure are discussed below.

- *IT strategic planning*. DHS's draft IRM strategic plan dated March 2004 lists the priorities of the department's and component agencies' CIOs for 2004. The department is also in the process of developing what it terms as road maps for each of these priority areas that include descriptions of the current condition of the area, the need for change, the planned future state, initiatives, and barriers. However, neither the draft IRM strategic plan nor the draft road maps fully define the department's IT goals and performance measures, the time frames to complete significant activities, and the staff resources to execute these activities.

- *Enterprise architecture*. DHS released the initial version of its enterprise architecture in September 2003.[2] Our recent report on this initial version stated that it provides a partial basis upon which to build future versions.[3] However, this version was not systematically derived from a DHS or national corporate business strategy. Moreover, it is missing most of the content necessary to effectively guide and constrain IT investments. Without such content, DHS runs the risk that its investments will not be well integrated, will be duplicative, will be unnecessarily costly to maintain and interface, and will not effectively optimize mission performance. The department recognizes the architecture's limitations and plans to issue a new version in September 2004.

- *IT investment management*. DHS has established an IT investment management process that includes departmental oversight of major IT projects. However, this process is still maturing and has yet to be institutionalized in that most projects have not undergone the departmental oversight process and a mechanism to ensure that such reviews are accomplished in a timely manner has not been established.

[2]Generally speaking, an enterprise architecture connects an organization's strategic plan with program and system solution implementations by providing the fundamental information details needed to guide and constrain implementable investments in a consistent, coordinated, and integrated fashion.

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

- *Systems development and acquisition management.* DHS has numerous ongoing major systems initiatives, but our reviews of several of these projects have found that rigorous systems development and acquisition processes were not consistently employed. In particular, we identified significant problems in critical areas, such as process controls associated with acquiring software-intensive systems, managing and conducting testing, and measuring the performance of a system.

- *Information security management.* The DHS Office of Inspector General reported that the department has made progress in establishing a framework for the department's information systems security program by, for example, appointing a chief information security officer and developing and disseminating information system security policies and procedures. However, the inspector general concluded that more needs to be done to ensure the security of DHS's IT infrastructure and prevent disruptions to mission operations. For example, none of the DHS components had a fully functioning IT security program.

- *Information management.* As agencies increasingly move to an operational environment in which electronic—rather than paper—records provide comprehensive documentation of their activities and business processes, a variety of information collection, use, and dissemination issues face these agencies, including DHS. For example, privacy issues are a major concern in certain IT investments, such as the Computer-Assisted Passenger Prescreening System II (CAPPS II), in which privacy was designated by law as one of eight key issues that the Transportation Security Administration (TSA) must fully address before the system is deployed or implemented. DHS has taken steps to deal with privacy at both the department and system-specific level. For example, in April 2003, DHS appointed its first chief privacy officer to, for instance, guide DHS agencies in developing appropriate privacy policies.

- *IT human capital management.* DHS has begun strategic human capital planning at the headquarters level, but the agency has not yet systematically gathered necessary human capital data. Moreover, the DHS CIO has expressed concern over IT staffing and acknowledged that progress in the IT human capital area has been slow.

Taken collectively, the breadth and complexity of information and technology management issues facing DHS is a formidable challenge. Overcoming this challenge will require the kind of institutional approach to

information and technology management that the aforementioned seven disciplines are intended to provide. We have made numerous recommendations aimed at institutionalizing these disciplines to the department's chief information officer and other responsible DHS entities that, in some cases, the department has implemented or begun to implement. This report contains additional recommendations to the Secretary of Homeland Security related to the important undertaking of effective IT strategic planning, including the establishment of IT goals and performance measures that demonstrate how information and technology management contributes to, for example, the efficiency and effectiveness of agency operations.

In written comments on a draft of our report signed by the Director, Departmental GAO/OIG Liaison within the Office of the Chief Financial Officer, DHS generally concurred with our recommendations. In addition, DHS provided additional information on our recommendations and actions that it has taken, which we incorporated in the report, as appropriate.

Background

In March 2003 DHS assumed operational control of about 209,000 civilian and military positions from 22 agencies and offices. Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. As we have previously reported,[4] such a transformation poses significant management and leadership challenges, including those associated with coordinating and facilitating the sharing of information, both among its component agencies and with other entities, and integrating numerous mission support, administrative, and infrastructure IT systems. Critical to DHS's ability to meet this challenge is the establishment of an effective IT governance mechanism, including IT plans, processes, and people.

DHS Organizational Structure

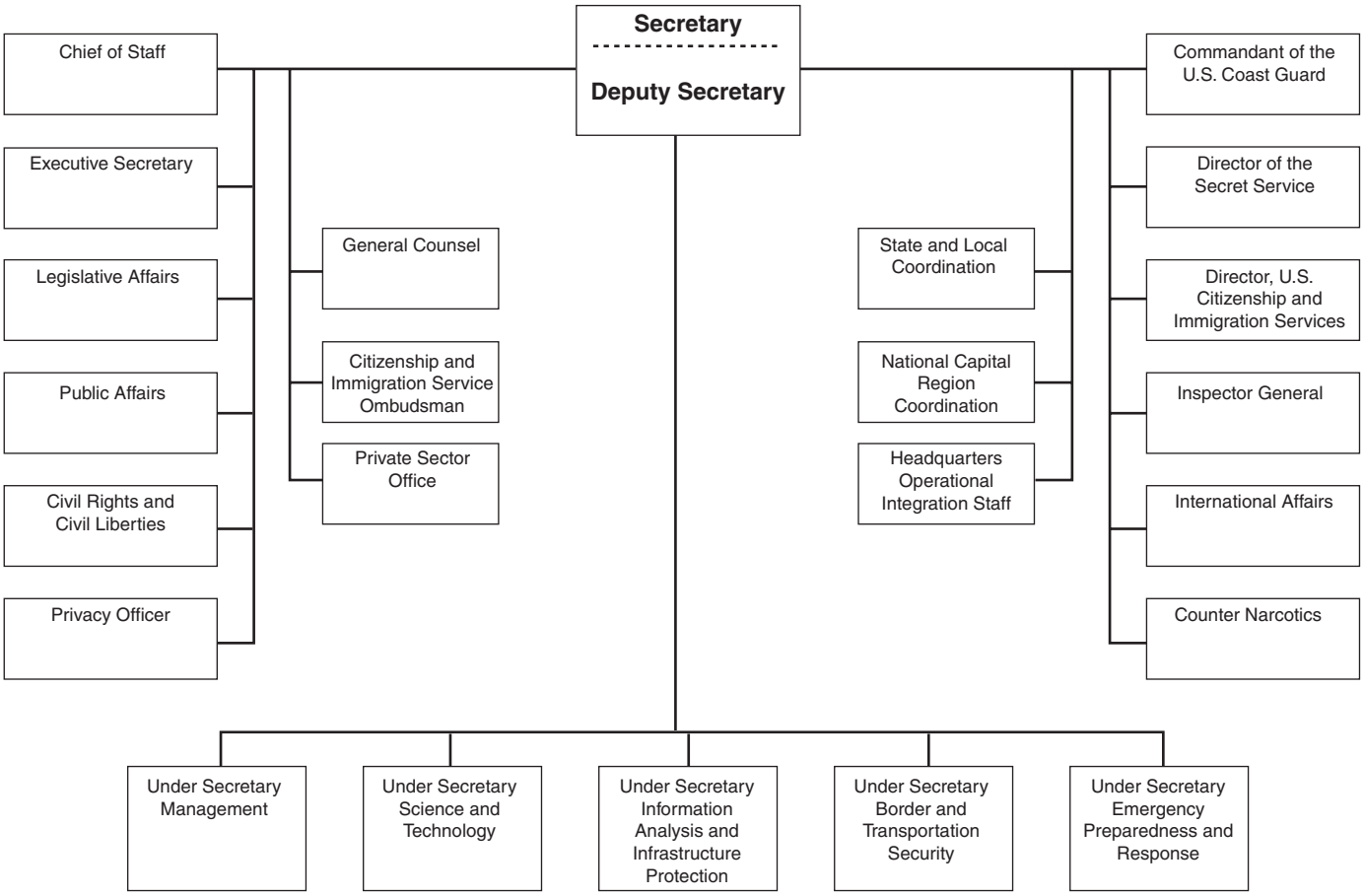
The Homeland Security Act of 2002 created DHS by merging agencies that specialize in one or more interrelated and interdependent aspects of homeland security, such as intelligence analysis, law enforcement, border security, transportation security, biological research, critical infrastructure

[4]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).

protection, and disaster recovery. DHS is in the early stages of transforming and integrating this disparate group of agencies with multiple missions, values, and cultures into a strong and effective cabinet department. The effective interaction, integration, and synergy of these agencies are critical to homeland security mission performance.

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. To accomplish this, the Homeland Security Act established five under secretaries with responsibilities over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response (see fig. 1). In addition to these directorates, the U.S. Secret Service and the U.S. Coast Guard continue as distinct entities within DHS. Each DHS directorate is responsible for its specific homeland security mission area and for coordinating related efforts with its sibling components, as well as other external entities.

Figure 1: Simplified Diagram of DHS Organizational Structure



Source: DHS.

