United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Government Management, Organization, and Procurement, House Committee on Oversight and Government Reform

For Release on Delivery
Expected at 9:30 a.m. EDT
Tuesday, September 15, 2009

HOMELAND SECURITY

Despite Progress, DHS Continues to Be Challenged in Managing Its Multi-Billion Dollar Annual Investment in Large-Scale Information Technology Systems

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

September 15, 2009

GAO
Accountability • Integrity • Reliability
Highlights

Highlights of GAO-09-1002T, a testimony before congressional requesters

HOMELAND SECURITY

Despite Progress, DHS Continues to Be Challenged in Managing Its Multi-Billion Dollar Annual Investment in Large-Scale Information Technology Systems

Why GAO Did This Study

The Department of Homeland Security (DHS) invests more than $6 billion annually in large-scale, information technology (IT) systems to help it achieve mission outcomes and transform departmentwide operations. For DHS to effectively leverage these systems as mission enablers and transformation tools, it needs to employ a number of institutional acquisition and IT management controls and capabilities, such as using an operational and technological blueprint to guide and constrain system investments (enterprise architecture) and following institutional policies, practices, and structures for acquiring and investing in these systems. Other institutional controls and capabilities include employing rigorous and disciplined system life cycle management processes and having capable acquisition and IT management workforces. As GAO has reported, it is critical for the department to implement these controls and capabilities on each of its system acquisition programs.

GAO has issued a series of reports on DHS institutional controls for acquiring and managing IT systems, and its implementation of these controls on large-scale systems. GAO was asked to testify on how far the department has come on both of these fronts, including its implementation of GAO's recommendations. To do this, GAO drew from its issued reports on institutional IT controls and IT systems, as well as our recurring work to follow up on the status of our open recommendations.

View GAO-09-1002T or key components. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov

What GAO Found

Since its inception, DHS has made uneven progress in its efforts to institutionalize a framework of interrelated management controls and capabilities associated with effectively and efficiently acquiring large-scale IT systems. To its credit, it has continued to issue annual updates to its enterprise architecture that have added previously missing scope and depth, and further improvements are planned to incorporate the level of content, referred to as segment architectures, needed to effectively introduce new systems and modify existing ones. Also, it has redefined its acquisition and investment management policies, practices, and structures, including establishing a system life cycle management methodology, and it has increased its acquisition workforce.

Nevertheless, challenges remain relative to, for example, implementing the department's plan for strengthening its IT human capital, and fully defining key system investment and acquisition management policies and procedures. Moreover, the extent to which DHS has actually implemented these investment and acquisition management policies and practices on major programs has been at best inconsistent, and in many cases, quite limited. For example, recent reviews by GAO show that major acquisition programs have not been subjected to executive level acquisition and investment management reviews at key milestones and have not, among other things, employed reliable cost and schedule estimating practices, effective requirements development and test management practices, meaningful performance measurement, strategic workforce management, proactive identification and mitigation of program risks, and effective contract tracking and oversight, among other things.

Because of these weaknesses, major IT programs aimed at delivering important mission capabilities have not lived up to expectations. For example, full deployment of the Rescue 21 "search and rescue" system had to be extended from 2006 to 2017; development and deployment of an "exit" capability under the US-VISIT program has yet to occur; and the timing and scope of an SBInet "virtual border fence" initial operating capability has been delayed and reduced from the entire southwest border to 28 miles of the border.

To assist the department in addressing its institutional and system-specific challenges, GAO has made a range of recommendations. While DHS and its components have acted on many of these recommendations, and as a result have arguably made progress and improved the prospects for success on ongoing and future programs, more needs to be done by DHS's new leadership team before the department can ensure that all system acquisitions are managed with the rigor and discipline needed to consistently deliver promised capabilities and benefits on time and on budget.

Madame Chairwoman and Members of the Subcommittee

I appreciate the opportunity to participate in today's hearing on the Department of Homeland Security's (DHS) efforts to manage its sizeable investment in large-scale information technology (IT) programs, such as the Secure Border Initiative Network (SBI*net*) and the U.S. Visitor and Immigrant Status Indicator Technology Program (US-VISIT). As you know, many of these programs are at the heart of DHS's quest to transform the 22 diverse and distinct agencies that it inherited into a single, integrated, high-performing department. In light of the importance of the department's mission, and the significance of the challenges facing it, in 2003 we designated the implementation of the department and its transformation as a high-risk undertaking, and we continue to do so today.[1]

For DHS to effectively manage the billions of dollars that it invests each year in IT, we reported in 2004[2] that it needed to put in place key institutional IT management controls, such as employing a departmentwide operational and technological blueprint to guide and constrain its acquisitions (enterprise architecture), and following institutional policies, practices, and structures for acquiring and investing in these programs. Other institutional controls and capabilities include employing rigorous and disciplined system life cycle management processes and having capable acquisition and IT workforces.

My testimony today addresses the evolving state of DHS's efforts to establish these institutional IT management controls and capabilities and implement them on large-scale IT acquisition programs. In preparing this testimony, we drew extensively from our previous work on DHS's efforts to institutionalize key

[1] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003); GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005); GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007); and GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

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

acquisition and IT management controls and capabilities and their application on large-scale IT acquisition programs, as well as our recurring work to follow up on the status of our open recommendations. Among other things, this follow up work included reviewing recently issued DHS acquisition management directives and related guidance, such as its recently issued system enterprise life cycle methodology, as well as the most recent version of the DHS enterprise architecture, in relation to relevant federal guidance.[3] In addition, it included documentation and interviews with key department and component agency officials associated with each of the management controls. We also discussed the updated information included in this statement with department and component agency officials. All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Background

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

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

[3] See, for example, OMB, Federal Segment Architecture Methodology, January 2009, and GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

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

As we reported before the department was created,[5] such a transformation is critically important and poses significant management and leadership challenges. For these reasons, we designated the implementation of the department and its transformation as high-risk in 2003, and we continue to do so today. In this regard, we have stated that failure to effectively address DHS's management challenges and program risks could have serious consequences for our national security.

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

DHS Components and IT Spending

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

[5] For example, see GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003) *and Homeland Security: Proposal for Cabinet Agency Has Merit, but Implementation Will be Pivotal to Success*, GAO-02-886T (Washington, D.C.: June 25, 2002).

