United States General Accounting Office

GAO

Report to the Chairman, Committee on Transportation and Infrastructure, House of Representatives

May 2004

INFORMATION TECHNOLOGY

Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems

GAO
Accountability ★ Integrity ★ Reliability

G A O
Accountability•Integrity•Reliability
Highlights

Highlights of GAO-04-509, a report to the Chairman, Committee on Transportation and Infrastructure, House of Representatives

Why GAO Did This Study

The Department of Homeland Security (DHS) faces the daunting task of bringing together 22 diverse agencies to lead efforts to protect the homeland. Among the challenges posed by this transformation is integrating these agencies' diverse information technology (IT) systems: mission support, administration, and infrastructure (e.g., networks). GAO was asked to determine (1) whether DHS has defined its IT systems integration strategy and (2) how DHS is ensuring that IT investments made by component agencies (specifically focusing on the Federal Emergency Management Agency, the Transportation Security Administration, and the Coast Guard) are aligned with the department's strategic direction.

What GAO Recommends

GAO is making recommendations to the Secretary aimed at limiting the department's investment in IT systems until the department's IT strategic management framework is sufficiently defined and the department's CIO has sufficient authority to effectively implement it.

GAO provided a draft of this report to DHS for comment. In its comments, DHS did not agree or disagree with our findings, conclusions, or recommendations. Rather, the comments provided information on DHS's IT challenges and priorities that is consistent with our report.

www.gao.gov/cgi-bin/getrpt?GAO-04-509.

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.

May 2004

INFORMATION TECHNOLOGY

Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems

What GAO Found

DHS is developing an IT systems integration strategy through its ongoing efforts to finalize and implement an IT strategic plan, an enterprise architecture, and IT capital planning and investment control processes. According to the department, these three elements—which are essential parts of a framework for achieving effective systems integration—are areas of focus and planned to be fully in place before the end of 2004. The DHS Chief Information Officer (CIO) attributed the limited progress on the systems integration framework to date to (1) insufficient staffing, (2) higher priority demands (such as establishing a departmentwide e-mail system), and (3) near-term high-payoff opportunities (such as consolidating wireless communication capabilities).

In the interim, DHS and its components have taken steps intended to promote the alignment of its components' ongoing and planned IT investments with the department's strategic direction. The steps include (1) subjecting major investments to review and approval by various departmental investment review boards, (2) continuing to have component agencies follow the IT strategic management structures and processes that they had before the department was formed, and (3) having meetings between component staff responsible for IT investments and staff working on the department's IT strategic management framework. GAO corroborated the department's use of this approach through analysis of IT investments being pursued by three DHS components, which the components indicated were representative of their general approach to aligning investments with the department's evolving strategic direction.

While these steps have merit, they do not provide adequate assurance of strategic alignment across the department. For example, the second step simply continues the various approaches that produced the diverse systems that the department inherited, while the third relies too heavily on oral communication about complex IT strategic issues that are not yet fully defined—which increases the chances of misunderstanding and missed opportunities for integration. Moreover, the DHS CIO does not have authority and control over departmentwide IT spending—although such control is important for effective systems integration, as shown by GAO's research on successful private and public sector organizations and experience at federal agencies. Until its IT strategic framework is fully defined and effectively implemented, DHS runs the risk that the component agencies' ongoing investments—collectively costing billions of dollars in fiscal year 2004—will need to be reworked in the future, so that they can be effectively integrated and provide maximum value across DHS.

Contents

Letter

Appendixes

Figure

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
IT	information technology
OMB	Office of Management and Budget
TSA	Transportation Security Administration

G A O
Accountability ★ Integrity ★ Reliability

**United States General Accounting Office
Washington, D.C. 20548**

May 21, 2004

The Honorable Don Young
Chairman, Committee on Transportation and Infrastructure
House of Representatives

Dear Mr. Chairman:

When the Department of Homeland Security (DHS) began operations in March 2003, it faced the daunting task of bringing together 22 diverse agencies. Not since the creation of the Department of Defense had the federal government undertaken a transformation of this magnitude. As we previously reported,[1] such a transformation poses significant management and leadership challenges, one of which is integrating the 22 agencies' respective mission support, administrative, and infrastructure (e.g., networks) information technology (IT) systems.

In response to your request to review this system integration challenge, we agreed with your office to determine (1) whether DHS has defined its systems integration strategy and (2) how DHS is ensuring that component agency system investments are aligned with the department's strategic direction. In performing our work on the second objective, as you requested, we focused on three DHS component agencies: the Federal Emergency Management Agency, the Transportation Security Administration, and the Coast Guard. Our work at DHS and component agencies was performed in accordance with generally accepted government auditing standards. Details of our scope and methodology are in appendix I.

[1] For example, see U.S. General Accounting Office, *Major Management Challenges and Program Risk: 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).

Results in Brief

DHS is in the process of defining its systems integration strategy. The department has several efforts under way: finalizing a draft IT strategic plan, institutionalizing its recently revised IT capital planning and investment control processes, and developing the next version of its enterprise architecture.[2] DHS initiated these efforts shortly after it began operations, and it plans to have them fully in place before the end of 2004. If defined and implemented properly, these efforts could go a long way toward providing the necessary strategic IT management framework for, among other things, integrating DHS's current and future systems and aligning them with the department's strategic goals and mission. According to DHS's Chief Information Officer (CIO), who is responsible for leading these efforts, progress to date on the systems integration strategy has been impeded by (1) insufficient staffing; (2) higher priority demands, such as establishing a departmentwide e-mail system; and (3) near-term, high-payoff opportunities, such as consolidating wireless communication capabilities. Nevertheless, the CIO stated that completing DHS's strategic IT management framework is important and an area of focus in 2004 because the longer the department's component organizations continue to invest in systems without such an effectively implemented framework, the greater the risk that these component systems will later require costly rework to integrate.

Until the framework has been completed, DHS is taking interim steps that are intended to address ongoing and planned component IT investments' integration and alignment with the evolving framework. These steps include (1) departmental assessment and approval of certain major investments, (2) component agencies' continued use of the same strategic IT management structures and processes that they had before the department was formed, and (3) meetings between persons in these components who are responsible for ongoing and planned IT investments and those persons who are putting in place the department's strategic IT management framework. While these steps have merit, they do not provide adequate assurance of strategic alignment across the department, and thus the risk is increased that the 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 maximize

[2] An enterprise architecture is the explicit description and documentation of the current and desired relationships among business and management processes and information technology. It describes the "current architecture" and "target architecture."

departmentwide value. For example, the second step continues reliance on the components' various approaches that produced the diverse set of systems that the department inherited, while the third relies too heavily on oral communication about strategic contexts and frames of reference that have not yet been fully defined, thus increasing the chances of both misunderstanding and missed integration opportunities. Moreover, they do not provide the department's CIO with the level of IT spending authority and control that our research at leading organizations and past work at federal departments and agencies has shown is important for effective integration of systems across organizational components.