Within the Management directorate is the Office of the CIO, which is expected to enhance mission success by leveraging best available information technologies and technology-management practices, provide shared services and coordinate acquisition strategies to minimize cost and improve consistency, support executive leadership in performance-based management by maintaining an enterprise architecture that is fully integrated with other management processes, and advocate and enable business transformation in support of enhanced homeland security. Other DHS entities also are responsible, or share responsibility, for critical information and technology management activities. For example, within DHS's major organizational offices (e.g., the directorates) are CIOs and IT organizations. Control over the department's IT budget is vested primarily with the CIO organizations within each of its component organizations, and the component CIO organizations are accountable to the heads of DHS's respective organizational components. Moreover, we have previously reported on the responsibilities held by various DHS directorates to ensure successful information sharing within the department and between federal agencies, state and local governments, and the private sector.[5]

The DHS CIO established a CIO Council, chaired by the CIO and composed of component-level CIOs, that serves as a focal point for coordinating challenges that cross agency boundaries. According to its charter, the specific functions of the DHS CIO Council include

- establishing a strategic plan and setting priorities for departmentwide IT;
- defining and continuously improving DHS IT governance structures and processes;
- advancing DHS IT priorities through well-defined road maps that detail actions and deliverables;
- identifying opportunities for sharing resources, coordinating multibureau projects and programs, and consolidating activities; and
- developing and executing formal communication programs for internal and external constituencies.

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

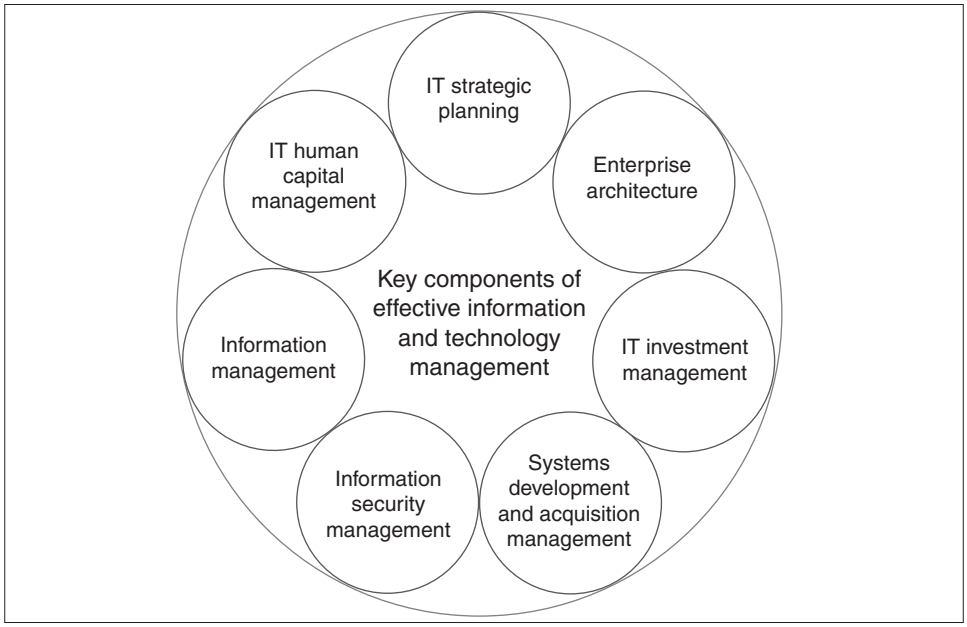
Key Components of an Effective Information and Technology Management Structure

As we have previously reported, information and technology management is a key element of management reform efforts that can help dramatically reshape government to improve performance and reduce costs.[6] Accordingly, it is critical that agencies manage their information resources effectively, taking into account the need to address planning, processes, and people. Key components of an effective information and technology management structure include (1) IT strategic planning, (2) enterprise architecture, (3) IT investment management, (4) systems development and acquisition management, (5) information security management, (6) information management, and (7) IT human capital management (see fig. 2).[7]

[6]GAO, *Major Management Challenges and Program Risks: A Governmentwide Perspective*, GAO-03-95 (Washington, D.C.: January 2003).

[7]As we recently reported, the Congress has made agency CIOs statutorily responsible for some of these key elements, such as IT investment management, information security management, and IT human capital management. See GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

Figure 2: Key Elements of an Effective Information and Technology Management Structure



Source: GAO.

Morever, effective implementation of information and technology management recognizes the interdependencies among these processes. Illustrations of some of these relationships are as follows:

- IT strategic planning defines what an agency seeks to accomplish and identifies the strategies that it will use to achieve desired results. The IT strategic plan, which is the outcome of this effort, is executed using the processes established through the other components of the information and technology structure, such as IT investment management.

- An organization's IT human capital approach must be aligned to support the mission, vision for the future, core values, goals and objectives, and strategies, which may be found in the IT strategic plan and the enterprise architecture. IT human capital management, in turn, ensures that the right people are in place with the right skills to perform critical system acquisition functions.

- The enterprise architecture is an integral component of the IT investment management process because an organization should

approve only those investments that move the organization toward the target architecture.

- A critical aspect of systems acquisition and development management is ensuring that robust information security is built into the projects early and is periodically revisited.

- Privacy—a component of information management—should be a consideration when acquiring and developing systems. For example, the E-Government Act of 2002 requires agencies to conduct privacy impact assessments before developing or acquiring IT systems that collect, maintain, or disseminate information that is personally identifiable to an individual. Such assessments would, in part, include what information is being collected, why it is being collected, and its intended use. In addition, ensuring that such personally identifiable data is secured against risks such as loss or unauthorized access, destruction, use, modification, or disclosure is an internationally recognized privacy principle.

DHS has recognized the importance of information and technology management to achieving its mission. In February of this year, it issued its first strategic plan, which outlines seven strategic goals. One of these goals is organizational excellence, which includes information and technology management objectives related to privacy and security and electronic government modernization and interoperability initiatives. In addition, at its various components, DHS has numerous ongoing major systems development and acquisition initiatives related to meeting mission needs, such as the following:

- *Border and Transportation Security Directorate*. The Automated Commercial Environment (ACE) project is to be a new trade processing system.

- *Border and Transportation Security Directorate*. CAPPS II is to identify airline passengers who pose a security risk before they reach the passenger screening checkpoint.

- *Border and Transportation Security Directorate*. The Student Exchange Visitor Information System (SEVIS) is expected to manage information about nonimmigrant foreign students and exchange visitors from schools and exchange programs.

- *Border and Transportation Security Directorate*. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is a governmentwide program intended to improve the nation's capacity for collecting information on foreign nationals who travel to the United States, as well as control the pre-entry, entry, status, and exit of these travelers.

- *Coast Guard*. Rescue 21 is to replace the Coast Guard's 30-year-old search and rescue communication system.

- *Science and Technology Directorate*. Project SAFECOM has the overall objective of achieving national wireless communications interoperability among first responders and public safety systems at all levels of government.

DHS's Progress in Dealing with Formidable Information and Technology Management Challenge Is Mixed

In the 18 months that it has been in operation, DHS has taken steps to institute key elements of an effective information and technology management structure. However, DHS's progress has been mixed in that some elements are further advanced than others and there is still considerable work remaining to institutionalize each of the areas across the department. An example of the former is that DHS established several key practices related to building an effective IT investment management process, whereas fundamental activities in the IT human capital area have not been started. IT strategic planning can serve as an example of the considerable amount of work remaining within individual elements of the information and technology management structure. Specifically, although DHS issued a draft IRM strategic plan this past March, it and other strategic planning documents do not contain sufficient information regarding the department's IT goals, how it will achieve them, and when it expects that significant activities will be completed.

DHS's mixed progress is not unexpected given the diversity of the inherited agencies and the size and complexity of the department and the daunting hurdles that it faces in integrating the systems and IT management approaches of its many organizational components. Nevertheless, new and existing IT investments continue to be pursued without a fully defined and implemented departmentwide governance structure, which increases the risk that they will not completely or optimally support the department's mission and objectives. To address the risks associated with DHS's departmental structures and specific IT investments, we have made recommendations to the DHS CIO and other responsible entities—such as

the Coast Guard and TSA—to help the department successfully overcome its information and technology management challenge. In some cases, the department has implemented or begun to implement these recommendations.

IT Strategic Planning

Strategic planning defines what an organization seeks to accomplish and identifies the strategies it will use to achieve desired results. In addition, the Paperwork Reduction Act requires that agencies indicate in strategic IRM plans how they are applying information resources to improve the productivity, efficiency, and effectiveness of government programs.[8] Further, Office of Management and Budget (OMB) Circular A-130 states that strategic IRM plans should support agency strategic plans and provide a description of how IRM helps accomplish agency missions. This plan serves as a vision or road map for implementing effective management controls and marshalling resources in a manner that will facilitate leveraging of IT to support mission goals and outcomes. It should be tied to and support the agency strategic plan and provide for establishing and implementing IT management processes.

DHS's draft IRM strategic plan dated March 2004, provides a high-level description of how IT supports the goals of the agency's strategic plan. According to the draft plan, although the department's component agencies have advanced their separate uses of information technology and services, serious gaps exist between the current and target environment necessary to support effective integration of information and collaboration of actions. The plan goes on to discuss steps taken in the investment management, enterprise architecture, and security disciplines.

The draft IRM plan also cites eight DHS CIO Council priorities for 2004; namely, (1) information sharing, (2) mission rationalization, (3) IT security, (4) one IT infrastructure, (5) enterprise architecture, (6) portfolio management, (7) governance, and (8) IT human capital. DHS is in the process of developing road maps for each of the CIO Council's priorities. These road maps are currently in draft and generally include a description of the current condition of the area, the need for a change, the planned future state, initiatives, and barriers.

[8]44 U.S.C. 3506(a).