Figure 1: DHS Organizational Structure

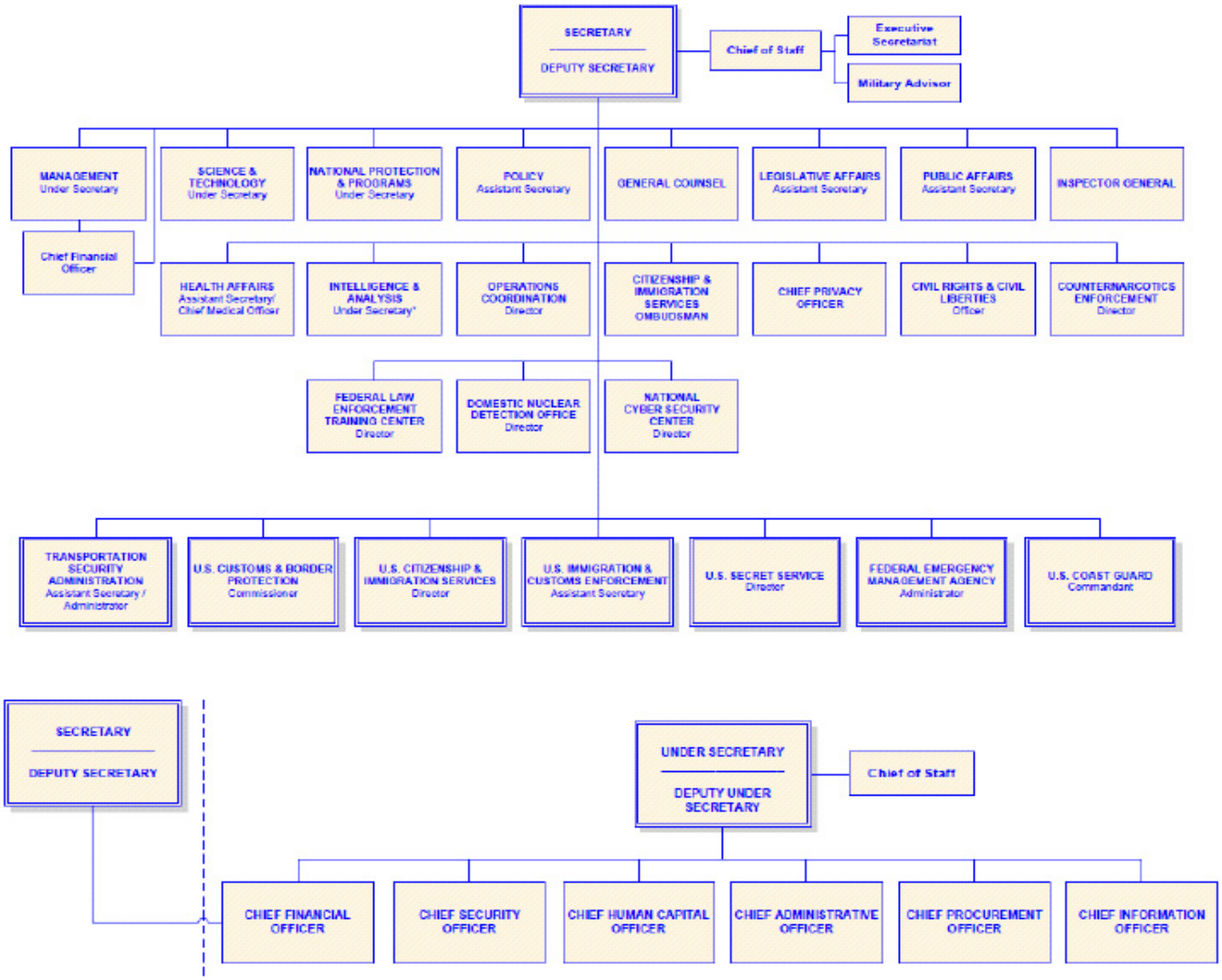


Table 1: DHS' Principal Component Organizations and their Missions

Principal Organizations[a]	Missions
Citizenship and Immigration Services	Administers immigration and naturalization adjudication functions and establishes immigration services policies and priorities
Coast Guard	Protects the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, and in any maritime region as required to support national security.
Customs and Border Protection	Protects the nation's borders to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.
Domestic Nuclear Detection Office	Protects the nation by detecting and reporting unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the nation.
Federal Emergency Management Agency	Prepares the nation for hazards, manages federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.
Health Affairs	Protects the nation against biohazards through coordinated efforts with all levels of government and the private sector to develop and support a scientifically rigorous, intelligence-based biodefense and health preparedness architecture.
Immigration and Customs Enforcement	Protects the nation's borders by identifying and shutting down vulnerabilities in the nation's border, economic, transportation, and infrastructure security.
Intelligence and Analysis	Works closely with DHS components, as well as state, local, and tribal entities, to fuse non-traditional and traditional intelligence information streams into national threat assessments, and disseminates the resulting information to DHS and external homeland security customers.
Management Directorate	Oversees department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, IT, facilities and equipment, and identifies and tracks performance measurements.
National Protection and Programs Directorate	Works with state, local, and private sector partners to identify threats, determine vulnerabilities, and target resources where risk is greatest to safeguard the nation's critical physical and cyber infrastructures.
Secret Service	Protects the President and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure.
Transportation Security Administration	Protects the nation's transportation systems to ensure freedom of movement for people and commerce

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

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

Within the Management Directorate is the Office of the Chief Information Officer (CIO). Among other things, this office is to leverage best available technologies and IT management practices, provide shared services, coordinate acquisition strategies, maintain an enterprise architecture that is fully integrated with other management processes, and advocate and enable business transformation. Other DHS entities also are responsible or share

responsibility for IT management activities. For example, DHS's major organizational components (e.g., directorates, offices, and agencies) have their own CIOs and IT organizations. Under this structure, control over the department's IT management functions is shared by the DHS CIO and the component CIOs.

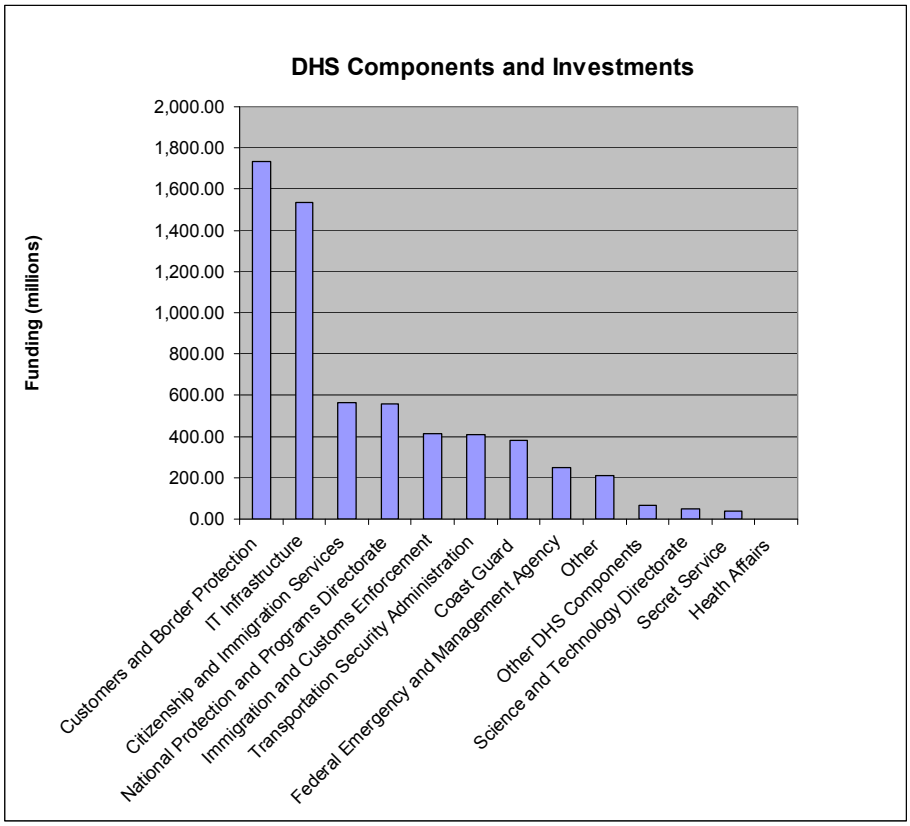
Also within the Management Directorate is the Office of the Chief Procurement Officer (CPO). The CPO is the department's senior procurement executive who has leadership and authority over DHS acquisition and contracting, including major investments. This office's responsibilities include issuing policies and implementing instructions, overseeing acquisition and contracting functions, and ensuring that a given acquisition's contracting strategy and plans align with the intent of the Acquisition Review Board, DHS's highest investment review board. Similar to the department and component CIOs, DHS relies on a structure of dual accountability and collaboration between the CPO and the heads of DHS components to carry out the acquisition function.

To promote coordination across DHS component boundaries, the DHS CIO and CPO have each established management councils. For example, the DHS CIO established the department's CIO council, which is chaired by the DHS CIO and composed of component-level CIOs. According to its charter, the specific functions of the council include establishing a strategic plan, setting priorities for departmentwide IT, identifying opportunities for sharing resources, coordinating multi-bureau projects and programs, and consolidating activities.