To help DHS better manage the risks that it faces, we are making recommendations to the Secretary aimed at limiting the department's near-term investment in new and existing IT systems until the department's strategic IT management framework is sufficiently defined and the department's CIO has sufficient authority to effectively implement it. Examples of our recommended areas of near-term investment are cost-effective efforts that are congressionally directed, take advantage of relatively small, low-risk opportunities to leverage technology in satisfying a compelling homeland security need, or support operations and maintenance of existing systems critical to DHS's mission.

In commenting on a draft of this report, DHS did not agree or disagree with our findings, conclusions, or recommendations. Rather, the department described DHS's IT challenges and priorities and provided documentation on them, including efforts to achieve its priorities. The information conveyed in DHS's comments is consistent with information obtained during our review that showed progress and plans for institutionalizing the department's strategic IT management framework.

Background

In the aftermath of the terrorist attacks of September 11, 2001, responding to potential and real threats to homeland security became one of the federal government's most significant challenges. To address this challenge, the Congress passed, and the President signed, the Homeland Security Act of 2002, which merged 22 federal agencies and organizations into DHS, making it the third largest federal department, with an annual budget of about $40 billion.[3] As we previously reported,[4] one of the department's key challenges will be integrating the 22 components' respective IT organizations and the approximately 700 mission support, administrative, and infrastructure IT systems.

DHS Mission and Organization

In establishing the new department, the Congress defined a seven-point mission for DHS:

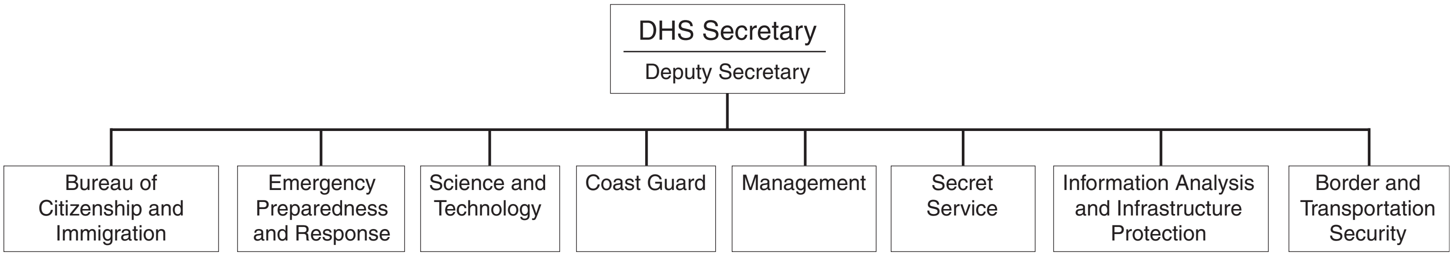
- prevent terrorist attacks within the United States;
- reduce the vulnerability of the United States to terrorism;
- minimize the damage and assist in the recovery from terrorist attacks;
- carry out all functions of entities transferred to the department, including acting as a focal point regarding natural and man-made crises and emergency planning;
- ensure that the functions of the components within the department that are not directly related to securing the homeland are not diminished or neglected;
- ensure that the overall economic security of the United States is not diminished by efforts aimed at securing the homeland; and
- monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

[3] U.S. Department of Homeland Security, *Budget in Brief: Fiscal Year 2005*.

[4] See GAO-03-102 and GAO-02-886T.

To help accomplish this integrated homeland security mission, the various mission areas and associated programs of 22 federal agencies were merged, in whole or in part, into DHS. The department's organizational structure generally consists of eight major entities, the U.S. Secret Service, the U.S. Coast Guard, the Bureau of Citizenship and Immigration Services, and five directorates—Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, Information Analysis and Infrastructure Protection, and Management (see fig. 1).

Figure 1: Simplified DHS Organization Chart


DHS Secretary
Deputy Secretary
Bureau of Citizenship and Immigration
Emergency Preparedness and Response
Science and Technology
Coast Guard
Management
Secret Service
Information Analysis and Infrastructure Protection
Border and Transportation Security

Source: GAO.

Within the Management Directorate is the DHS Office of the CIO, which is assigned primary responsibility for addressing departmentwide system integration issues. According to the CIO, this office is responsible for, among other things, developing and facilitating the implementation of such integration enablers as the department's IT strategic plan, key aspects of the IT investment management process, and enterprise architecture. (Each of these three system integration enablers is discussed in greater detail in app. II.) According to the CIO, his office was authorized 65 positions[5] and provided $245 million in funding for fiscal year 2004.[6]

[5] Of these positions, 14 are currently vacant, and 9 are in the process of being filled.

[6] Of this amount, $185 million is for new systems, and $60 million is for operation and maintenance of existing systems.

DHS Predecessor Agencies and Programs Have Varying Characteristics

The 22 agencies and agency components that were merged into DHS vary in a number of ways, including their time in existence, size, and mission focus, the latter ranging from law enforcement and border security to biological research, computer security, and disaster mitigation. The Federal Emergency Management Agency (FEMA), the Transportation Security Administration (TSA), and the U.S. Coast Guard illustrate this variety:

- *FEMA*: This agency was formed about 25 years ago to consolidate emergency and disaster relief functions that were spread across several federal agencies. FEMA's mission is to help the United States prepare for, prevent, respond to, and recover from disasters. FEMA, which is now in DHS's Emergency Preparedness and Response directorate, has about 2,500 full-time employees, an additional 5,000 stand-by disaster reservists, and an annual operating budget of about $4.8 billion.

- *TSA*: This agency was established about 2½ years ago as part of the U.S. Department of Transportation in response to the September 11 terrorist attacks. TSA's mission includes ensuring safety in civil aviation and at airports through screening, intelligence, education, and regulation. Now in DHS's Border and Transportation Security directorate, TSA has about 53,000 employees and an annual operating budget of about $5.3 billion.

- *Coast Guard*: This agency was established over 200 years ago, and in time of war is under the direction of the Department of the Navy. The Coast Guard's mission is to protect the public, the environment, and U.S. economic and security interests in international waters and America's coasts, ports, and inland waterways. The Coast Guard, which is an agency that reports directly to the DHS Secretary, has approximately 39,000 full-time military personnel, 6,000 full-time permanent civilian employees, and an operating budget of about $7.5 billion.