Currently, neither the draft IRM strategic plan nor the draft priority area road maps contain sufficient information regarding the department's IT goals and performance measures, when the department expects that significant activities will be completed, and the staff resources necessary to implement these activities. For example:

- Neither the draft IRM strategic plan nor the draft road maps include fully defined goals and performance measures. Leading organizations define specific goals, objectives, and measures, use a diversity of measurement types, and describe how IT outputs and outcomes affect organizational customer and agency program delivery requirements.[9] In addition, the Paperwork Reduction Act and the Clinger-Cohen Act of 1996 require agencies to establish goals and performance measures on how information and technology management contributes to program productivity, the efficiency and effectiveness of agency operations, and service to the public.[10]

- The draft IRM plan does not include milestones for when major information and technology management activities will be initiated or completed. In addition, the milestones in the draft road maps are generally vague (e.g., using terms like short term and long term without defining them or including specific months with no year). Without milestone information, meaningful measurement of progress is not possible. This is particularly important since DHS did not always meet the target dates laid out by the CIO in February 2003. For example, the CIO planned to introduce a balanced scorecard[11] for the DHS IT community in the department's first year. Although the draft IRM strategic plan states that the DHS CIO Council has endorsed the use of a balanced scorecard approach, as of mid-July, this scorecard had not been developed.

- The plan does not address whether, or to what extent, DHS has staff with the relevant skills to obtain its target environment and, if it does,

[9]GAO, *Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments*, GAO/AIMD-98-89 (Washington, D.C.: March 1998).

[10]44 U.S.C. 3506(h); 40 U.S.C. 11313.

[11]A balanced scorecard is a tool to measure performance at various levels of an organization and to provide employees with data to help them achieve individual and organizational results.

whether they are allocated appropriately. This is particularly important since the DHS CIO Council has targeted IT human capital as a priority area and, according to the draft road map document associated with this priority, DHS is facing such issues as an aging IT workforce and too little investment in continuous learning.

The DHS CIO noted that the draft IRM strategic plan, the department's initial attempt at IT strategic planning, was primarily intended to meet OMB's requirements that a plan be developed. He further stated that through the development of the road maps, DHS is defining the operational details for its IT priority areas, which, in turn, will be used to update and improve the next version of the IRM plan. In responding to a draft of this report, DHS stated that the CIO intends to issue an IT strategic plan before the end of the calendar year and that, over the next few months, each priority area will develop goals, performance measures, and time lines for implementation.

A key emphasis of version 1.0 of the DHS draft IRM plan is its recognition of the importance of the department's integration efforts and its description of its plan to implement a single IT infrastructure. In particular, to maximize its mission performance, DHS faces the enormous task of integrating and consolidating a multitude of systems. This includes exploiting opportunities to eliminate and consolidate systems in order to improve mission support and reduce system costs. We recently reported that DHS is in the process of developing its systems integration strategy and that, in the interim, the department has taken steps to address ongoing and planned component IT investments integration and alignment with its evolving strategic IT management framework.[12] However, we concluded that while these steps have merit, they do not provide adequate assurance of strategic alignment across the department. For example, one step simply continued the various approaches that produced the diverse systems that the department inherited, while another relied too heavily on oral communication about complex IT strategic issues that are not yet fully defined. Thus, DHS has an increased risk that its component agencies' ongoing investments, collectively costing billions of dollars in fiscal year 2004, will need to be reworked at some future point to be effectively integrated and to maximize departmentwide value.

[12]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).

Moreover, we reported that the DHS CIO does not have authority and control over departmentwide IT spending, even though such control is important for effective systems integration. According to our research on leading private and public sector organizations and experience at federal agencies, leading organizations adopt and use an enterprisewide approach under the leadership of a CIO or comparable senior executive who has the responsibility and authority, including budgetary and spending control, for IT across the entity.[13] To help DHS better manage the risks that it faces, we made several recommendations, including that the Secretary examine the sufficiency of IT 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. In commenting on a draft of this report, DHS did not address whether it would implement these recommendations.

Enterprise Architecture

Effective use of enterprise architectures is a trademark of successful public and private organizations. For a decade, we have promoted the use of architectures to guide and constrain systems modernization, recognizing them as a crucial means to a challenging goal: establishing agency operational structures that are optimally defined in both business and technological environments. The Congress, OMB, and the federal CIO Council have also recognized the importance of an architecture-centric approach to modernization. The Clinger-Cohen Act of 1996 mandates that an agency's CIO develop, maintain, and facilitate the implementation of IT architectures. This should provide a means of managing the integration of business processes and supporting systems. Further, the E-Government Act of 2002[14] requires OMB to oversee the development of enterprise architectures within and across agencies.

Generally speaking, an enterprise architecture connects an organization's strategic plan with program and system solution implementations by providing the fundamental information details needed to guide and constrain implementable investments in a consistent, coordinated, and integrated fashion. An enterprise architecture provides a clear and

[13]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).

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

comprehensive picture of an entity, whether it is an organization (e.g., federal department) or a functional or mission area that cuts across more than one organization (e.g., homeland security). This picture consists of snapshots of both the enterprise's current or "As Is" operational and technological environment and its target or "To Be" environment, as well as a capital investment road map for transitioning from the current to the target environment. These snapshots further consist of "views," which are basically one or more architecture products that provide conceptual or logical representations of the enterprise.

For the last 2 years, we have promoted the development and use of a homeland security enterprise architecture. For example, in June 2002 we testified[15] on the need to define the homeland security mission and the information, technologies, and approaches necessary to perform this mission in a way that is divorced from organizational parochialism and cultural differences. We also stressed that a particularly critical function of a homeland security architecture would be to establish processes and information/data protocols and standards that could facilitate information collection and permit sharing.

Recognizing the pivotal role that an architecture will play in successfully merging the diverse operating and systems environments that the department inherited, DHS issued an initial version in September 2003. Our recent report on this initial enterprise architecture found that it provides a partial basis upon which to build future versions.[16] However, the September 2003 version of the enterprise architecture is missing most of the content necessary to be considered a well-defined architecture. Moreover, the content in this version was not systematically derived from a DHS or national corporate business strategy, but rather was more the result of an amalgamation of the existing architectures that several of DHS's predecessor agencies already had, along with their respective portfolios of system investment projects. Such a development approach is not consistent with recognized architecture development best practices.

DHS officials agreed with our content assessment of their initial architecture, stating that it is largely a reflection of what could be done

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

[16]GAO-04-777.

without a departmental strategic plan to drive architectural content and with limited resources and time. They also stated that the primary purposes in developing this version were to meet an OMB deadline for submitting the department's fiscal year 2004 IT budget request and for the department to develop a more mature understanding of enterprise architecture and its ability to execute an approach and methodology for developing and using the next version of the architecture.

Nevertheless, we concluded that DHS does not yet have the architectural content that it needs to effectively guide and constrain its business transformation efforts and the hundreds of millions of dollars it is investing in supporting systems. For example, the architecture does not (1) include a description of the information flows and relationships among organizational units, business operations, and system elements; (2) provide a description of the business and operational rules for data standardization to ensure data consistency, integrity, and accuracy; or (3) include an analysis of the gaps between the baseline and target architecture for business processes, information/data, and services/application systems to define missing and needed capabilities.

Moreover, the architecture does not adequately recognize the interdependencies with other critical IT management processes since it does not include (1) a description of the policies, procedures, processes, and tools for selecting, controlling, and evaluating application systems to enable effective IT investment management and (2) a description of the system development lifecycle process for application development or acquisition and the integration of the process with the architecture. In addition, although the architecture recognizes the need for a governance structure and contains a high-level discussion of same, it does not include an architecture governance and control structure and the integrated procedures, processes, and criteria (e.g., investment management and security) to be followed. Without such content, DHS runs the risk that its investments will not be well integrated, will be duplicative, will be unnecessarily costly to maintain and interface, and will not effectively optimize mission performance.

To assist DHS in developing a well-defined enterprise architecture, our August report contained numerous recommendations directed to the architecture executive steering committee—composed of senior executives from technical and business organizations across the department—in collaboration with the CIO, that are aimed at ensuring that

the needed content is added and that the approach followed adheres to best practices.

Given DHS's intended purpose of its enterprise architecture, which is to use it as the basis for departmentwide (and national) operational transformation and to support systems modernization and evolution, it is important that individual IT investments be aligned with the architecture. Moreover, according to the CIO, DHS is developing a process to align its systems modernization activities with its enterprise architecture. However, earlier this year, we reported that this alignment had not been determined for two of the department's major investments—ACE and US-VISIT—but the CIO and program officials stated that they planned to address this issue.[17]

IT Investment Management

Investments in IT can have a dramatic impact on an organization's performance. If managed effectively, these investments can vastly improve government performance and accountability. If not, they can result in wasteful spending and lost opportunities for improving delivery of services to the public. An IT investment management process provides a systematic method for agencies to minimize risks while maximizing return on investment. A central tenet of the federal approach to IT investment management has been 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.

[17]GAO, *Information Technology: Early Releases of Customs Trade System Operating, but Pattern of Cost and Schedule Problems Needs to Be Addressed*, GAO-04-719 (Washington, D.C.: May 14, 2004) and *Homeland Security: First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed*, GAO-04-586 (Washington, D.C.: May 11, 2004).