To accomplish their respective missions, DHS and its component agencies rely on and invest heavily in IT systems and supporting infrastructure. For example, in fiscal year 2009, DHS IT-related funding totaled about $6.2 billion. Of DHS's principal component organizations, Customs and Border Protection (CBP) represents the largest IT investor (about $1.7 billion or 28 percent). The next largest single investment in IT transcends DHS organizations and is for DHS-wide IT infrastructure ($1.5 billion), which includes, among other things, development of a replacement for the system used to share homeland security information with its federal, state, and local partners. The U.S. Citizenship and Immigration Services and

the National Protection and Programs Directorate are the next largest investors in IT ($561 and $556 million, respectively). See figure 2 for more information on DHS components and their fiscal year 2009 funding.

Figure 2: DHS Components and Their Fiscal Year 2009 IT Funding



Source: DHS

According to DHS, the $6.2 billion in funding supports 279 major IT acquisition programs. Examples of these programs are described below.

- **Automated Commercial Environment (ACE):** ACE is a CBP program that was begun in 2001 to modernize trade processing and support border security by, among other things, fully automating commercial import and export data processing and

facilitating information sharing among federal agencies with a trade-related mission. ACE capabilities are being delivered in a series of increments, and thus far operational capabilities include screening cargo and conveyances, analyzing data to support targeting of high-risk entities, and processing truck manifests electronically. Future increments are to provide additional screening and combined manifest processing across all types of transportation. Through fiscal year 2009, DHS has been appropriated about $2.7 billion for ACE, and for fiscal year 2010, the department has requested about $268 million.

- **United States Visitor and Immigrant Status Indicator Technology (US-VISIT):** This program dates to 2002 and is within the National Protection and Programs Directorate. It is to enhance the security of our citizens and visitors, ensure the integrity of the U.S. immigration system, protect privacy, and facilitate legitimate trade and travel. The program is to achieve these goals by, among other things, (1) collecting, maintaining, and sharing information on certain foreign nationals who enter and exit the United States; (2) identifying foreign nationals who have overstayed or violated the terms of their visit or who can receive, extend, or adjust their immigration status; (3) detecting fraudulent travel documents, verifying visitor identity, and determining visitor admissibility through the use of biometrics (digital fingerprints and a digital photograph); and (4) facilitating information sharing and coordination within the immigration and border management community.

  DHS has delivered US-VISIT capabilities in a series of increments. As a result, a biometrically enabled entry capability has been operating at about 300 air, sea, and land POEs since December 2006 (115 airports, 14 seaports, and 154 of 170 land ports).[6] Since 2004, DHS has evaluated a number of biometric exit solutions, and several exit pilot evaluations are currently

[6]According to program officials, 14 of the remaining 16 POEs have no operational need to deploy US-VISIT because visitors subject to US-VISIT are, by regulation, not authorized to enter into the United States at these locations. The other two POEs do not have the necessary transmission lines to operate US-VISIT, and thus they process visitors manually.

underway. However, an exit capability is not yet operational. Through fiscal year 2009, DHS had been appropriated about $2.5 billion for US-VISIT, and for fiscal year 2010, the department has requested about $356 million.

- **Rescue 21:** This is a Coast Guard program to modernize a 30-year-old search and rescue communications system used for missions 20 miles or less from shore, referred to as the National Distress and Response System. Among other things, it is to increase communications coverage area, allow electronic tracking of department vessels and other mobile assets, and enable secure communication with other federal and state entities. As of June 2009, Rescue 21's initial operating capability has been deployed and accepted at 23 of 42 regions. Additional system capability (e.g., the ability to track vessels) remains to be developed, as does a system to meet the unique needs of the Alaska region. Through fiscal year 2009, DHS has been appropriated about $723 million for Rescue 21, and for fiscal year 2010, the department has requested about $117 million.

- **Secure Flight**: This is a Transportation Security Administration (TSA) program to allow the federal government to assume from airlines the responsibility of prescreening passengers for domestic flights by matching of passenger biographic information against watch lists. Among other things, Secure Flight is to prevent people suspected of posing a threat to aviation from boarding commercial aircraft in the United States, protect passengers' privacy and civil liberties, and reduce the number of people unnecessarily selected for secondary screening. TSA is currently in the process of phasing in its use of Secure Flight for domestic flights. Through fiscal year 2009, DHS has been appropriated about $326 million for Secure Flight, and for fiscal year 2010, the department has requested about $84.4 million.

- **SBI*net***: SBI*net* is the technology component of a CBP program known as SBI, which is to help secure the nation's borders and reduce illegal immigration through physical infrastructure (e.g., fencing), surveillance systems, and command, control, communications, and intelligence technologies. As of 2009, a

pilot of SBI*net* capabilities referred to as Project 28 has been deployed and is currently operating along 28 miles of the southwest border in Tucson, Arizona. Through fiscal year 2009, DHS has been appropriated about $3.6 billion for SBI, and for fiscal year 2010, the department has requested about $779 million.

DHS Has Made Uneven Progress in Establishing Institutional Management Controls and Capabilities for Large-Scale IT Acquisitions

The department has continued to work to establish effective corporate IT and acquisition management controls and capabilities, but progress across these disciplines has been uneven, and more remains to be done. Until DHS fully institutionalizes these controls and capabilities, it will be challenged in its ability to effectively and efficiently acquire large-scale IT systems and thereby leverage technology to support transformation and achieve mission goals and results.

Enterprise Architecture Continues to Evolve, But Key Content Still Missing

Leading organizations recognize the importance of having and using an enterprise architecture (EA)—a corporate blueprint that describes—in useful models, diagrams, tables, and narrative—how a given entity operates today and how it plans to operate in the future, and provides a road map for transitioning from today to tomorrow. Our experience with federal agencies has shown that attempting to acquire systems without an EA often results in investments that are duplicative, not well integrated, unnecessarily costly to maintain, and limited in terms of optimizing mission performance.[7]

[7] See for example, GAO, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458 (Washington, D.C.: Feb. 28, 2003).

Since 2003, DHS has issued annual updates to its EA that have improved on prior versions by adding previously missing content.[8] Specifically, we reported in November 2003[9] that DHS's initial version of its EA was not sufficiently mature to guide and constrain investments. For example, while the department had established the management foundation for developing, maintaining, and implementing its EA and had issued an initial version of its target architecture, it had yet to develop products that fully described its current and target architectural environments, as well as a plan for transitioning from the current to the target environment.

In August 2004, we reported that the initial version of the department's architecture provided a useful foundation on which to build a more complete architecture, but that it was still missing important content that limited its utility.[10] For example, the content of this version was not systematically derived from a DHS or national corporate business strategy; rather it was an amalgamation of the existing architectures of the DHS predecessor agencies, along with their portfolios of systems investment projects. To assist DHS in evolving its architecture, we made 41 recommendations aimed at adding needed content.

In May 2007, we reported[11] on the third version of DHS's EA, concluding that while this version partially addressed each of our prior recommendations, it did not fully address them, and thus important content was still missing. Further, we reported that DHS organizational components were not adequately involved in its development. Accordingly, we made additional recommendations.

[8] The Homeland Security EA version 1.0 was issued in September 2003 and version 2.0 was issued in October 2004. The next version, HLS EA 2006, was issued in June 2006, followed by HLS EA 2007 in March 2007, HLS EA 2008 in February 2008, and the HLS EA 2009 in June 2009. .

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

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

[11] GAO, *Homeland Security: DHS Enterprise Architecture Continues to Evolve, but Improvements Needed*, GAO-07-564 (Washington, D.C.: May 9, 2007).