Each of the 22 agencies or agency components also brought with it its individual IT management organization. In particular, FEMA, TSA, and the Coast Guard each have CIO organizations to perform IT management functions, such as investment management, information security, and enterprise architecture. According to FEMA, its CIO organization has about 262 permanent employees and approximately 70 temporary (disaster-related) employees. TSA reports that its CIO organization has roughly 145 employees. The Coast Guard reports that its CIO organization has approximately 140 employees. Collectively, these three CIO organizations account for about 600 authorized positions and control about $3.6 billion in fiscal year 2004 IT budget and spending.

Integrating 22 Component Organizations' Numerous and Diverse IT Systems Poses a Formidable Challenge

In addition to the aforementioned differences among the 22 agencies and agency components, the 22 agencies also brought their respective IT systems. DHS inherited about 700 of these systems, and, according to the DHS CIO, the department has categorized them into three groups: direct mission support, back office, and infrastructure. In fiscal year 2004, DHS requested about $4.1 billion—the third largest IT budget in the federal government[7]—to manage these systems, including operating and maintaining existing systems and acquiring new systems that were being initiated or were under way within the 22 agencies and agency components before the department was formed. Examples of new system investments include the following in the Border and Transportation Security directorate:

- *Integrated Surveillance Intelligence System*: This system is to provide full-time border coverage through ground-based sensors, fixed cameras, and computer-aided detection capabilities. For fiscal year 2004, funding for the system is about $55.7 million. The life-cycle cost for the system is estimated to be about $1.17 billion.

- *Computer Assisted Passenger Prescreening System II*: This system, better known as CAPPS II, is to identify airline passengers requiring additional security attention. For fiscal year 2004, funding for the system is about $45 million. The life-cycle cost of the system through fiscal year 2008 is estimated to be about $380 million.[8]

- *Automated Commercial Environment*: This system, also known as ACE, is to be a new trade processing system that is planned to support effective and efficient movement of goods into the United States. For

[7] Office of Management and Budget, *Budget of the U.S. Government, Fiscal Year 2005, Report on IT Spending for the Federal Government for Fiscal Years 2003, 2004, and 2005.* According to this document, the Departments of Defense and Health and Human Services have the first and second largest IT budgets, respectively.

[8] U.S. General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: February 2004).

fiscal year 2004, funding for the system is about $318.7 million. The life-cycle cost of the system is estimated to be about $1.5 billion.[9]

- *United States Visitor and Immigrant Status Indicator Technology*: This system, commonly called US-VISIT, is to strengthen management of the pre-entry, entry, status, and exit of foreign nationals who travel to the United States. For fiscal year 2004, funding for US-VISIT is about $330 million. The department did not provide us with an estimated life-cycle cost for the system.[10]

Control over the department's IT budget is vested primarily with the CIO organizations within each of its component organizations. These component CIO organizations are accountable to the heads of DHS's respective organizational components. For example, the CIO for the Bureau of Customs and Border Protection, which is a component of the Border and Transportation Security directorate, reports to the Commissioner of Customs and Border Protection, not to the DHS CIO.

To maximize its mission performance, DHS faces the enormous task of integrating and consolidating its roughly 700 systems. This includes exploiting opportunities to eliminate and consolidate systems in order to improve mission support and reduce system costs. As we recently reported,[11] OMB, before DHS's formation, reviewed the IT investments within the department's predecessor agencies and agency components to identify, among other things, whether savings could be realized through integration and consolidation. In July 2002, OMB reported that 2-year savings of between $165 million and $285 million could be possible through consolidation of the components' IT investments in infrastructure and business systems alone. OMB also acknowledged that at the time of its review, the anticipated budgetary savings had not yet occurred, and for that reason, it assigned DHS responsibility for executing the consolidations and tracking savings when they are realized. Accordingly, we recommended,

[9] U.S. General Accounting Office, *Automated Commercial Environment Progressing, but Further Acquisition Management Improvements Needed*, GAO-03-406 (Washington, D.C.: February 2003).

[10] U.S. General Accounting Office, *Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, GAO-03-1083 (Washington, D.C.: September 2003).

[11] For more information, see U.S. General Accounting Office, *Information Technology: OMB and Department of Homeland Security Investment Reviews*, GAO-04-323 (Washington, D.C.: February 2004).

among other things, that DHS periodically report to its congressional committees the budgetary savings that result from department consolidation and integration efforts.

DHS Is in the Process of Defining Its Systems Integration Strategy

Our research on successful public and private sector organizations and our experience in reviewing the management of agency integration efforts shows that those entities that were successful in such integration relied on effective strategic IT management frameworks to guide their efforts, including developing IT strategic plans, implementing effective IT investment management and decision-making practices, and developing and enforcing an enterprise architecture.[12] Moreover, we have previously reported that the effective integration of new and existing IT systems is a critical success factor for DHS because this integration is a means to (1) more efficient operations, through, for example, elimination of system redundancies and overlap, and (2) more effective operations, through, for example, increased information sharing within DHS and between it and other agencies involved in homeland security (e.g., the Federal Bureau of Investigation and the Central Intelligence Agency).[13] The tenets of developing and using a strategic management framework are described in our prior research on best practices in private-sector firms and government organizations[14] and are called for in federal IT management laws and guidance, such as the Clinger-Cohen Act[15] and OMB Circular No. A-130.[16] Jointly, the act and circular direct federal agencies to develop and

[12] For example, see U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO-03-584G (Washington, D.C.: Apr. 1, 2003); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Version 1.1)*, GAO-04-394G (Washington, D.C.: March 2004); and *Executive Guide: Improving Mission Performance through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1994).

[13] For example, see U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).

[14] We have issued guidance to agencies related to enterprise architecture, IT investment management, and other management issues. For example, see GAO-03-584G and GAO-04-394G.

[15] Clinger-Cohen Act, 40 U.S.C. 11101–11703.

[16] Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130.

implement systems integration strategies through a comprehensive strategic IT management framework that, among other things, includes

- developing and implementing an IT strategic plan that defines how IT will be managed to support agency missions;
- establishing and implementing an IT investment management process that is linked to budget formulation and execution, and provides for continuous and informed investment decision-making based on the relative costs, benefits, and risks of competing investment options; and
- developing and implementing an enterprise architecture that describes the current and future operational and technological states and provides a plan for sequencing between the two states that can be used for system acquisition and investment decision-making purposes.

(Each of these framework components is described in more detail in app. II.) The processes and tools associated with these strategic management disciplines serve to provide a common, authoritative understanding of both the desired ends, such as systems integration, and the means to these ends.

DHS has not yet completed a systems integration strategy, but it is in the process of doing so through its ongoing efforts to finalize a draft IT strategic plan, institutionalize a recently revised IT investment management process, and develop a more complete enterprise architecture. Each is discussed below.