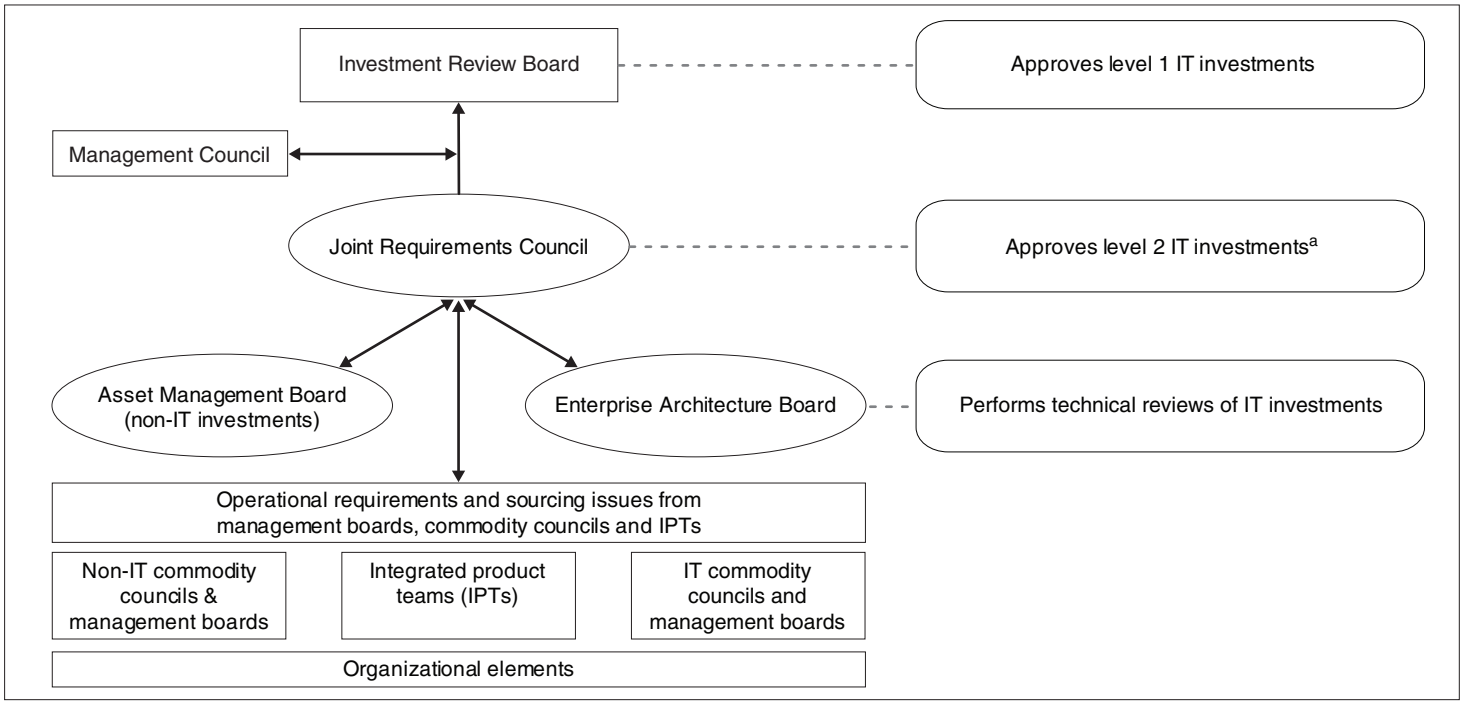
DHS has developed and begun implementing a departmental IT investment management process. In May 2003 DHS issued an investment review management directive[18] and IT capital planning and investment control guide, which provide the department's component organizations with requirements and guidance on documentation and review of IT investments. In February 2004, we reported that DHS's investment management process was evolving.[19] Since that time, DHS has changed its process to reflect lessons learned during the department's first year of operation and continuous improvement of the process. Moreover, DHS issued a new interim IT capital planning and investment control guide in May 2004 and is in the process of revising the investment review management directive to reflect the changes that have been made. Among the changes is a shifting of responsibilities of some of its investment management boards and increases to the thresholds that determine which board approves an investment.

Figure 3 illustrates the governance boards DHS uses to execute its investment review process. Under this process, DHS has four levels of investments, the top three of which are subject to review by department-level boards—the Investment Review Board, Joint Requirements Council, and Enterprise Architecture Board. (App. I provides more specific information on the boards and their responsibilities.)

[18]This management directive covers both IT and non-IT investments.

[19]GAO, *Information Technology: OMB and Department of Homeland Security Investment Reviews*, GAO-04-323 (Washington, D.C.: Feb. 10, 2004).

Figure 3: DHS Investment Governance Boards

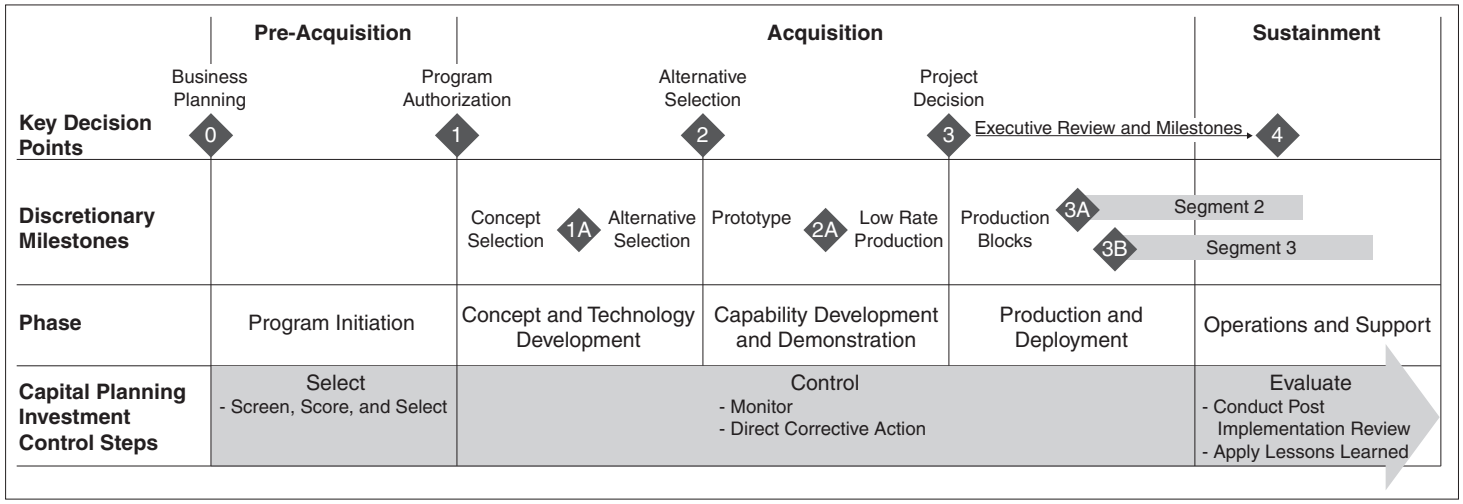


Source: DHS.

[a]According to the DHS coordinator of this process, level 3 IT investments are approved by the component agency and are subject to review by the CIO, Chief Financial Officer, and Chief Procurement Officer, also known as the Management Review Council. If these officials have concerns about the investment or find that there are cross-programmatic issues to be addressed, they can refer the investment to the Joint Requirements Council for review.

In addition, DHS has established a five-phase review process that calls for these investments to be reviewed at key decision points, such as program authorization (see fig. 4).

Figure 4: DHS Investment Review Process



Source: DHS.

With the establishment of the governance boards and the investment review process, DHS has established several key practices associated with building the investment foundation as described by our IT investment management framework.[20] In addition, as part of the selection phase of its capital planning and investment control process, DHS reviewed component agency IT investments for its fiscal year 2005 budget submission. Specifically, according to DHS IT officials, (1) the CIO approved the department's IT portfolio and (2) all of the major IT systems submitted to OMB for the fiscal year 2005 budget were assessed and scored by an investment review team.[21]

[20]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004).

[21]The investment review team was made up of representatives from the offices of the CIO, the chief financial officer, and the chief procurement officer, as well as several component agencies.

In addition, earlier this year, as we reported, with the department's establishment of the department's top investment management board, the ACE and CAPPS II investments met legislative conditions contained in the Department of Homeland Security Appropriations Act, 2004 (P.L. 108-90).[22] For example, in February 2004 we reported that that creation of the Investment Review Board satisfied a CAPPS II legislative requirement associated with the establishment of an oversight board, with the caveat that the board oversee the program on a regular and thorough basis. In addition, in May 2004 we reported that DHS satisfied a prior recommendation of ours to establish and charter an executive body to guide and direct the US-VISIT program by establishing a three-entity governance structure, which includes the department's Investment Review Board.[23]

Although DHS has made noticeable progress, it still has much work remaining to fully implement its IT investment management process, particularly as it relates to carrying out effective departmental control over IT investments. For example:

- Many of DHS's IT investments have not undergone control reviews. As of early July, one or more of DHS's investment management boards had reviewed less than a quarter of the major IT investments subject to departmental review (level 1, 2, and 3 investments). According to the coordinator of this process, the investments that have undergone control reviews were considered DHS's highest priority IT investments based on criteria such as cost, visibility, or that a key decision point was forthcoming. In addition, DHS stated that its ability to complete control reviews in a timely manner is affected by the amount of resources, people, time, and funding allocated to the department. Nevertheless, our reviews of several DHS level 1 investments indicate the importance of such reviews, since we have found cost, schedule, and performance problems as well as significant management activities that have not been completed.

[22]GAO, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: Feb. 12, 2004) and GAO-04-719.

[23]GAO-04-586.

- DHS has not established a process to ensure that control reviews of IT investments are performed in a timely manner. Our February 2004 report recommended that the DHS CIO develop a control review schedule for IT investments, subject to departmental oversight.[24] DHS concurred with this recommendation, but has not yet implemented it. However, for the fiscal year 2006 budget cycle, which is being formulated now, DHS entities were asked to provide the dates of prior and future key decision points for each major IT investment. According to Office of the CIO capital planning and investment control officials, this is their first step toward building a control review schedule.