To the department's credit, recent versions of its EA largely address our prior recommendations aimed at adding needed architectural depth and breadth. For example, in response to our prior recommendation that the architecture include a technical reference model (TRM) that describes, among other things, the technical standards to be implemented for each enterprise service, the 2008 version of the EA included a TRM that identified such standards. It also adopted an approach for extending the architecture through segments, which is a "divide and conquer" approach to architecture development advocated by OMB. To implement this approach, OMB guidance[12] states that agencies should define and prioritize enterprise segments,[13] focusing first on those segments that will help it perform its mission most effectively, and that they should first focus on developing architectures for high priority segments. However, while the 2008 EA identified 22 segments, it did not prioritize the segments.

DHS recently issued the latest version of its EA, and this version continues to improve on the prior version. For example, it contains a revised DHS business model that decomposes functional areas into business functions, describes information exchanges that support information sharing across organizational boundaries, and provides updated information security profiles for existing systems. It also updates the transition strategy for migrating to the target architecture by including planned 2010 investments. However, this version still does not contain prioritized segments and does not include OMB required architecture information for each segment (e.g., information exchanges between the critical business processes, conceptual solution architecture for each segment). Instead, the EA states that future versions will include revised segmented architectures within the context of its newly developed

[12] OMB, Federal Segment Architecture Technology, January 2009, OMB, *Improving Agency Performance Using Information and Information Technology* (Enterprise Architecture Assessment Framework 3.0), December 2008; OMB, *Federal Enterprise Architecture Practice Guidance*, November 2007.

[13] OMB guidance identifies three segment types: core mission areas (e.g., screening/watch lists), business services (e.g., financial management), or enterprise services (e.g., information sharing).

functional areas. As we have previously reported[14], segment architectures serve as a bridge between the corporate frame of reference captured in the EA and each individual system investment. Without well-defined segment architectures, DHS does not have a sufficient basis for investing in IT programs in a manner to ensure that they investments are properly sequenced, well integrated, and not duplicative.

IT Acquisition and Investment Management Improvements Made, But More Needs to be Done

Through effective corporate acquisition and investment management, organizations can make informed decisions when selecting among competing investment options and when controlling them throughout their acquisition life cycles. Based on our research, we issued an IT investment management framework[15] that encompasses, among other things, best practices of successful public and private sector organizations relative to selecting and controlling individual investments as well as portfolios (segments) of investments. During the select phase, organizations are to (1) identify and analyze program/project risks and value before committing significant funds and (2) select those that will best support its mission needs. In the control phase, they are to ensure that programs/projects are meeting cost, schedule, and performance expectations at key milestone events, and that actions are taken to address deviations.

Since 2003, DHS has attempted to define and implement a corporate approach to overseeing its acquisition of major system investments, and we have continued to report limitations in its efforts to do so. Specifically, in August 2004, we reported[16] that DHS had established

[14] GAO, *Information Technology: HUD Needs to Strengthen its Capacity to Manage and Modernize its Environment*, GAO-09-675 (Washington, D.C.: July 31, 2009).

[15] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

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

an investment management process that provided for departmental oversight of major IT programs at key milestones, but that most programs (about 75 percent) had not undergone defined milestone reviews in a timely manner. At that time, DHS attributed this to the newness of the process. Based on our findings, we made recommendations aimed at strengthening the process.

In March 2005,[17] we again reported on the department's acquisition and investment review process, noting that while it incorporated some best practices and provided for senior management having information required to make well-informed investment decisions at key points in the acquisition life cycle, the process did not require senior management attention and oversight at all key decision points. For example, management reviews were not required prior to investment in a prototype or prior to passing a key acquisition milestone. Accordingly, we made further recommendations to improve the process.

In April 2007,[18] we assessed DHS's investment management structures, policies, and procedures against our ITIM framework, and concluded that while DHS had established investment decisionmaking bodies (e.g., investment review board) to oversee its IT investments, it had yet to fully define 8 of 11 key policies and procedures associated with selecting investments and controlling their acquisition. For example, procedures for selecting among competing investment options did not cite either the specific criteria or the steps for prioritizing and selecting investments at either the individual program level or the portfolio of programs level. In addition, the department had yet to document a methodology, with explicit criteria, for determining a given investment's alignment to the EA. Instead, it relied on the undocumented and subjective determinations of individuals. We also reported that DHS had not fully implemented the key practices needed to control programs and

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

[18] GAO, *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments*, GAO-07-424 (Washington, D.C.: Apr. 27, 2007).

portfolios of programs. For example, DHS investment review boards were not conducting regular investment reviews, and while program-specific control activities were sometimes performed, they were not performed consistently and thoroughly across investments.. Accordingly, we made recommendations aimed at establishing and implementing mature investment management processes.

In November 2008, we again reported that DHS was not effectively implementing its acquisition and investment review process.[19] Specifically, while DHS's review process called for its decision-making bodies to review investments at key points in their life cycles—including program authorization—45 of the 48 major investments that we examined were not reviewed in accordance with this process. In addition, DHS was unable to enforce decisions made by these investment bodies because it did not track whether its component organizations took actions called for in the decisions. Further, many of these major investments lacked basic acquisition documents necessary to inform the investment review process, such as program baselines; and two of nine components—which managed a total of 8 major investments—did not have required component-level investment management processes in place. Moreover, almost a third of the 48 major investments received funding without having validated mission needs and requirements, and two-thirds did not have life cycle cost estimates. Finally, DHS had not conducted regular reviews of its investment portfolios to ensure effective performance and minimize unintended duplication of effort. We concluded that without validated requirements, life cycle cost estimates, and regular portfolio reviews, DHS could not ensure that its investment decisions were appropriate and would ultimately address capability gaps. To address these weaknesses, we made a number of recommendations.

To strengthen its institutional approach to acquisition and IT investment management, DHS established the Acquisition Program Management Division (APMD) within the Office of the CPO, and

[19] GAO, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, GAO-09-29 (Washington, D.C.: Nov. 18, 2008).

assigned it responsibility for developing and maintaining the department's acquisition policy and providing support and assistance to the department's acquisition workforce. To that end, DHS issued a new departmental directive[20] and related guidance in November 2008,[21] which together provide the framework for departmental management, support, review, and approval of programs, including IT acquisitions.

The directive established a revised acquisition review process, including roles and responsibilities of DHS approving authorities, threshold levels for acquisitions, and acquisition decision events and the corresponding documentation required. Specifically, it established the Acquisition Review Board as the department's highest review body and charged it with reviewing and approving all programs at key milestone decision points that are above $300 million in life cycle costs. It also described working groups and other boards, such as the Enterprise Architecture Board, and Program Review Board, to provide subject matter expertise to the Acquisition Review Board and DHS executives, and to review and approve investments that meet lower dollar thresholds. Recently established, according to a DHS official, was the DHS Asset Board (to provide lead technical authority on acquisition of real property and acquisition of vehicles). Finally, it is establishing the Joint Requirements Council (to validate the results of the strategic requirements planning process).

DHS has also reinstated regular acquisition review board meetings and acquisition decision memorandums. Specifically, DHS's acquisition review board reports that it completed 14 acquisition reviews in 2008, and has thus far completed 18 reviews in 2009, including reviews of SBI*net*, US-VISIT, and Secure Flight. DHS also reports that 7 additional reviews are scheduled to occur by the end of the fiscal year. In addition, DHS components have designated Component Acquisition Executives (CAEs) to serve as the senior

[20] Department of Homeland Security, *Acquisition Directive 102-01*, Interim Version 1.9, November 7, 2008

[21] Department of Homeland Security, *Acquisition Instruction/Guidebook 102-01-01*, Interim Version 1.9, November 7, 2008

acquisition officials within the components and to be responsible for implementation of management and oversight of all component acquisition processes. DHS has also begun to make use of a new system to track program cost, schedule, and performance information, as well as action items that result from acquisition oversight board decisions. To support acquisition oversight, the CPO has identified a need for 58 additional positions. As an initial step, DHS's fiscal year 2010 budget request included 10 additional full time equivalent positions for acquisition oversight support.