- *IT strategic plan.* DHS is in the process of finalizing a draft plan. According to a March 2004 draft,[17] which department officials told us was current, the plan is to be the driving force in establishing DHS's strategic IT management framework. Its stated purpose is to discuss how the department plans to manage and use IT to achieve strategic mission goals.

  To achieve mission goals, the plan identifies eight priorities for 2004: information sharing, mission rationalization, portfolio management, security, single infrastructure, enterprise architecture, governance, and human capital. DHS officials said that, when completed, the plan is to

[17] Department of Homeland Security, *Information Resources Management Strategic Plan 2003-2008 v. 1.0*, draft (Washington, D.C.: March 2004).

define the associated steps to achieve each priority. For example, to achieve the priority of a single infrastructure, which calls for the establishment of a single wide area network and associated infrastructure connecting the department's components, the plan identifies eight initiatives—such as establishing enterprise information assurance, implementing a standard desktop computing environment, and consolidating data centers. The plan also provides for establishing key IT management processes and products—namely, investment management and enterprise architecture, respectively—that the department views as essential to implementing the plan. According to the CIO, the department has recently identified a senior DHS business sponsor and a member of the CIO's office to develop detailed plans for each priority, and these plans are to be completed by mid-2004.

- *Investment management process.* DHS has developed and has begun implementing a departmental IT investment management process. Specifically, in May 2003, DHS issued an investment review management directive and an IT capital planning and investment control guide, which specify investment documentation and review requirements. The stated purpose of the management directive includes ensuring that spending on IT investments directly supports DHS's mission goals and objectives, and that duplicative spending on system investments is identified for cost-saving consolidation. Among other things, this directive requires that system investments support the department's mission goals and objectives, including those identified in the IT strategic plan, enterprise architecture, other department policies and strategies (e.g., business strategic plan), and federal strategies and guidance (e.g., the National Strategy for Homeland Security[18]). The directive also requires that as part of the investment approval process, component organizations demonstrate to executive management that proposed project requirements are consistent with DHS's strategic plans and enterprise architecture.

  We reported in February 2004[19] that this process was being refined and institutionalized. For example, while DHS had established a

[18] Office of Homeland Security, The White House, *National Strategy for Homeland Security* (Washington, D.C.: July 2002).

[19] For more information, see U.S. General Accounting Office, *Information Technology: OMB and Department of Homeland Security Investment Reviews*, GAO-04-323 (Washington, D.C.: February 2004).

departmentwide IT Investment Review Board for managing and overseeing expensive and mission-critical system investments, the board had only reviewed 9 investments, while about 100 investments were eligible for review. Accordingly, we recommended that DHS develop a schedule for reviewing the investments under its control and oversight. According to the CIO, DHS has since refined its investment review and control process by, for example, creating a hierarchy of investment review boards, adjusting the criteria governing the level of board review needed for projects, and developing templates and other tools to aid in the review process. The CIO stated that the potential effect of these changes will be to expedite the backlog of project reviews. DHS is now focusing on institutionalizing this process, including developing review schedules for the respective boards.

- *Enterprise architecture:* DHS is in the process of developing the next version of its enterprise architecture. In August 2003, DHS issued the first version of its architecture, which DHS officials described as conceptual and high-level. Nevertheless, DHS officials said the department has been able to use the architecture on a limited basis to, for example, consolidate investments into related areas in developing the department's fiscal year 2005 budget request, including identifying opportunities to merge proposals. DHS plans to continue evolving the architecture and issue another version in September 2004. We are currently reviewing the initial version of the architecture at the request of the Chairman of the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform.

According to the CIO, although DHS started working on its strategic IT management framework soon after the department began operation, progress to date on completing the framework—which would provide, among other things, a departmentwide systems integration strategy—has been impeded by (1) insufficient staffing; (2) higher priority demands, such as establishing a departmentwide e-mail system and linking and consolidating existing DHS component networks; and (3) near-term, high-payoff opportunities, such as consolidating wireless communication and computer operations capabilities, and linking DHS networks with partner agencies outside the department.

Of these three issues, the CIO stated that insufficient staffing is currently the biggest obstacle. More specifically, the CIO said that his office received substantially less 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. The CIO also said that his office does not have authority over the hundreds of staff in the component CIO offices and billions of dollars that the 22 agencies and agency components control, and he acknowledged that DHS components often each have substantially more IT staff resources than his office. In contrast, 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.[20]

Additionally, the CIO told us that completing the department's strategic IT management framework and implementing the kind of IT budgetary control and authority model needed for its effective implementation and enforcement is important and is an area of focus in 2004. The CIO added that completing this effort is important because the department continues to make substantial IT investments without the strategic management framework and the IT spending authority and control model needed to effectively integrate new and existing systems across the department. Our research on leading organizations and our experience at federal agencies show that proceeding in this manner increases the risk that investments may later require expensive rework to be effectively integrated and brought into alignment with the framework.[21]

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

[21] For example, see GAO-03-231 and GAO-01-376G.

DHS's Interim Steps to Reduce Risk of Rework for Ongoing IT Investments Are Not Sufficient

OMB has issued guidance to federal agencies directing them to develop and implement management structures and processes to ensure proper alignment between IT system investments and mission goals, strategic visions, plans, and future architectural states.[22] Additionally, our prior reviews at federal agencies and research on enterprise IT management have shown that attempts to align new and existing systems without an effective strategic management framework increase the risk of investing in system solutions that are duplicative, are not well integrated, are unnecessarily costly to maintain and interface, and do not effectively optimize mission performance.[23] Accordingly, until agencies develop strategic management frameworks, we have recommended[24] limiting IT spending to cost-effective efforts that are congressionally directed; are near-term, relatively small, and low-risk opportunities to leverage technology in satisfying a compelling agency need; support operations and maintenance of existing mission-critical systems; involve deploying an already developed and fully tested system; or support the establishment of an agency's strategic IT management framework.

Although DHS has defined and is institutionalizing structures and processes for IT investment management that are intended to align investments with the department's strategic direction, these investment management structures and processes are not yet fully implemented. Moreover, two key ingredients to effective investment management—a departmentwide IT strategic plan and the next version of the enterprise architecture—are not yet in place. In the interim, DHS has relied on its evolving investment management structures and processes. In addition, DHS officials told us that component agencies and organizations have followed the respective investment management approaches, strategic plans, and architectures that existed within their pre-DHS organizations, augmented by informal contacts with department-level strategic planners and architects, and consideration of the President's National Strategy for

[22] OMB Circulars No. A-130 and No. A-11.

[23] GAO/AIMD-10.1.23.

[24] For example, see U.S. General Accounting Office, *Tax Systems Modernization: Blueprint Is a Good Start, but Not Yet Sufficiently Complete to Build or Acquire Systems*, GAO/AIMD/GGD-98-54 (Washington, D.C.: February 1998).