- Officials from DHS's offices of the CIO and chief financial officer characterized the department's investment management process as still maturing. For example, Office of the CIO capital planning and investment control officials stated that the department will be concentrating on developing and building a disciplined and structured control process in fiscal year 2005. Officials from the offices of the CIO and chief financial officer also described various initiatives that are being undertaken to improve this process. For example, portfolio management is a CIO Council priority and, according to the draft road map for this priority, the planned future environment will have IT investments aligned and optimized against mission requirements at the DHS level. DHS has procured an automated portfolio management system to help in this endeavor. According to Office of the CIO capital planning and investment control officials, DHS has inserted its fiscal year 2005 business cases for major investments (also known as budget exhibit 300s) into this system and plans to add the fiscal year 2006 business cases later this year. In addition, according to these officials, the department's Investment Review Team plans to use this system to perform portfolio analysis to provide additional insight to DHS investment management boards as they make their investment selections for fiscal year 2006.

Systems Development and Acquisition Management

Our work and other best-practice research have shown that applying rigorous management practices to the development and acquisition of IT systems and the acquisition of IT services improves the likelihood of delivering expected capabilities on time and within budget. In other words,

[24] GAO-04-323.

the quality of IT systems and services is largely governed by the quality of the management processes involved in developing and acquiring them.

DHS has numerous ongoing major systems development and acquisition initiatives that are critical to meeting its mission needs. Our reviews of several major DHS systems development and acquisition efforts have found that these rigorous processes are not always employed. We have made numerous recommendations that address a variety of system development and acquisition issues. DHS has generally agreed with these recommendations and, in some cases, has implemented, or begun to implement, them. For example:

- *Process controls for acquiring software-intensive systems.* Disciplined processes for acquiring software are essential to software-intensive system acquisitions. The Software Engineering Institute at Carnegie Mellon University[25] has defined the tenets of effective software acquisition, which identify, among other things, a number of key process areas that are necessary to effectively manage software-intensive system acquisitions. In the past, we have reported that such key processes had not been fully implemented for ACE and US-VISIT. Consequently, we made recommendations for both of these programs related to instituting acquisition process controls called for in the Software Engineering Institute's SA-CMM® model.[26] As of May of this year, the acquisition control recommendation had been implemented by the ACE program in that the Software Engineering Institute had assigned the program a level 2 rating, meaning that it had established basic acquisition management processes.[27] Also in May of this year we reported that US-VISIT was planning to implement our recommendation on instituting acquisition process controls.[28]

[25]Carnegie Mellon University's Software Engineering Institute is recognized for its expertise in developing models and methods that define and determine organizations' software-intensive systems process maturity.

[26]GAO, *Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project*, GAO-02-545 (Washington, D.C.: May 13, 2002) and *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to be Addressed*, GAO-03-1083 (Washington, D.C.: Sept. 19, 2003).

[27]GAO-04-719.

[28]GAO-04-586.

- *Managing and conducting testing.* Complete and thorough testing is essential to providing reasonable assurance that new or modified systems process information correctly and will meet an organization's business needs. According to leading IT organizations, to be effective, software testing practices should be planned and conducted in a structured and disciplined fashion.[29] We have expressed concerns about testing and issued related recommendations for three DHS IT investments—Rescue 21, CAPPS II, and US-VISIT. For example, in September 2003 we reported that the Coast Guard planned to compress and overlap the testing schedules for Rescue 21, which increased its risk that, for instance, all requirements would not be tested during formal qualification testing, system integration testing, and operational testing and evaluation.[30] To mitigate Rescue 21 risks, we made recommendations to the Coast Guard related to establishing a new testing schedule and ensuring that milestones are established for completing test plans and that these plans address all requirements of the system. The Coast Guard agreed with these recommendations, which the agency has begun to implement. In the cases of CAPPS II and US-VISIT, we made recommendations to TSA and the Border and Transportation Security Directorate, respectively, covering system and database testing and developing and approving complete test plans before testing begins, respectively.[31] DHS generally concurred with these recommendations.

[29]GAO, *Year 2000 Computing Crisis: A Testing Guide*, GAO/AIMD-10.1.21 (Washington, D.C.: November 1998).

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

[31]GAO-04-385 and GAO-04-586.

- *Measuring the performance of a system.* By using comprehensive performance information, more informed decisions can be made about IT investments. An effective performance measurement system produces information that (1) provides an early warning indicator of problems and the effectiveness of corrective actions, (2) provides input to resource allocation and planning, and (3) provides periodic feedback about the quality, quantity, cost, and timeliness of products and services. We have reported on a variety of performance measure concerns associated with five DHS IT investments and have made relevant recommendations. For example, in February 2004, we reported that TSA had established preliminary goals and measures for CAPPS II but that they could be strengthened.[32] We also noted that TSA had not fully established policies and procedures to monitor and evaluate the use and operation of the system. Similarly, our review of SEVIS, which is operational, found that several key system performance requirements were not being formally measured.[33] This is problematic because without formally monitoring and documenting key system performance requirements, DHS cannot adequately ensure that potential system problems are identified and addressed early, before they have a chance to become larger and affect the DHS mission objectives supported by SEVIS.

In addition to our recommendations related to specific DHS IT investments, we have also issued guidance to assist agencies in improving their systems development and acquisitions.[34]

Information Security Management

Since 1997 we have designated information security as a governmentwide high-risk issue because of continuing evidence indicating significant, pervasive weaknesses in the controls over computerized federal operations.[35] Moreover, related risks continue to escalate, in part due to the

[32]GAO-04-385.

[33]GAO, *Homeland Security: Performance of Information System to Monitor Foreign Students and Exchange Visitors Has Improved, but Issues Remain*, GAO-04-690 (Washington, D.C.: June 18, 2004).

[34]See, for example, GAO/AIMD-98-89 and GAO/AIMD-10.1.21.

[35]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) for our latest high-risk series report on this issue.

government's increasing reliance on the Internet and on commercially available information technology. Government officials are increasingly concerned about attacks launched by individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. In addition, the disgruntled organization insider is a significant threat, since such individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions.

Based on its annual evaluation required by the Federal Information Security Management Act of 2002[36], in September 2003 the DHS Office of Inspector General reported that DHS had made progress in establishing a framework for an IT systems security program.[37] For example, DHS has (1) appointed a chief information security officer, (2) developed and disseminated information system security policies and procedures, (3) implemented an incident response and reporting process, (4) initiated a security awareness training program, and (5) established a critical infrastructure protection working group.

However, the inspector general report concluded that still more needs to be done to ensure the security of DHS's IT infrastructure and prevent disruptions to mission operations. For example, DHS did not have a process to ensure that all plans of action and milestones for identified weaknesses were developed, implemented, and managed. In responding to a draft of this report, DHS stated that it has instituted a tool to monitor each organizational element's progress in developing and achieving the milestones identified in the plans of action and milestones.

In addition, the Office of Inspector General stated that none of the DHS components had a fully functioning IT security program and a number of key security areas needed attention. For example, less than half of DHS's systems had a security plan and been assessed for risk. Among the Office of Inspector General's recommendations were that the CIO (1) develop and implement a process to identify information security-related material weaknesses in mission-critical programs and systems, (2) implement an oversight and reporting function to track the progress of remediation of

[36]44 U.S.C. 3545.

[37]Department of Homeland Security, Office of Inspector General, *DHS Information Technology: Information Security Program Evaluation, FY2003*, OIG-IT-03-02 (September 2003).

material weaknesses, and (3) require DHS information officers to assign information systems security officers to oversee the security controls of each major application and general support system.

More recently, the DHS Office of Inspector General reported that DHS cannot ensure that the sensitive information processed by its wireless systems is effectively protected from unauthorized access and potential misuse.[38] In particular, the Inspector General reported that DHS had not (1) provided sufficient guidance on wireless implementation to its components, (2) established adequate security controls to protect its wireless networks against commonly known security vulnerabilities, and (3) certified or accredited its wireless networks.[39] The Inspector General made several recommendations to address the deficiencies cited in the report, which the DHS CIO agreed to and has taken steps to implement.

In addition, we have long held that it is important that security be addressed in the early planning stages of the development of IT systems,[40] and have reported on security planning in the US-VISIT and CAPPS II programs. For example, in June 2003 we recommended that the US-VISIT program manager develop a system security plan[41] and in May 2004 we reported that this recommendation had been partially implemented.[42] Specifically, DHS provided a draft security plan, but this plan did not include (1) specific controls for meeting the security requirements, (2) a risk assessment methodology, or (3) the roles and responsibilities of individuals with system access.

[38]Department of Homeland Security, Office of Inspector General, *Inadequate Security Controls Increase Risks to DHS Wireless Networks*, OIG-04-27 (June 2004).

[39]*Accreditation* is the authorization of an IT system to process, store, or transmit information, granted by a management official that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. *Certification* is the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

[40]GAO, *Executive Guide: Information Security Management*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[41]GAO, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning*, GAO-03-563 (Washington, D.C.: June 9, 2003).

[42]GAO-04-586.

DHS reported four departmentwide information security-related material weaknesses in its fiscal year 2003 Performance and Accountability Report.[43] For example, DHS reported that it had (1) limited tracking, evaluation, and reporting tools necessary to provide oversight over its information security efforts and (2) insufficient resources, processes, policies, and guidelines in place to ensure the identification, protection, and continuity of services to reduce the department's vulnerabilities and risks and to sustain mission-critical functions in the event of a man-made or natural disaster. According to the DHS report, the department plans to take corrective actions related to these material weaknesses by September 30, 2004.

The DHS CIO Council has also pronounced information security a priority area. The draft road map associated with this area includes various short- , mid- , and long-term initiatives. Moreover, to lay a foundation for departmental improvements in information security management, DHS has developed an information security program strategic plan, which identifies major program areas, goals, and objectives. According to this April 2004 plan, these major security program areas allow DHS to implement and maintain information security as part of its capital investment control process, systems development life cycle, and the enterprise architecture, and are essential to providing security services that protect the confidentiality, integrity, and availability of information and to provide accountability for activities on DHS networks and computing platforms.