Notwithstanding these actions, the department's acquisition and investment management processes still do not meet some of the program- and portfolio-level management practices in our ITIM framework, which are based on the investment management requirements in the Clinger-Cohen Act.[22] With respect to program-level practices, DHS has not defined specific criteria for selecting and prioritizing new programs or for reselecting and reprioritizing existing ones. Without such criteria, it is unlikely that investment selection and prioritization decisions will be made consistently and will best support mission needs. Without proper management controls in place, it is unlikely that investment oversight decisions will be made consistently and will best support mission needs. In addition, DHS has yet to adequately address how it determines and ensures that an investment is aligned with its EA. Specifically, while it has recently chartered its Enterprise Architecture Board and assigned it responsibility for ensuring that each investment is architecturally aligned throughout its life cycle, and while its new acquisition guidance specifies the architecture products that investments are to be aligned with (e.g., the business functions within the EA business model, the data objects in the conceptual data model, and the technical standards in the reference model), it has yet to define a methodology, including explicit criteria, for making a risk-based alignment determination. Also, the new directive and other DHS guidance do not provide for development of action plans for addressing areas of misalignment. DHS, in its comments, stated that they do not believe a methodology for alignment determinations is needed and that having subject matter

[22] The Clinger-Cohen Act of 1996, codified in relevant part at 40 U.S.C §§ 11311-11313.

experts involved in each determination is preferable given the wide range of IT programs at DHS; however, we believe that without such a methodology, it is not possible for the department to ensure that such alignment determinations are made consistently and repeatably. Without such acquisition and investment management controls, architecture alignment assessments will continue to largely be based on subjective and unverifiable judgments, and thus will not provide a sufficient basis for ensuring that systems are not duplicative and are interoperable.

With respect to portfolio-level practices, DHS does not have policies and procedures for evaluating or controlling its investment portfolios. Further, while post-implementation reviews are mentioned in DHS guidance, the guidance lacks specific procedures that would, for example, define roles and responsibilities for conducting these reviews and specify how the lessons learned and results of such reviews would be shared and used. Without such policies and procedures for portfolio management, DHS is at risk of not selecting and controlling the mix of investments in a manner that best supports the department's mission needs.

We are continuing to monitor DHS's efforts to more fully define its acquisition and investment management processes, as well as the extent to which acquisition reviews are performed regularly and consistently.

System Life Cycle Management Process Guidance Issued, But Improvements Still Needed

Managing IT projects and programs throughout their life cycles requires applying engineering discipline and rigor when defining, designing, developing, integrating, testing, deploying, and maintaining IT systems and services. Our evaluations and research show that applying such rigorous management practices improves the likelihood of delivering expected capabilities on time and within

budget.[23] In other words, the quality of IT systems and services is greatly influenced by the quality of the management processes involved in developing and acquiring them. According to leading practices, institutional system engineering maturity requires life cycle management processes that are clearly defined and applied on a repeatable basis across an organization.

A system life cycle management process normally begins with initial concept development and continues through requirements definition to design, development, various phases of testing, implementation, and maintenance. More specifically, during requirements definition, functional requirements are delineated in terms of system functionality (what the system is to do), performance (how well the system is to execute functions), data (what data are needed by what functions, when, and in what form), interfaces (what interactions with related and dependent systems are needed), and security (what controls are needed to address the assessed level of risk). As part of requirements definition, activities and documentation are produced to ensure that requirements are unambiguous, consistent with one another, linked (that is, traceable from one source level to another),[24] verifiable, understood by stakeholders, and fully documented.

The steps in the life cycle process each have important purposes and they have inherent dependencies among themselves. Thus, if earlier life cycle steps are omitted or not performed effectively, later steps will be affected, potentially resulting in costly and time-consuming rework. For example, a system can be effectively tested

[23] See, for example, GAO, *Aviation Security, Significant Management Challenges May Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: Feb. 29, 2006), and GAO, *Secure Border Initiative: DHS Needs to Address Significant Risks In Delivering Key Technology Investment*, GAO-08-1086 (Washington D.C.: Sept. 22, 2008).

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

to determine whether it meets requirements only if these requirements have been completely and correctly defined. To the extent that interdependent life cycle management steps or activities are not effectively performed, or are performed concurrently, a system acquisition or development program will be at risk of cost, schedule, and performance shortfalls.

Since 2004, we have reported that DHS lacked a standard and repeatable life cycle management process, and instead was relying on the processes that each of its components had in place. In 2008, DHS issued an interim life cycle management guide to introduce a standard system development methodology that can be tailored to specific projects.[25] To the department's credit, this guide addresses important aspects of effective system acquisition and development. For example, the guide requires that business objectives and systems requirements, as well as baseline performance goals, be defined and used as the measures of success for each program, and it requires that all programs be aligned with the HLS EA. Further, it requires acquisition management oversight and defines the roles and responsibilities of key stakeholders, including component CIOs and DHS IT portfolio managers, and to accomplish this it requires checkpoint reviews (i.e., stage reviews) throughout the program's life cycle. In addition, it specifies key activities associated with each life cycle stage (planning, requirements definition, design, development, integration and test, implementation, operation and maintenance, and disposition).

However, the interim guide does not address all key activities for each life cycle phase. For example, it does not address key practices associated with acquiring commercial products or services, such as evaluating commercial product and supplier viability and assessing commercial product dependencies/interoperability before purchasing the products. Also, while it does identify a list of work products that are to be created and updated to record the results of the activities performed for each life cycle stage, it does not address the content of all of these work products. For example, it does not provide a sample document or content template for a quality

[25] DHS, *Systems Engineering Life Cycle Instruction Guide v 1.9*, Nov. 7, 2008.

assurance plan, a configuration management plan, or a service reuse plan. Thus, opportunities remain to further define the SDLC. Moreover, it is unclear when and how this SDLC will be implemented. Until addressed, DHS will remain challenged in its ability to acquire and develop systems in a defined and repeatable manner.

Acquisition and IT Workforce Management Remains a Challenge

A strategic approach to human capital management is critical to ensuring that an organization has the right people with the right skills at the right time to perform a given function. Based on our research of leading organizations, we issued a model[26] for strategic human capital management in which strategic human capital planning was one cornerstone.[27] Through such planning, organizations can remain aware of its current workforce capabilities and its future workforce needs, and can be prepared for meeting these needs. According to our guidance, key practices for effective strategic human capital planning are generic, applying to any organization or component, such as an agency's acquisition or IT organization.[28] They include:

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

[26] GAO-02-373SP.

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

[28] GAO-04-39.

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

As is summarized below, DHS has yet to address either its acquisition or IT workforce needs in a manner that is fully consistent with these practices. Until DHS does so, it will continue to be at risk of not having sufficient people with the right knowledge, skills, and abilities to effectively and efficiently acquire key system investments.

Acquisition Workforce

In November 2008,[29] we reported that DHS had not developed a comprehensive strategic acquisition workforce plan to direct the department's future acquisition workforce efforts, and that the department lacked several elements that are key to developing such a plan. More specifically, we reported that DHS

- lacked an overall direction for acquisition workforce planning, and notwithstanding some recent actions, had not fully involved key stakeholders, such as the CHCO and component procurement and program offices, both of which have been shown to increase the likelihood of success for workforce planning;

- excluded some acquisition-related career fields from its definition of acquisition workforce, thus limiting the scope of its planning efforts, and while it intended to expand its definition, it had yet to identify which positions should be included;

- lacked sufficient data to fully assess its acquisition workforce needs, including the gaps in the number of employees needed or the skills of these employees; and

[29] GAO, *Department of Homeland Security: A Strategic Approach Is Needed to Better Ensure the Acquisition Workforce Can Meet Mission Needs*, GAO-09-30 (Washington, D.C.: Nov. 19, 2008).