Homeland Security[25] and statutory provisions related to homeland security, such as the Maritime Transportation Security Act. The use of these respective approaches is evident in the following three IT system investments from FEMA, TSA, and Coast Guard. According to the three components, these are illustrative of how each is ensuring that its IT investments are aligned with the department's strategic direction:

- *Grant Business Management System.* FEMA began acquiring this system in 2003 to automate its end-to-end grant management processes. According to FEMA, the system is to be fully operational by fiscal year 2009, and about $8.2 million is to be spent on it in fiscal year 2004. Currently, FEMA reports that the system's requirements have been defined and system design activities are under way. To justify its 2004 investment in the system, agency officials told us that they followed internal FEMA investment management processes, including explicitly mapping the system's functions to the goals and objectives in the National Strategy for Homeland Security, the President's Management Agenda,[26] and the FEMA Strategic Plan. These officials also told us that they have since begun to justify the system's fiscal year 2005 request following DHS's capital planning and investment control guidance, augmented by meetings with DHS's enterprise architecture team to discuss the system's alignment with the department's strategic direction. According to the officials, these meetings were not documented, but they said a discussion topic was the system's mission-needs statement, and whether it could be linked to the DHS enterprise architecture.

- *Integrated Intermodal Information System.* TSA began developing this system in 2003 to integrate selected multimodal passenger and cargo data for the purpose of identifying suspicious or anomalous situations. During fiscal year 2004, TSA plans to spend about $1 million for the concept development phase of the system. In proposing the system, agency officials stated that they followed TSA internal investment management processes, including linking the system's mission needs statement and its requirements with the goals and objectives specified in the National Strategy on Homeland Security and the President's

[25] Office of Homeland Security, The White House, *National Strategy for Homeland Security* (Washington, D.C.: July 2002).

[26] The agenda points out important challenges for the federal government. It is intended to focus agencies' efforts on making progress in achieving management and performance improvements.

Management Agenda. However, system initiation documents show only that TSA linked the system to TSA's draft strategic plan. The officials said that as the system acquisition progresses, they plan to follow the DHS investment management process, including the appropriate steps to ensure that the system is aligned with DHS's strategic plans and enterprise architecture.

- *Aviation Logistics Management Information System.* The Coast Guard began acquiring this system in 2001 to support aircraft operations, logistics, and maintenance. In 2002, and after about $12.3 million was invested, the system began operating; the Coast Guard reports that it spends about $5 million each year to operate and maintain it. Coast Guard officials told us that they followed internal Coast Guard capital planning and investment control guidance, along with OMB guidance, in justifying this and other IT investments as part of the annual budget cycle. Project documentation shows that system performance goals and measures have been mapped to the Coast Guard's annual performance plan and strategic plan. The Coast Guard Chief Knowledge Officer said that since the Coast Guard became a separate component agency within DHS, it has continued to monitor the system's strategic alignment using this same capital planning and investment control guidance.

In summary, these examples show that to align their ongoing system investments with DHS's evolving systems integration strategy, the component organizations have thus far relied primarily on the respective investment management approaches, strategic plans, and architectures that existed within their pre-DHS organizations, augmented by informal contacts with department-level strategic planners and architects, and consideration of the President's National Strategy on Homeland Security. However, this approach continues reliance on the components' individual IT strategies, investment processes, and architectures that produced the diverse set of systems that the department inherited when it was established. In addition, using informal communication relies too heavily on oral discussions of complex strategic contexts and frames of reference that are still being explicitly defined, thus increasing the chances of both misunderstanding and misinformed decisions.

According to the DHS CIO and officials within the three component organizations, this approach was adopted to permit the department to pursue mission need–based system capabilities while the department's strategic IT management framework was being developed. DHS officials said that as the framework is institutionalized, component agencies are beginning to use DHS processes. Nevertheless, the longer the department continues to invest in major IT systems without the completed framework and sufficient department-level CIO authority over component IT organizations' resources and spending, the greater the risk is that new and existing system investments will later require rework to be properly aligned with the framework.

Conclusions

Having a well-defined and executed departmentwide strategic IT management framework is critical to DHS's ability to effectively and efficiently integrate its components' new and existing systems. DHS's CIO recognizes this and has stated his commitment to ensuring that the framework is put in place. However, DHS-wide allocation of resources across the department has yet to reflect this criticality; huge sums are going to component IT management organizations and investments, while relatively fewer resources are being invested in the department's strategic IT framework. Moreover, DHS has yet to assign the department's CIO explicit authority over all of its IT spending. It is important that DHS strike the proper balance between component organizations' pursuit of new and enhanced systems and establishing the means for achieving its departmentwide systems environment—a homogeneous family of systems that optimally support departmentwide operations and mission performance. Steps taken thus far have yet to strike this balance, which increases the risk that today's IT system investments will have to be redone tomorrow to produce the target systems environment.

Recommendations for Executive Action

Until DHS's strategic IT management framework is completed and available to effectively guide and constrain the billions of dollars that it is spending on IT investments, we recommend that the Secretary of Homeland Security direct the heads of the department's directorates and agencies to limit spending on their respective IT investments to cost-effective efforts that

- are congressionally directed;
- take advantage of near-term, relatively small, low-risk opportunities to leverage technology in satisfying a compelling homeland security need;
- support operations and maintenance of existing systems critical to DHS's mission;

- involve deploying an already developed and fully tested system; or
- support establishment of a DHS strategic IT management framework, including IT strategic planning, enterprise architecture, and investment management.

We also recommend that in determining the cost-effectiveness of these IT investments, the Secretary direct the heads of DHS's directorates and agencies to ensure that full consideration be given to the estimated cost of any future system rework that would be needed to later align the system with the department's emerging systems integration strategy.

Further, we recommend 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.

Agency Comments and Our Evaluation

In written comments on a draft of this report, which are reprinted in appendix III, the DHS Assistant Secretary for Legislative Affairs did not agree or disagree with our findings, conclusions, or recommendations. Rather, the Assistant Secretary described DHS's IT challenges and priorities, and provided documentation on them, including efforts to achieve its priorities. Specifically, the Assistant Secretary stated that three major IT challenges face DHS: ensuring that homeland security employees have system-enabled solutions and tools to safeguard our country, integrating existing IT systems within the context of the department's enterprise architecture, and identifying and eliminating IT system overlap and redundancy while not hampering ongoing mission activities. In addition, the Assistant Secretary (1) identified eight departmentwide priorities (e.g., IT portfolio management, enterprise architecture, and information sharing) that the DHS and component CIOs have set and (2) described efforts under way to develop business cases and other plans needed to address the eight. The information conveyed in DHS's comments is consistent with information obtained during the course of our review that showed progress and plans for institutionalizing the department's strategic IT management framework.