Information Management

As agencies increasingly move to an operational environment in which electronic—rather than paper—records provide comprehensive documentation of their activities and business processes, a variety of information collection, use, and dissemination issues have emerged. Such issues are particularly relevant to DHS because the Homeland Security Act of 2002 and federal policy assign responsibilities to the department for the coordination and sharing of information related to threats of domestic terrorism—within the department and with and among other federal agencies, state and local governments, the private sector, and other entities.

[43]Department of Homeland Security, *Performance and Accountability Report, Fiscal Year 2003* (Feb. 13, 2004).

Among the information management issues facing DHS are information sharing, privacy, and compliance with the information collection requirements. Namely:

Information sharing. As we have reported, information sharing is critical to successfully addressing increasing threats and fulfilling the missions of DHS.[44] For example, to accomplish its missions, the department must (1) access, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources, and (2) analyze such information to identify and assess the nature and scope of terrorist threats. Further, DHS must share information both internally and externally with agencies and law enforcement on such matters as goods and passengers inbound to the United States and individuals who are known or suspected terrorists and criminals. It also must share information among emergency responders in preparing for and responding to terrorist attacks and other emergencies.

We have made numerous recommendations over the last several years related to information-sharing functions that have been transferred to DHS, which are focused on sharing information on incidents, threats, and vulnerabilities and providing warnings related to critical infrastructures, both within the federal government and between the federal government and state and local governments and the private sector. In September 2003 we testified[45] that although progress has been made in addressing our recommendations, further efforts were needed, such as (1) improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector, and (2) developing a comprehensive and coordinated national plan to facilitate information sharing on critical infrastructures. More recently, in July 2004 we reported that DHS's ability to gather, analyze, and disseminate information could be improved by developing information sharing-related policies and procedures for its

[44]GAO-03-715T.

[45]GAO, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: Sept. 17, 2003).

components.[46] In commenting on a draft of this report, DHS provided planned actions in response to its recommendations.

The DHS Secretary has recognized the criticality of information sharing in the department's strategic plan. In addition, information sharing is one of the DHS CIO Council's priorities in 2004. In the draft road map associated with this priority area, DHS described a future state that includes seamless access and dissemination of information in real time or near real time, that information is shared with all constituents, at all levels of government, and with the private sector, and that there are agreed-upon data standardization rules. We have issued guidance on information-sharing practices of organizations that successfully share sensitive or time-critical information, which could aid DHS in its efforts.[47]

Privacy. With the emphasis on information sharing, privacy issues have emerged as a major, and contentious, concern. Since the terrorist attacks of September 11, 2001, data mining[48] has been seen increasingly as a useful tool to help detect terrorist threats by improving the collection and analysis of public and private-sector data. Our May 2004 governmentwide report[49] on data mining described 14 data mining efforts reported by DHS.[50] Mining government and private databases containing personal information creates a range of privacy concerns because agencies can quickly and efficiently obtain information on individuals or groups by exploiting large databases containing personal information aggregated from public and private records. Concerns have also been raised about the quality and accuracy of the mined data; the use of the data for other than the original purpose for

[46]GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004).

[47]GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[48]Data mining is the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.

[49]GAO, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, GAO-04-548 (Washington, D.C.: May 4, 2004).

[50]As part of our methodology for this report, we aggregated the data collected by each agency and sent them to the agency chief information officer, comparable official, or their designee, and asked that they review the characteristics for completeness and accuracy. DHS did not respond to our request to review the reported data.

which the data were collected without the consent of the individual; the protection of the data against unauthorized access, modification, or disclosure; and the right of individuals to know about the collection of personal information, how to access that information, and how to request a correction of inaccurate information. In April 2003, DHS appointed its first chief privacy officer. According to this officer, among other things, the DHS privacy office promotes best practices with respect to privacy, guides DHS agencies in developing appropriate privacy policies, and serves as a resource for questions related to privacy and information collection and disclosure.

Privacy concerns have also been a critical factor in the development and acquisition of US-VISIT and CAPPS II. With respect to CAPPS II, the 2004 DHS appropriations act designated privacy as one of eight key issues that TSA must address before CAPPS II is deployed or implemented. In our February 2004 report on whether TSA had fulfilled these legislative requirements, we stated that the agency's plans appear to address many of the requirements of the Privacy Act,[51] the primary legislation that regulates the government's use of personal information.[52] However, while TSA had taken initial steps, it had not finalized its plans for complying with the Privacy Act. We also looked at the TSA's plans in the larger context of eight Fair Information Practices, which are internationally recognized privacy principles that include practices such as data quality and security safeguards.[53] The TSA's plans reflect some actions to address each of these practices. However, to meet its evolving mission goals, the agency also appears to limit the application of some of these practices. This reflects TSA's efforts to balance privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency.

Compliance with the information collection requirements of the Paperwork Reduction Act. The Paperwork Reduction Act prohibits an agency from conducting or sponsoring the collection of information unless (1) the agency has submitted the proposed collection and other documents

[51]5 U.S.C. 552a.

[52]GAO-04-385.

[53]We refer to the eight Fair Information Practices proposed in 1980 by the Organization for Economic Cooperation and Development and that were endorsed by the U.S. Department of Commerce in 1981. These are collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, individual participation, and accountability.

to OMB, (2) OMB has approved the proposed collection, and (3) the agency displays an OMB control number on the collection. We testified in April 2004 that DHS had 18 reported violations of the Paperwork Reduction Act in fiscal year 2003, all related to OMB approvals that had expired and had not been reauthorized.[54]

IT Human Capital Management

Our work with leading organizations shows that they develop human capital strategies to assess their skill bases and recruit and retain staff who can effectively implement technology to meet business needs.[55] They assess their IT skills on an ongoing basis to determine what expertise is needed to meet current responsibilities and support future initiatives and evaluate the skills of their current employees, which are then compared against the organization's needed skills to determine gaps in the IT skills base. The challenges the federal government faces in maintaining a high-quality IT workforce are long-standing and widely recognized.

The success of the transformation and implementation of DHS is based largely on the degree to which human capital management issues are addressed. We have issued several reports examining how DHS plans to implement its new human capital system.[56] For example, in June 2004 we reported that DHS had begun strategic human capital planning efforts at the headquarters level since the release of the department's overall strategic plan and the publication of proposed regulations for its new human capital management system.[57] However, DHS had not yet systematically gathered relevant human capital data at the headquarters level, although efforts were under way to collect detailed human capital

[54]GAO, *Paperwork Reduction Act: Agencies' Paperwork Burden Estimates Due to Federal Actions Continue to Increase*, GAO-04-676T (Washington, D.C.: Apr. 20, 2004).

[55]GAO-01-376G.

[56]GAO, *Human Capital: DHS Personnel System Design Effort Provides for Collaboration and Employee Participation*, GAO-03-1099 (Washington, D.C.: Sept. 30, 2003); *Human Capital: Preliminary Observations on Proposed DHS Human Capital Regulations*, GAO-04-479T (Washington, D.C.: Feb. 25, 2004); *Posthearing Questions Related to Proposed Department of Homeland Security (DHS) Human Capital Regulations*, GAO-04-570R (Washington, D.C.: Mar. 22, 2004); and *Additional Posthearing Questions Related to Proposed Department of Homeland Security (DHS) Human Capital Regulations*, GAO-04-617R (Washington, D.C.: Apr. 30, 2004).

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

information and design a centralized information system so that such data could be gathered and reported departmentwide. These strategic human capital planning efforts can enable DHS to remain aware of and be prepared for current and future needs as an organization.

It is important that DHS address its IT human capital challenges expeditiously since, according to the DHS CIO, the biggest obstacle to the implementation of a departmentwide systems integration strategy has been insufficient staffing. More specifically, the CIO said that his office received substantially fewer staff than he requested when the department was originally established in 2003. To illustrate his statement, the CIO said that after studying other comparably sized federal department CIO organizations, he requested approximately 163 positions. However, he said that his office received about 65 positions. In addition, CIO officials told the Office of Inspector General that, given the relatively small staff resources provided, they have been "busy putting out fires" and, as a result, have been hindered in carrying out some critical IT management responsibilities, including instituting central guidance and standards in areas such as information security and network management.[58] Lastly, the DHS CIO also noted the lack of properly skilled IT staff within the component agencies. Challenges facing DHS in this area, he stated, include overcoming political and cultural barriers, leveraging cultural beliefs and diversity to achieve collaborative change, and recruiting and retaining skilled IT workers.

[58]Department of Homeland Security, Office of Inspector General, *Improvements Needed To DHS' Information Technology Management Structure*, OIG-04-30 (July 2004).

In addition, we have expressed concerns about human capital issues related to two of DHS's major IT investments, ACE and US-VISIT. In May 2002 we reported that the program office managing ACE did not have the people in place to perform critical system acquisition functions, which increased the risk that promised system capabilities would not be delivered on time or within budget.[59] Accordingly, we recommended that a human capital management strategy be immediately implemented for this office. Two years later we reported that U.S. Customs and Border Protection is in the process of implementing this recommendation.[60] In particular, the program office had developed and begun implementing a human capital management plan, but the office has continued to experience difficulty in filling key positions. The ACE program office has begun implementing a new staffing plan intended to address DHS's concern that the program office has insufficient government program management staff. We have reported on similar IT human capital problems associated with US-VISIT and recommended that it develop and implement a human capital strategy, which the department is in the process of doing.[61]

As mentioned, the DHS CIO Council established IT human capital as one of its eight priority areas. As with the other priority areas, a component agency sponsor has been named for human capital. However, unlike the other priority areas, as of mid-July 2004, an Office of the CIO official had not been assigned to work in this area. An Office of the CIO official explained that the person originally assigned this task is no longer with the department and that the office was determining who would take over this role. Moreover, in February 2003, the DHS CIO set July 2003 as a milestone for developing a current inventory of IT skills, resources, and positions, and September 2003 as the target date for developing an action plan. In mid-July 2004, the CIO stated that these milestones were not met and acknowledged that progress in IT human capital has been slow. He stated that he still plans to complete an inventory and action plan but could not provide an estimated completion date.