- lacked sufficient insight into the number of contractors supporting its acquisition function or the types of tasks that contractors were performing.

DHS has undertaken several initiatives to begin addressing its acquisition workforce challenges. For example, its recruiting, hiring, and training initiatives have allowed it to hire new contract specialists and expand workforce access to acquisition-related training. Specifically, in January 2008, the CPO implemented the Acquisition Professional Career Program, and as of September 2008, had hired 49 contract specialist interns. In addition, CPO established an Acquisition Training Program in 2008 that included DHS-specific training for program managers, and it formed a council to coordinate acquisition workforce training opportunities across components.

In November 2008, we reported on several challenges that DHS faced in managing these initiatives.[30] For example, most initiatives aimed at defining and identifying the acquisition workforce and assessing acquisition workforce needs had yet to produce results, and in some cases were progressing more slowly than originally projected. DHS's initiatives also primarily focused on contract specialists despite other identified acquisition workforce shortages, and DHS had not determined how it would expand the initiatives. Further, DHS generally lacked documented performance goals and implementation steps—such as actions to be taken, needed resources, and milestones—for these initiatives.

Since that time, DHS has taken steps to expand two of its recruiting and hiring initiatives to additional acquisition-related career fields. Specifically, DHS developed plans to include career fields such as program management and engineering in its fall 2009 Acquisition Professional Career Program cohort. According to a CPO representative, DHS also plans to add acquisition career fields to its centralized hiring program and has recently hired a recruitment coordinator to carry out this expansion.

[30] GAO-09-30

IT Workforce

In June 2004,[31] we reported that DHS had begun strategic planning for IT human capital at the headquarters level, but it had not yet systematically gathered baseline data about its existing IT workforce across the department. Moreover, the DHS CIO had expressed concern at that time about staffing and acknowledged that progress in this area had been slow. In our report, we recommended that the department analyze whether it had appropriately allocated and deployed IT staff with the relevant skills to obtain its institutional and program-related goals. In response, the CIO established an IT human capital Center of Excellence to deliver, plans, processes, and procedures to execute an IT human capital strategy and to conduct an analysis of the skill sets of DHS IT professionals.

In September 2007,[32] we reported that DHS had developed a IT human capital plan and related documents that were largely consistent with federal guidance and associated best practices. For example, they provided for developing a complete inventory of existing IT staff skills, identifying IT skills needed to achieve agency goals, determining skill gaps, and developing plans to address such gaps. They also provided for involving key stakeholders—such as the CIO, Chief Human Capital Officer (CHCO), and component agency CIOs and human capital directors—in carrying out the skill gap analyses and follow on workforce planning.

However, we also reported that the plan did not fully address twelve key practices. For example, although the plan and supporting documents described the department's IT human capital goals and steps necessary to implement them, most steps did not include associated milestones. In addition, although the plan and supporting documents provided for involving key stakeholders, they did not assign those stakeholders specific responsibilities against which to

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

[32] GAO, *Information Technology: DHS's Human Capital Plan Is Largely Consistent with Relevant Guidance, but Improvements and Implementation Steps Are Still Needed*, GAO-07-425 (Washington, D.C.: Sept. 10, 2007).

hold them accountable for results. We also reported at that time that DHS had made limited progress in implementing its IT human capital plan. In particular, DHS CIO and CHCO officials, as well as officials from the three DHS agencies that we examined (CBP, FEMA, and the Coast Guard), all told us that they had yet to begin implementing the plan. Accordingly, we made recommendations aimed at strengthening and implementing the plan.

DHS has made limited progress in addressing our recommendations. For example it has not established implementation milestones, assigned stakeholder responsibilities and accountability, or begun to track, document, and report on human capital risks. Also, while DHS reported in 2007 that it intended to analyze its IT workforce makeup every 2 years, CIO and CHCO officials told us that this will not be done until after a planned 2010 Federal CIO Council-sponsored survey of the governmentwide IT workforce. Further, these officials stated that implementation of the 2007 IT human capital plan has been limited because the department's focus has been on strengthening its executive leadership team and its acquisition workforce, and that it only recently became engaged on departmentwide IT workforce issues. However, they added that DHS component organizations have been working to strengthen staff core competencies in four IT disciplines—Project Management, Security/Information Assurance, Enterprise Architecture, and Solutions Architecture.

According to officials from CBP, FEMA, and the Coast Guard, none of these component organizations have taken specific actions to implement the 2005 DHS IT human capital plan because they have not received any departmental instruction or guidance for doing so. Moreover, the extent to which they are each proactively and strategically addressing their respective human capital needs varies. For example, CBP's Office of Information Technology Workforce Management Group has a strategic IT human capital plan that defines goals (e.g., creating and enabling a team of leaders who have both the technical expertise and skills to manage and motivate employees, and providing education, training and development opportunities to allow employees to grow in their jobs and their careers), and the group has taken actions to achieve the goals (i.e., identifying employees with leadership potential, developing a

leadership curriculum for them, establishing an internship program, and creating a skills inventory). In contrast, FEMA's Office of Information Technology does not have a strategic IT human capital plan, although officials report that one is to be completed in fiscal year 2010, and in the interim, this office is assessing its workforce competency gaps, among other things. Further, while the Coast Guard has an IT strategic human capital plan, this plan is more than a decade old, as officials report that they have no immediate plans to update it.

Large-Scale IT Investments Exposed to Risk Because Key Acquisition and IT Management Controls Have Not Always Been Effectively Implemented

The success of a major IT program can be judged by the extent to which it delivers promised system capabilities and mission benefits on time and within schedule. As our research and evaluations show, a key determinant of program success is the extent to which the earlier discussed institutional acquisition and IT management controls are appropriately employed in managing each and every IT investment.

In this regard, our reviews of a number of large-scale DHS IT investments have disclosed a range of program management control weaknesses that have increased the risk of cost, schedule, and performance shortfalls. In many cases, DHS has since taken steps to address the weaknesses that we identified. However, some weaknesses have lingered, and we continue to identify issues on other programs. Moreover, these weaknesses are contributing to programs falling short of their capability, benefit, cost, and schedule expectations. To illustrate the prevalence and significance of these acquisition and IT management weaknesses, as well as DHS's progress in addressing them, we discuss work related to five large-scale programs—ACE, US-VISIT, Rescue 21, Secure Flight, and SBI*net*.

ACE

ACE is a multi-billion dollar program to incrementally modernize trade processing and support border security. Since 1999, we have issued a series of reports that have disclosed a number of acquisition and investment management weaknesses that have contributed to ACE performance shortfalls, including program costs increasing from $1 billion to about $3.1 billion, and ACE schedule slipping from fiscal year 2007 to fiscal year 2010. To address the weaknesses, we have made a number of recommendations. CBP has largely agreed with our recommendations, and continues to work to implement many of them. Below we provide a brief summary of ACE-related efforts to implement effective acquisition and IT management controls.

Beginning in May 1999,[33] we reported that ACE was not being defined in the context of an enterprise architecture, and that its life cycle cost estimates and cost/benefit analysis were inadequate. Further, ACE was not being acquired in accordance with disciplined investment management processes. As a result, CBP was not positioned to know that it was pursuing the right system solution for its needs and to deliver a defined a solution on time and schedule. Subsequently, CBP adopted an incremental approach to acquiring ACE, which we supported as a proven risk reduction measure for acquiring large-scale systems, but as we reported in June 2001,[34] ACE was being pursued separate from another trade-related system (known as the International Trade Data System), which was duplicative of and not aligned with ACE. Subsequently, this related system was merged with ACE.