We will send copies of this report to the Secretary of Homeland Security, and the Director, OMB. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov. If you have any questions on matters discussed in this report, please contact me at (202) 512-3439 or at hiter@gao.gov. Key contributors to this report are listed in appendix IV.

Sincerely yours,

Randolph C. Hite

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

Appendix I

Scope and Methodology

To evaluate whether the Department of Homeland Security (DHS) has defined a systems integration strategy, we requested and reviewed relevant plans and documents from the department, including policies, procedures, guidance, and other business and information technology (IT) strategic documents. Because these documents were being developed, we did not evaluate their quality or completeness. We also interviewed DHS officials, including the Chief Information Officer (CIO) and other department and selected component agency officials responsible for strategic planning to, among other things, identify the status of their efforts to develop an IT strategic plan, to refine its capital planning and investment control process, and to develop an enterprise architecture.

To determine how DHS is ensuring that component agency IT investments are aligned with the department's strategic direction, we reviewed department investment management policies and procedures and other associated documents. We also interviewed DHS's CIO and other department officials responsible for IT planning and investment management, including strategic investment alignment. As requested, we focused on three DHS components agencies: the Federal Emergency Management Agency (FEMA), the Transportation Security Administration (TSA), and the U.S. Coast Guard. We requested that each of these components provide a representative example of an IT system investment that best demonstrated the interim steps that it was taking to align system investments with DHS's evolving strategic IT management framework. The examples provided were FEMA's Grant Business Management System, TSA's Integrated Intermodal Information System, and the Coast Guard's Aviation Logistics Management Information System. We reviewed available documentation for the examples to determine how each component is ensuring that investments are aligned with DHS's strategic direction. We also interviewed FEMA, TSA, and Coast Guard officials as necessary to understand the steps they had taken to strategically align these investments.

We performed our work at DHS and component agency facilities in the Washington, D.C., area from September 2003 through March 2004, in accordance with generally accepted government auditing standards.

Appendix II

Strategic Information Technology Management Framework Components

The tenets of a strategic information technology (IT) management framework are described in our prior research on best practices in private-sector firms and government organizations[1] and are called for in federal management laws and guidance, such as the Clinger-Cohen Act[2] and Office of Management and Budget (OMB) Circular No. A-130.[3] Three key components of such a framework are an IT strategic plan, an IT investment management process, and an enterprise architecture.

An IT strategic 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. The strategic plan should be tied to and support the agency strategic plan and provide for establishing and implementing IT management processes. Among other things, the plan should describe the management processes required for the IT function to execute its roles and responsibilities, thereby facilitating achievement of agency missions.

An IT investment management process provides a systematic method for agencies to minimize risks while maximizing return on investment. A central element of the federal approach to investment management has been the select/control/evaluate model. This model was initially identified in our Strategic Information Management Executive Guide,[4] expanded in OMB's investment guidance,[5] and then refined in our subsequent guidance.[6]

[1] We have issued guidance to agencies related to enterprise architecture, IT investment management, and other management issues. For example, see U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO-03-584G (Washington, D.C.: April, 2003) and *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Version 1.1)*, GAO-04-394G (Washington, D.C.: March 2004).

[2] Clinger-Cohen Act, 40 U.S.C. 11101–11703.

[3] Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130.

[4] U.S. General Accounting Office, *Executive Guide: Improving Mission Performance through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1994).

[5] Executive Office of the President, Office of Management and Budget, *Evaluating Information Technology Investments*, *A Practical Guide* (Washington, D.C.: November 1995).

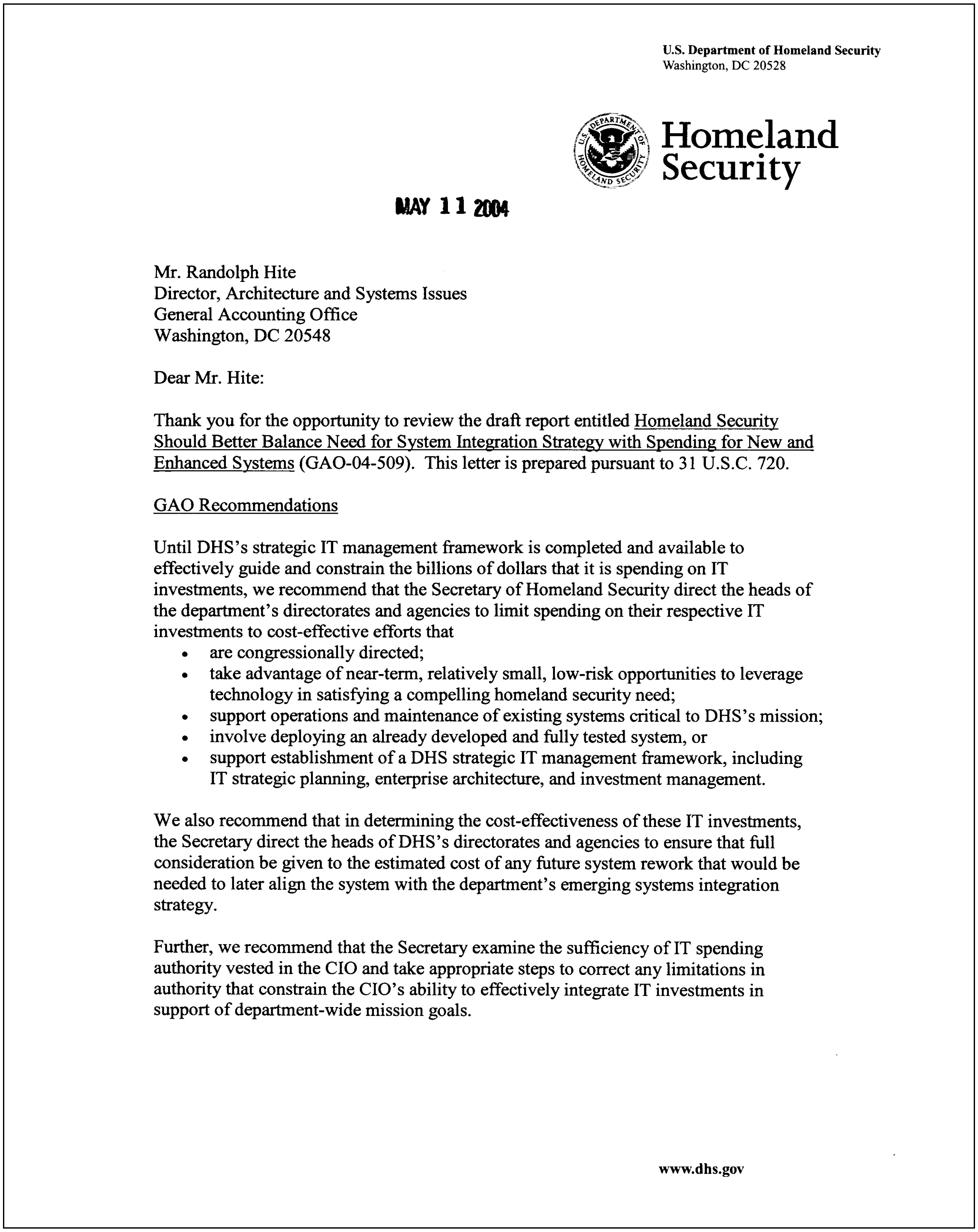
[6] GAO-04-394G.