[59]GAO-02-545.

[60]GAO-04-719.

[61]GAO-03-1083 and GAO-04-586.

We have issued a large body of human capital work that could assist in this undertaking. For example, while agencies' approaches to workforce planning will vary, our guide on strategic workforce planning lays out five key principles that such a process should address irrespective of the context in which planning is done.[62] These are as follows:

- Involve top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.
- Determine the critical skills and competencies that will be needed to achieve current and future programmatic results.
- Develop strategies that are tailored to address gaps in number, deployment, and alignment of human capital approaches for enabling and sustaining the contributions of all critical skills and competencies.
- Build the capability needed to address administrative, educational, and other requirements important to support workforce strategies.
- Monitor and evaluate the agency's progress toward its human capital goals and the contribution that human capital results have made toward achieving programmatic goals.

Conclusions

DHS faces the formidable challenge of defining and implementing an effective information and technology management structure at the same time that it is developing and acquiring major IT systems that are critical to meeting its mission needs. Although DHS has made progress in addressing this challenge, it does not yet have a fully institutionalized structure in place, which puts its pursuit of new and enhanced IT investments at risk of not optimally supporting corporate mission needs and not meeting cost, schedule, capability, and benefit commitments. In particular, still lacking in the department's IT strategic planning process—which is critical because it defines what an agency seeks to accomplish and how that will be achieved—are goals, performance measures, and milestones for significant activities and whether DHS has appropriately skilled and deployed IT staff. The department's CIO and DHS CIO Council—which is responsible for

[62]GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

establishing a strategic plan and setting priorities for departmentwide IT—are organizationally placed to improve this planning process and to consider the needs of DHS as a whole. With regard to the other six elements of an effective information and technology management structure, DHS can be guided by the many recommendations that we and the Office of Inspector General have already made to the CIO and other responsible entities, along with our best practices guidance, as it uses technology to help better secure the homeland.

Recommendations

To strengthen DHS's IT strategic planning process, we recommend that the Secretary of Homeland Security direct the CIO, in conjunction with the DHS CIO Council, to take the following three actions:

- Establish IT goals and performance measures that, at a minimum, address how information and technology management contributes to program productivity, the efficiency and effectiveness of agency operations, and service to the public.
- Establish milestones for the initiation and completion of major information and technology management activities.
- Analyze whether DHS has appropriately deployed IT staff with the relevant skills to obtain its target IT structure and, if it does, whether they are allocated appropriately.

Agency Comments and Our Evaluation

In written comments on a draft of our report signed by the Director, Departmental GAO/OIG Liaison within the Office of the Chief Financial Officer, DHS generally concurred with our recommendations. DHS also offered specific comments related to these recommendations, including:

- Regarding our recommendation that DHS establish IT goals and performance measures, the department emphasized that it is developing road maps for its eight priority areas that, over the next few months, will include developing goals, performance measures, and time lines for implementation. We believe that DHS's plans are consistent with our recommendation.
- On our recommendation to establish milestones for the initiation and completion of major information and technology management activities,

DHS stated that its interpretation was that the recommendation pertained to having an established IT investment management structure and centered its comments on its plans related to two of its priorities—enterprise architecture and portfolio management. We agree that these two areas are covered by our recommendation. However, our recommendation is broader than just these two areas, instead covering any information and technology management activity identified as significant through DHS's IT strategic planning processes (e.g., the development of milestones related to activities associated with each of DHS's IT priorities).

- With respect to our recommendation on IT staffing, DHS stated that on July 30, 2004, the CIO approved funding for an IT human capital center of excellence. This center is 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. DHS's stated action represents a first step toward accomplishing these activities.

DHS also provided specific comments on our characterization of the department's progress related to its IT investment management process. The department described its IT investment governance boards and processes and stated that it believed that its IT investment management process has matured and that IT investments are subject to a rigorous corporate review. While our report acknowledges that DHS had changed its IT investment management process to reflect lessons learned and continuous improvement of the process, we believe that our characterization of this process as still maturing is appropriate. For example, the directive that instructs DHS component entities on which investments need to be approved and by what governance board does not reflect the current process. Regarding DHS's comment that its IT investments are subject to a rigorous corporate review, as we reported, DHS has not established a process to ensure that control reviews of IT investments are performed in a timely manner and many of DHS's IT investments have not undergone such reviews.

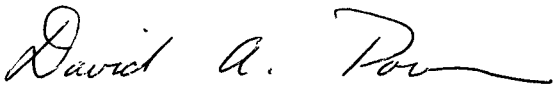
Lastly, DHS provided technical comments, which we addressed in the report as appropriate. DHS's written comments, along with our responses, are reproduced in appendix II.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the

report date. At that time, we will send copies of this report to the Secretary of Homeland Security and the Director, Office of Management and Budget. Copies will also be available at no charge on GAO's Web site at www.gao.gov.

If you have any questions on matters discussed in this report, please contact Randy Hite at (202) 512-3439 or via e-mail at hiter@gao.gov. Other key contributors to this report were Season Dietrich, Tamra Goldstein, and Linda Lambert.

Randolph C. Hite
Director
Information Technology Architecture
and Systems Issues



David A. Powner
Director, Information Technology Management Issues

Department of Homeland Security Governance Entities

Governance board	Membership	Example of responsibilities
Investment Review Board	Chaired by Deputy Secretary Members include under secretaries and other department executives, including the Chief Information Officer (CIO)	Makes final determination as to whether to approve level 1 investments
Department of Homeland Security (DHS) Management Council	Chaired by Under Secretary for Management Members include chief operating officers or equivalents	Ensures that management activities are in alignment with DHS mission, strategies, and goals Makes recommendations regarding departmental management policies, procedures, and processes
Joint Requirements Council	Chaired by chief operating officers or equivalent of one of the line agencies on a rotating basis (currently 1 year) Members include senior managers,[a] including the Chief Technology Officer, who is within the office of the CIO	Decision authority for level 2 investments[b] Reviews all projects/programs and new initiatives greater than $100 million in preparation for the investment review board Validates requirements
Asset Management Board	Chaired by DHS Director of Asset Management Members are designated asset managers from the component agencies	Reviews and approves real property acquisitions, sales, and transfers $1 million and above Develops and implements asset management policy, procedures, and business practices
Enterprise Architecture Board	Chaired by CIO Members are CIOs from component entities	Performs technical reviews of IT investments Approves IT business cases and develops IT strategic guidance
Integrated Product Teams	Members include subject matter experts from appropriate functional disciplines	Convened by the Joint Requirements Council to address specific issues Has a defined scope and duration and disbands upon completion
Commodity Councils/ Management Boards	Members include program and procurement experts from organizational elements	Develop and implement DHS sourcing strategy for a specific commodity and manages specific asset types Coordinate policy formulation and define authorities and processes for achieving integrated asset management

Source: DHS.

[a]Senior executives (SES) with a broad operating background who understand the requirements and capabilities of their agencies and who have sufficient authority to make decisions for the agency in their role on the Joint Requirements Council.

[b]According to the DHS coordinator of this process, level 3 IT investments are approved by the component agency and are subject to review by the CIO, Chief Financial Officer, and Chief Procurement Officer, also known as the Management Review Council. If these officials have concerns about the investment or find that there are cross-programmatic issues to be addressed, they can refer the investment to the Joint Requirements Council for review.

Comments from the Department of Homeland Security

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

Homeland Security

August 12, 2004

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

Dear Mr. Hite:

RE: Draft Report GAO-04-702: Formidable Information Technology Challenge Requires Institutional Approach (GAO Job Code 310464)

Thank you for the opportunity to review the above referenced draft report. We generally concur with the draft report's recommendations but there are several items we want to address.

DHS appreciates that the draft report acknowledges both DHS's progress and challenges in information and technology management, particularly in light of the diversity of the 22 inherited agencies and the size and complexity of the Department. DHS is both meeting these challenges while at the same time shepherding the integration of IT systems and management approaches of its many organizational elements into an enterprise architecture.

See comment 1.

The draft report discusses the draft IRM Strategic Plan that DHS had worked on and incorrectly suggests that in March 2004, the Department issued the IRM plan as an official Version 1.0 of its IT Strategic Plan. This IRM plan, however, is still draft and does not reflect the full scope of DHS' IT Strategic Planning initiative. The DHS Chief Information Officer (CIO) intends to issue an IT Strategic Plan before the end of this calendar year.

See comment 2.

Nevertheless, the Department's IT efforts are designed to support the Department's Strategic Plan goals. As noted in the draft GAO report, the DHS CIO, in conjunction with the DHS CIO Council, has identified eight priority areas and has developed roadmaps for each of these priorities. These roadmaps include a description of the current condition of the areas, the need for change, the planned future state, initiatives underway or needed, and any barriers to achieving these goals.

Equally important, the Department released Version 1.0 of its Enterprise Architecture (EA) in September 2003. The Department recognizes that due to time constraints, Version 1.0 was not an all-inclusive product; and accordingly, the Department continues its efforts to improve and will release Version 2.0 of the EA in September 2004.