Between May 2002 and February 2003, we continued to report on ACE challenges and weaknesses. Specifically, we reported that ACE was risky for a variety of reasons, including cost overruns, implications for changing how trade processing was performed, and

[33] GAO, *Customs Service Modernization: Actions Initiated to Correct ACE Management and Technical Weaknesses*, AIMD-99-198R (Washington, D.C.: May 18, 1999).

[34] GAO, *Customs Service Modernization: Results of Review of First Automated Commercial Environment Expenditure Plan*, GAO-01-696 (Washington, D.C.: June 5, 2001).

known key acquisition and IT management control weaknesses associated with, for example, program office human capital and software management processes.[35] Subsequently, we reported that CBP was working to implement our previous recommendations aimed at addressing acquisition and IT management control weaknesses, but that problems continued.[36] For example, ACE cost estimates were not reliable because they were not derived in accordance with estimating best practices. The next year we again reported that ACE was not following rigorous and disciplined acquisition and IT management controls, such as those related to managing the program office human capital, risks, and contract management.[37] For example, while initial ACE test results were positive, CBP had not taken steps to independently oversee the contractor's testing.

In May 2004,[38] we reported that the first two ACE system increments were operating, but that CBP's approach to incrementally acquiring and deploying ACE involved excessive overlap among increments. Moreover, the scheduling of increments had allowed for considerable overlap and concurrency among them, and this had produced a pattern of having to borrow resources from later increments to complete earlier increments. We concluded that this pattern had and would continue to result in ACE cost overruns and schedule delays. The next year, we reported that while CBP had revised its cost baselines in light of ACE overruns, this was not sufficient because the number of ACE increments had increased and system quality standards had been relaxed to allow increments to

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

[36] GAO, *Customs Service Modernization: Third Expenditure Plan Meets Legislative Conditions, but Cost Estimating Improvements Needed*, GAO-02-908 (Washington, D.C.: Aug. 9, 2002).

[37] GAO, *Customs Service Modernization: Automated Commercial Environment Progressing, but Further Acquisition Management Improvements Needed*, GAO-03-406 (Washington, D.C,: Feb. 28, 2003)

[38] 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)

proceed through key milestones despite the presence of material system defects.[39] We concluded that this practice, combined with the concurrency of increments, would exacerbate the program's cost and schedule shortfalls. We also reported that previously identified management control weaknesses remained, such as in system testing and in cost estimation, and that progress in addressing our recommendations had been slow.

In May 2006,[40] we reported that CBP had begun to make progress in addressing our recommendations through the establishment and use of a program-wide performance and accountability framework, as we had also recommended. However, control weaknesses remained. For example, considerable concurrency still remained among increments, thus increasing the risk of continued cost and schedule overruns. Also, while earned value management[41] was an OMB requirement, CBP discontinued its use on two ACE increments, thus limiting its ability to measure performance and progress.

In October 2007,[42] we reported that CBP had continued to take steps to establish an accountability framework grounded in measuring and disclosing progress against program performance measures and targets. However, ACE costs were likely to increase further because prior limitations in how system requirements were defined had resulted in an increase requirements and the need to replace a key

[39] GAO, *Information Technology: Customs Automated Commercial Environment Program Progressing, but Need for Management Improvements Continues*, GAO-05-267 (Washington, D.C.: Mar. 14, 2005)

[40] GAO, *Information Technology: Customs Has Made Progress on Automated Commercial Environment System, but It Faces Long-Standing Management Challenges and New Risks,* GAO-06-580 (Washington, D.C.: May 31, 2006).

[41] Earned value management is a project management tool that integrates the investment scope of work with schedule and cost elements for investment planning and control. This method compares the value of work accomplished during a given period with that of the work expected in the period. Differences in expectations are measured in both cost and schedule variances. OMB requires agencies to use earned value management as part of their performance-based management system for the parts of an investment in which development effort is required or system improvements are under way.

[42] GAO, *Information Technology: Improvements for Acquisition of Customs Trade Processing System Continue, but Further Efforts Needed to Avoid More Cost and Schedule Shortfalls*, GAO-08-46 (Washington, D.C.: Oct. 25, 2007)

software product, even though the new product may reduce user productivity. In addition, the inventory of ACE-related risks was incomplete and that information needed to make informed decisions on these risks was not being maintained.

We plan to continue to monitor CBP's progress in implementing our ACE-related recommendations.

US-VISIT

US-VISIT is a multi-billion dollar program to collect and maintain biographic and biometric information on certain foreign nationals who enter and exit the United States through over 300 air, sea, and land ports of entry. Since 2003, we have continued to report on US-VISIT acquisition and IT management control weaknesses that increased the risk of delivering less system capabilities and mission benefits than envisioned, and taking longer and costing more than expected. To the department's credit, it has addressed many of the recommendations that we have made for addressing these weaknesses, and as a result the program is better positioned today for success than it has been in the past. However, these weaknesses have contributed to instances of the program not living up to expectations, and some weaknesses still remain that pose future risks. Below we provide a brief summary of US-VISIT-related efforts to implement effective acquisition and IT management controls.

We first reported on US-VISIT in June 2003,[43] finding that program plans did not sufficiently define what specific system capabilities and benefits would be delivered, by when, and at what cost, and how US-VISIT intended to manage the acquisition to provide reasonable assurance that it would meet their commitments. Without defining such commitments, it was not possible to measure program performance and promote accountability for results. Shortly thereafter, in September 2003[44], we concluded that the

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

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

program was high risk because, among other things, its size, complexity, mission criticality, and enormous potential costs, coupled with a range of program management control weaknesses, including an immature governance structure, lack of clarity about its operational environment, facility implications, and mission value. In May 2004,[45] we reported that US-VISIT did not have a current life-cycle cost estimate or a cost benefit analysis, and that testing of an initial increment of system capabilities was not well-managed, and was not completed until after the increment became operational. Moreover, the test plan used was not completed until after testing was concluded.

In February 2005,[46] we reported that DHS had hired a prime integration contractor to augment its ability to deliver US-VISIT, but that acquisition management weaknesses continued. For example, we found that an effort to pilot alternative system solutions for delivering the capability to track persons exiting the U.S. was faced with a compressed time line, missed milestones, and a reduced scope that limited its value.

In February 2006,[47] we reported that the DHS's progress in implementing 18 GAO recommendations made in previous reports was mixed, but overall slow in critical areas, including completing cost-benefit analyses for increments, determining whether proposed increments would produce mission value consistent with costs and risks, developing well-defined and traceable test plans prior to testing, and assessing workforce and facility needs for new functionality.

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

[46] GAO, *Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program*, GAO-05-202 (Washington, D.C.: Feb. 23, 2005).

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

In February 2007,[48] we reported that DHS had not adequately defined and justified its proposed investment in planned and ongoing exit pilot and demonstration projects, and that it continued to invest in US-VISIT without a clearly defined operational context (enterprise architecture) that included explicit relationships with related border security and immigration enforcement initiatives. At the same time, program management costs had risen sharply, while costs for development had decreased, without any accompanying explanation of the reasons. We also reiterated our prior findings concerning a lack of program transparency and accountability due to inadequate definition and disclosure of planned expenditures, timelines, capabilities, and benefits, as well as limited measurement and reporting on progress against each.

In August 2007,[49] we reported that while US-VISIT entry capabilities were operating at over 300 ports of entry, exit capabilities were not, and that DHS did not have a comprehensive plan or a complete schedule for delivering a biometric exit solution. In addition, DHS continued to invest heavily in program management activities without adequate justification for doing so, and it continued to propose spending tens of millions of dollars on US-VISIT exit projects that were not well-defined, planned, or justified on the basis of costs, benefits, and risks.