During the select phase, the organization (1) identifies and analyzes each project's risks and returns before committing significant funds to any project and (2) selects those projects that will best support its mission needs. During the control phase, the organization ensures that, as projects develop and investment expenditures continue, the project continues to meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems have arisen, steps are quickly taken to address the deficiencies. If mission needs have changed, the organization is able to adjust its objectives for the project and appropriately modify expected project outcomes. During the evaluate phase, actual versus expected results are compared after a project has been fully implemented. This is done to (1) assess the project's impact on mission performance, (2) identify any changes or modifications to the project that may be needed, and (3) revise the investment management process based on lessons learned.

As discussed in our framework for assessing and improving enterprise architecture management,[7] an enterprise architecture provides a clear and comprehensive picture of the structure of an entity, whether an organization or a functional or mission area. It is an essential tool for effectively and efficiently engineering business processes and for implementing and evolving supporting systems. More specifically, enterprise architectures are systematically derived and captured blueprints or descriptions—in useful models, diagrams, and narrative—of the mode of operation for a given enterprise. This mode of operation is described in both (1) logical terms, such as interrelated business processes and business rules, information needs and flows, data models, work locations, and users, and (2) technical terms, such as hardware, software, data, communications, security attributes, and performance standards. They provide these perspectives both for the enterprise's current, or "as is," environment and for its target, or "to be," environment, as well as a transition plan for moving from the "as is" to the "to be" environment.

[7] GAO-03-584G.

Comments from the Department of Homeland Security



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

Homeland
Security

MAY 11 2004

Mr. Randolph Hite
Director, Architecture and Systems Issues
General Accounting Office
Washington, DC 20548

Dear Mr. Hite:

Thank you for the opportunity to review the draft report entitled Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems (GAO-04-509). This letter is prepared pursuant to 31 U.S.C. 720.

GAO Recommendations

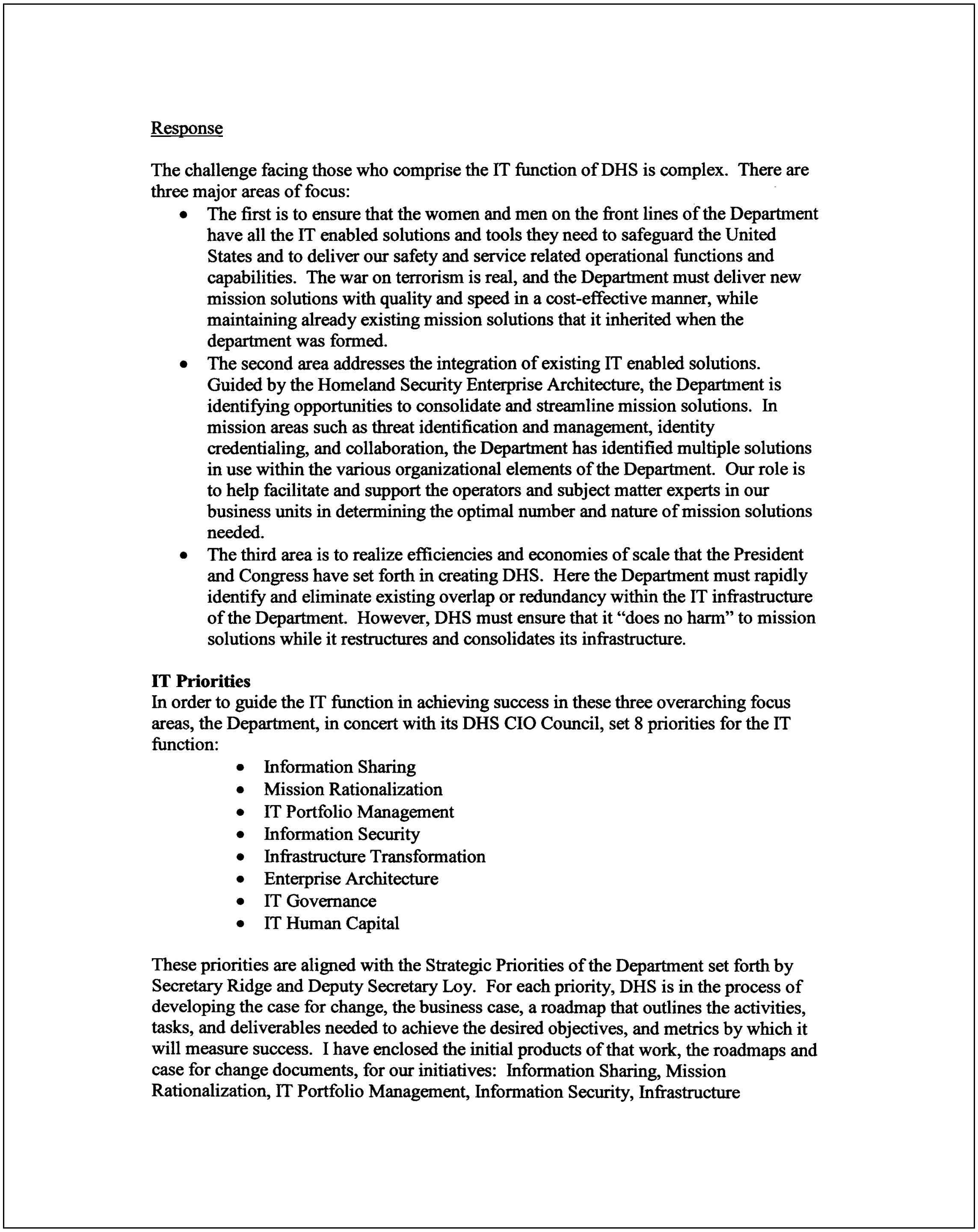
Until DHS's strategic IT management framework is completed and available to effectively guide and constrain the billions of dollars that it is spending on IT investments, we recommend that the Secretary of Homeland Security direct the heads of the department's directorates and agencies to limit spending on their respective IT investments to cost-effective efforts that

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

We also recommend that in determining the cost-effectiveness of these IT investments, the Secretary direct the heads of DHS's directorates and agencies to ensure that full consideration be given to the estimated cost of any future system rework that would be needed to later align the system with the department's emerging systems integration strategy.