The draft report states that the investment management process is still maturing and has yet to be institutionalized, and that most projects have not yet been incorporated into a departmental oversight process. The functionality and effectiveness of the investment governance bodies have matured during the last year. The Investment Review Board (IRB) is the executive review board that provides acquisition oversight of DHS Level 1 investments (greater than $100 million), and conducts portfolio management reviews. The IRB conducts systematic reviews of investment submissions and

approves key decisions. It also serves as a forum for discussing investment issues and resolving problems requiring senior management attention. The DHS CIO serves on the IRB and actively participates in all IT investment decisions.

Similarly, a Joint Requirements Council (JRC) was established as a senior requirements review board that conducts program reviews to oversee the requirements generation process, validate mission needs statements, review cross-functional needs and requirements, and make programmatic recommendations to the IRB on proposed new programs. The JRC has decision authority for projects/programs whose cost is $50-$100 million. The DHS CIO also is a member of the JRC.

See comment 3.

In addition, the Department created an Enterprise Architecture Board (EAB) chaired by the CIO and composed of all CIOs from the Organizational Elements. The EAB exercises architecture oversight of IT investments, reviews and approves IT investments with an acquisition cost between $1-$10 million or a Life Cycle Cost of $5-$20 million, and approves IT business cases and develops IT strategic guidance. Another component of this effort involves an Asset Management Board, chaired by the DHS Director of Asset Management, with membership from the Organizational Elements. The Asset Management Board develops and implements asset management policy, procedures and business practices, and establishes asset management controls and program metrics. This Board reviews IT programs from various perspectives. Interim guidance governing DHS investment review process responsibilities was issued in May 2004. For certain, the DHS investment management process has matured through the above described processes and structures. As a result, DHS IT investments are subject to a rigorous corporate review.

See comment 4.
See comment 5.

The draft report states that, as related to information security management, DHS did not have a process to ensure that all plans of action and milestones (POAM) for identified weaknesses were developed, implemented, and managed. The Department has instituted use of a tool, Trusted Agent FISMA, which allows the CIO and the Chief Information Security Officer (CISO) to monitor each Organizational Element's progress in developing and achieving the milestones identified in the POAM. On the other hand, the draft report also states that "DHS has developed an information security program strategic plan, which identifies major program areas, goals, and objectives. These major security program areas allow DHS to implement and maintain information security as part of its capital investment control process, systems development life cycle, and the enterprise architecture, and are essential to providing security services that protect the confidentiality, integrity, and availability of information and to provide accountability for activities on DHS networks and computing platforms." We find such statements somewhat conflicting as presented.

See comment 6.

See comment 7.

See comment 8.

Human capital management issues are the key to successful implementation of the Department and are crucial to design, development, implementation, and maintenance of information and technologies. The draft report discusses IT human capital management and points out the need for strategic human capital planning. This is a government-wide issue that transcends the IT environment; the DHS CIO has taken steps to address GAO's concerns. For example, there is currently underway an initiative that responds directly to your recommendation, regarding analysis of IT staff to determine whether IT professionals have the appropriate skills for the areas in which they are deployed. The DHS CIO, in conjunction with the DHS CIO Council, has as one of his eight priorities, IT Human Capital. On July 30, 2004, the DHS CIO formally approved funding for the IT Human Capital Center of Excellence (COE). The COE is lead by the CIO of the Federal Law Enforcement Training Center (FLETC) and is supported by a Director within the OCIO (Office of the CIO) and a team of Human Capital professionals drawn from several of the Organizational

See comment 9.

Elements within DHS. The COE is working under the governance of the DHS CIO Council and with the guidance of the DHS Chief Human Capital Officer (CHCO) and is tasked with delivering plans, processes and procedures to execute the IT human capital strategy necessary to support the mission and goals of DHS. The COE will be conducting an analysis of the skill sets of all DHS IT professionals. This analysis will include an assessment of which skills are currently held by the IT employees versus which skills are necessary for each employee to have in order to meet the DHS mission and goals.

See comment 10.

The draft report recommends that the DHS CIO establish IT goals and performance measures to address how information and technology management contributes to program productivity, the efficiency and effectiveness of agency operations, and the service to the public. The draft report, however, glosses over DHS's performance measures process. At the capital and investment level the Department has performance measures that are captured in the OMB Exhibit 300. At the program level DHS is developing more robust monitoring of on-going programs using key measures. The DHS CIO and the DHS CIO Council have established eight priority areas: Information Sharing, Governance, IT Human Capital, Enterprise Architecture, Mission Rationalization, Infrastructure, Portfolio Management, and Information Security. Initial roadmaps have been developed for each of these priority areas. Over the next few months, each priority area will develop goals, performance measures, and timelines for implementation.

See comment 11.

The Department interprets GAO's recommendation to establish milestones for the initiation and conception of major information and technology management activities, to mean that there should be an established IT Investment Management structure. Two of the eight priorities established by the DHS CIO and the DHS CIO Council support this recommendation: Enterprise Architecture and Portfolio Management. The DHS CIO is establishing an Enterprise Architecture COE and is developing a Portfolio Management process, which will direct our IT investment decisions. Additionally, we have established and implemented a Capital Planning and Investment Control Process, and have used this process to influence and direct our investments. The Department has developed a draft Systems Development Life Cycle Model which is currently under review and will be implemented in the first quarter of FY 2005. In addition, the Department is developing consolidated tools, processes, and procedures for Program Reviews. Once these initiatives are complete, the Department will have all the elements in place for a robust investment management system covering all aspects of the investment life cycle including the Selection, Control, and Evaluation phases.

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

Sincerely,

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

The following are GAO's comments on the Department of Homeland Security's (DHS) letter dated August 12, 2004.

GAO Comments

1. Although the IRM strategic plan is not labeled draft, we changed our characterization of the plan in the report based on the DHS comments.

2. As discussed in the report, these road maps are draft and incomplete (e.g., they do not include fully defined goals and performance measures).

3. The Joint Requirements Council's charter does not list the CIO as a member of this council; instead the chief technology officer is the Office of the CIO's representative on the council, which is reflected in our report.

4. We believe that our characterization of DHS's IT investment management process as still maturing is appropriate. For example, the May 2003 directive that instructs DHS component entities on which investments need to be approved and by what governance board does not reflect the current process, and more recent DHS documentation related to the process provides inconsistent information.

5. We disagree because, as we stated in the report, DHS has not established a process to ensure that control reviews of IT investments are performed in a timely manner, and many of DHS's IT investments have not undergone such reviews.

6. We added information about the DHS tool to the report.

7. The DHS quote does not include our attribution in the report that the assessment of the information security program areas is the department's own representation. We did not evaluate the information security program strategic plan.

8. We do not agree that these statements are conflicting. The management of the department's plans of action and milestones is just one of many planned actions discussed in the information security program strategic plan.

9. As stated in the report, we agree that human capital management is a key to the success of the department and that the challenges that the

federal government faces in maintaining a high-quality IT workforce are long-standing and widely recognized. It is because of these views that we are concerned that the department did not meet the CIO's goal of having a current inventory of IT skills by July 2003 and an action plan by September 2003. Nevertheless, DHS's stated action represents a first step toward accomplishing these activities.

10. Our report dealt with enterprise-level performance measures, not project-specific measures as required by the exhibit 300s. With respect to DHS's plans for each of the priority areas, we believe this is consistent with our recommendation.

11. We agree that the two priority areas discussed in the DHS letter are covered by our recommendation. However, our recommendation is broader than just these two areas. Specifically, our recommendation covers any information and technology management activity identified as significant through DHS's IT strategic planning processes (e.g., the development of milestones related to activities associated with each of DHS's IT priorities).

Related GAO Products

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

Homeland Security: Performance of Information System to Monitor Foreign Students and Exchange Visitors Has Improved, but Issues Remain. GAO-04-690. Washington, D.C.: June 18, 2004.

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

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.

Information Technology: Early Releases of Customs Trade System Operating, but Pattern of Cost and Schedule Problems Needs to Be Addressed. GAO-04-719. Washington, D.C.: May 14, 2004.

Homeland Security: First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed. GAO-04-586. Washington, D.C.: May 11, 2004.

Additional Posthearing Questions Related to Proposed Department of Homeland Security (DHS) Human Capital Regulations. GAO-04-617R. Washington, D.C.: April 30, 2004.

Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration. GAO-04-494. Washington, D.C.: April 16, 2004.

Posthearing Questions Related to Proposed Department of Homeland Security (DHS) Human Capital Regulations. GAO-04-570R. Washington, D.C.: March 22, 2004.

Human Capital: Preliminary Observations on Proposed DHS Human Capital Regulations. GAO-04-479T. Washington, D.C.: February 25, 2004.

Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges. GAO-04-385. Washington, D.C.: February 12, 2004.

Information Technology: OMB and Department of Homeland Security Investment Reviews. GAO-04-323. Washington, D.C.: February 10, 2004.

Coast Guard: New Communication System to Support Search and Rescue Faces Challenges. GAO-03-1111. Washington, D.C.: September 30, 2003.

Human Capital: DHS Personnel System Design Effort Provides for Collaboration and Employee Participation. GAO-03-1099. Washington, D.C.: September 30, 2003.

Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed. GAO-03-1083. Washington, D.C.: September 19, 2003.

Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning. GAO-03-563. Washington, D.C.: June 9, 2003.

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

Customs Service Modernization: Automated Commercial Environment Progressing, but Further Acquisition Management Improvements Needed. GAO-03-406. Washington, D.C.: February 28, 2003.

Major Management Challenges and Program Risks: Department of Homeland Security. GAO-03-102. Washington, D.C.: January 2003.

Homeland Security: Information Technology Funding and Associated Management Issues. GAO-03-250. Washington, D.C.: December 13, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project. GAO-02-545. Washington, D.C.: May 13, 2002.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

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

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00