Further, we recommend 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 department-wide mission goals.

www.dhs.gov



Response

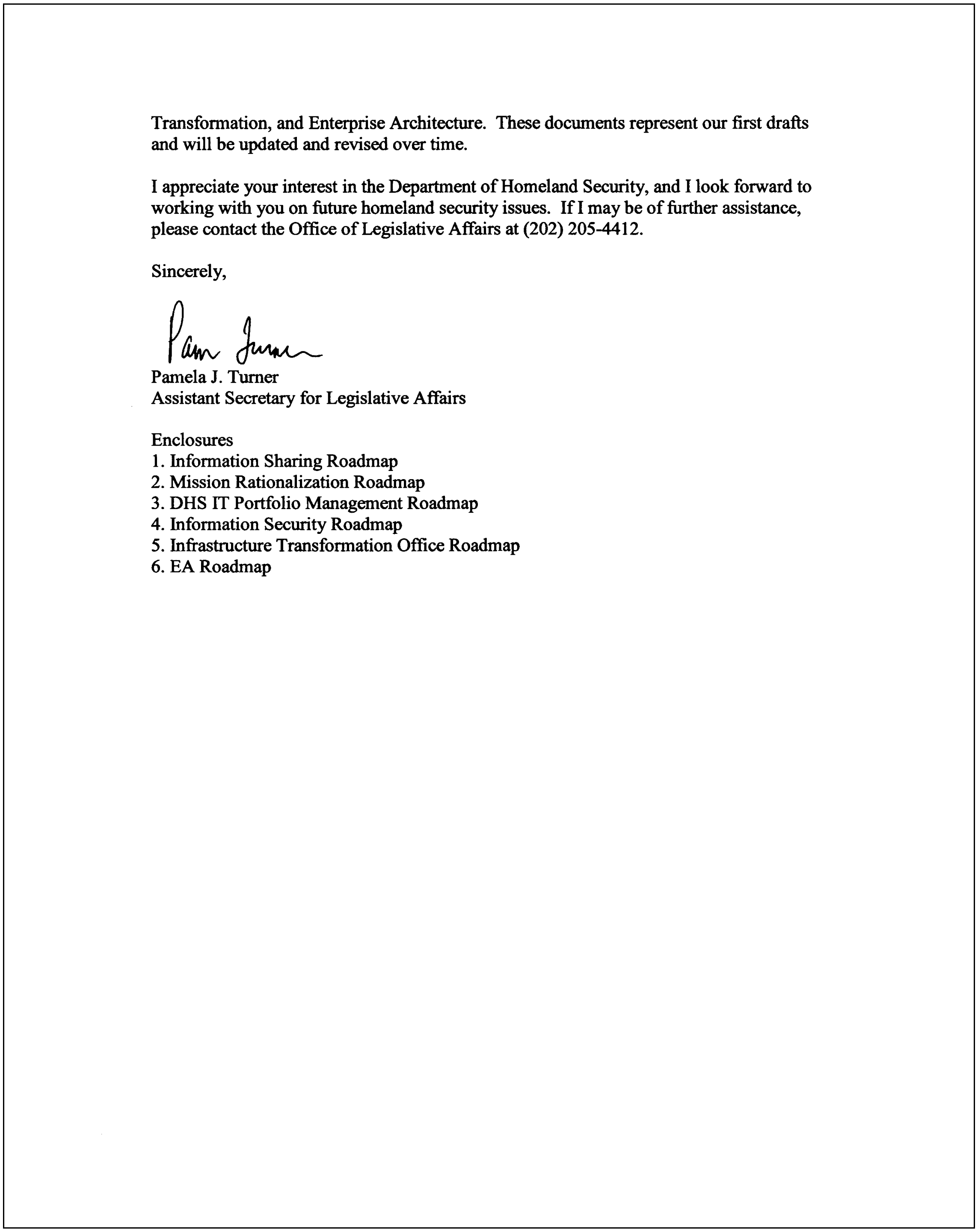
The challenge facing those who comprise the IT function of DHS is complex. There are three major areas of focus:

- The first is to ensure that the women and men on the front lines of the Department have all the IT enabled solutions and tools they need to safeguard the United States and to deliver our safety and service related operational functions and capabilities. The war on terrorism is real, and the Department must deliver new mission solutions with quality and speed in a cost-effective manner, while maintaining already existing mission solutions that it inherited when the department was formed.
- The second area addresses the integration of existing IT enabled solutions. Guided by the Homeland Security Enterprise Architecture, the Department is identifying opportunities to consolidate and streamline mission solutions. In mission areas such as threat identification and management, identity credentialing, and collaboration, the Department has identified multiple solutions in use within the various organizational elements of the Department. Our role is to help facilitate and support the operators and subject matter experts in our business units in determining the optimal number and nature of mission solutions needed.
- The third area is to realize efficiencies and economies of scale that the President and Congress have set forth in creating DHS. Here the Department must rapidly identify and eliminate existing overlap or redundancy within the IT infrastructure of the Department. However, DHS must ensure that it "does no harm" to mission solutions while it restructures and consolidates its infrastructure.

IT Priorities
In order to guide the IT function in achieving success in these three overarching focus areas, the Department, in concert with its DHS CIO Council, set 8 priorities for the IT function:

- Information Sharing
- Mission Rationalization
- IT Portfolio Management
- Information Security
- Infrastructure Transformation
- Enterprise Architecture
- IT Governance
- IT Human Capital

These priorities are aligned with the Strategic Priorities of the Department set forth by Secretary Ridge and Deputy Secretary Loy. For each priority, DHS is in the process of developing the case for change, the business case, a roadmap that outlines the activities, tasks, and deliverables needed to achieve the desired objectives, and metrics by which it will measure success. I have enclosed the initial products of that work, the roadmaps and case for change documents, for our initiatives: Information Sharing, Mission Rationalization, IT Portfolio Management, Information Security, Infrastructure



Transformation, and Enterprise Architecture. These documents represent our first drafts and will be updated and revised over time.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

Pam Turner

Pamela J. Turner
Assistant Secretary for Legislative Affairs

Enclosures
1. Information Sharing Roadmap
2. Mission Rationalization Roadmap
3. DHS IT Portfolio Management Roadmap
4. Information Security Roadmap
5. Infrastructure Transformation Office Roadmap
6. EA Roadmap

Appendix IV

GAO Contact and Staff Acknowledgments

GAO Contact

Gary Mountjoy, (202) 512-6367

Acknowledgments

Barbara Collier, Vijay D'Souza, and Carl Urie made key contributions to this report.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

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

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

[redacted]