In February 2008,[50] we reported that while DHS had partially defined a strategic solution for meeting US-VISIT goals, including defining and beginning development of a key capability known as "Unique Identity," which was to establish a single identity for all individuals at their earliest possible interaction with any U.S. immigration and border management organization by capturing the individual's

[48] GAO, *Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified*, GAO-07-278 (Washington, D.C.: Feb. 14, 2007).

[49] GAO, *Homeland Security: U.S. Visitor and Immigrant Status Program's Long-standing Lack of Strategic Direction and Management Controls Needs to Be Addressed*, GAO-07-1065 (Washington, D.C.: Aug. 31, 2007)

[50] GAO, *Homeland Security: Strategic Solution for US-VISIT Program Needs to Be Better Defined, Justified, and Coordinated*, GAO-08-361 (Washington, D.C.: Feb. 29, 2008).

biometrics, including 10 fingerprints and a digital image. However it had not defined and economically justified a comprehensive strategic solution for controlling and monitoring the exit of foreign visitors, which was critical to accomplishing the program's goals. DHS was also taking a range of evolving actions, partially at the department level, to coordinate relationships among US-VISIT and other immigration and border control programs; however, this evolution had yet to progress to the point of reflecting the full scope of key practices that GAO previously identified as essential to enhancing and sustaining collaborative efforts that span multiple organizations. As a result, the department was at increased risk of introducing inefficiencies and reduced effectiveness resulting from suboptimizing these programs' collective support of immigration and border management goals and objectives.

In December 2008,[51] we reported on a lack of effective DHS executive oversight of the program, including involvement from the DHS CPO and the CHCO. In addition, we again reported that DHS lacked a detailed schedule for implementing an exit capability, and that, among other things, cost estimates for the then proposed exit solution were not reliable, risk management was not being effectively performed, and the program's task orders were frequently rebaselined, thus minimizing the significance of earned value management-based schedule variances.

Currently, we have work underway for the Chairman of the House Homeland Security Committee on the US-VISIT Comprehensive Exit project, including the extent to which the project's component efforts are being managed in an integrated fashion. In addition, we are required by statute to review the results of an ongoing pilot of exit solutions at airports.

[51] GAO, *Homeland Security: U.S. Visitor and Immigrant Status Indicator Technology Program Planning and Execution Improvements Needed*, GAO-09-96 (Washington, D.C.: Dec. 12, 2008).

Rescue 21

Rescue 21 is a billion dollar Coast Guard program to replace its existing search and rescue communications system—installed in the 1970's. Among other things, Rescue 21 is to allow continuous, uninterrupted communications on the primary ship-to-shore channel, limit communications gaps to less than 10 percent in the United States, provide direction finding and digital selective calling to better locate boaters in distress, allow communication with other federal and state systems, and protect communication of sensitive information. We have issued reports citing a number of acquisition and investment management weaknesses that have contributed to Rescue 21 performance shortfalls, including program costs increasing from $250 million to about $1 billion, and the schedule slipping from fiscal year 2006 to fiscal year 2017. To address the weaknesses, we have made a number of recommendations. Coast Guard has largely agreed with our recommendations, and continues to work to implement many of them. Below we provide a brief summary of Rescue 21-related efforts to implement effective acquisition and IT management controls.

In September 2003,[52] we reported that Rescue 21's initial operating capability milestone of September 2003 had been postponed, and that a new schedule had yet to be finalized. Also, while the program had established processes for managing system requirements and managing risks, the processes were not being followed. For example, key deliverables for testing, such as test plans, were not yet defined and approved.

In May 2006[53], we reported that Rescue 21 continued to experience acquisition management weaknesses relative to requirements management, project monitoring and oversight, risk management, cost and schedule estimating, and executive oversight, and that these weaknesses had contributed to program cost overruns and

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

[53] GAO, *United States Coast Guard: Improvements Needed in Management and Oversight of Rescue System Acquisition*, GAO-06-623 (Washington, D.C.: May 31, 2006).

schedule delays. Specifically, Rescue 21's total acquisition cost had risen from $250 million to $710.5 million, an increase of 184 percent, and its timeline for achieving full operational capability had been delayed from 2006 to 2011. Moreover, the most recent cost and schedule estimates were not reliable, and the program faced a possible future cost overrun of $161.5 million, which would bring the total acquisition cost to $872 million. Finally, the schedule estimate was uncertain due to ongoing contract renegotiations for the remaining sites, and pending decisions regarding vessel tracking functionality. Since then, the Coast Guard estimates that the program's total acquisition cost will exceed $1 billion; deployment of Rescue 21 to the 48 continuous states will be delayed to 2012; deployment of the vessel tracking capability will be delayed to 2015; and deployment to Alaska will not occur until 2017.

Secure Flight

Secure Flight is a multi-billion dollar TSA program to allow DHS to assume from airlines the responsibility of prescreening passengers for domestic flights by matching of passenger biographic information against terrorist watch lists. Among other things, Secure Flight is to prevent people suspected of posing a threat to aviation from boarding commercial aircraft in the United States, protect passengers' privacy and civil liberties, and reduce the number of people unnecessarily selected for secondary screening. TSA is currently in the process of phasing in its use of Secure Flight for domestic flights. Since 2005, we have reported on a number of acquisition and investment management weaknesses, such as requirements, testing, cost and schedule estimation, and security management, and made recommendations to address them. To TSA's credit, it has addressed most of the recommendations. Below we provide a brief summary of TSA efforts to implement effective acquisition and IT management controls.

We first reported on Secure Flight in March 2005,[54] finding that TSA had not yet completed key development activities needed to successfully deliver an operational system, such as finalizing requirements documents or completing required test activities. In addition, TSA had not developed performance goals and measures to gauge the effectiveness of the Secure Flight program, nor had it developed life-cycle cost estimates, which limited oversight and accountability.

In February 2006,[55] we reported that while TSA had made some progress in developing and testing Secure Flight, it had not followed a disciplined life cycle approach and, as a result, some project activities were conducted out of sequence, requirements were not well defined, and documentation contained contradictory information or omissions. Further, while TSA had taken steps to implement an information security management program for protecting information and assets, its efforts were incomplete, and that the program lacked schedule and cost estimates. Accordingly, we made recommendations to address these limitations. Later that year we reported that TSA had begun taking actions to address our recommendation, [56] including suspending development and undertaking a rebaselining, of the program.

In February 2007,[57] we reported that despite 4 years of effort, TSA had been unable to develop and implement Secure Flight, in large part, because it had not employed a range of acquisition and IT management control disciplines to effectively manage cost, schedule, performance, and privacy risks. At that time, TSA officials

[54] GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should be Managed as System is Further Developed*, GAO-05-356 (Washington, D.C.: Mar. 28, 2005).

[55] GAO, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: Feb. 9, 2006).

[56] GAO, *Transportation Security Administration's Office of Intelligence: Response to Posthearing Questions on Secure Flight*, GAO-06-1051R.(Washington, D.C.: Aug. 4, 2006).

[57] GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, But More Work Remains*, GAO-07-448T, (Washington, D.C.: Feb. 13, 2007).

stated that they intended to put in place a new management team; rebaseline the program's goals, capabilities, costs, and schedule; and establish more structured and controlled acquisition and IT management processes.

In February 2008,[58] we reported that TSA had made substantial progress in instilling more discipline and rigor into Secure Flight's development and implementation. For example, TSA had developed a detailed concept of operations, established a cost and schedule baseline, and drafted key management and systems development documents, among other systems development efforts. However, TSA had not followed established risk management processes and it had not followed key practices for developing reliable cost and schedule estimates. Further, TSA had yet to incorporate end-to-end testing into its testing strategy, and had not addressed all system security requirements and vulnerabilities.

On January 7, 2009,[59] we reported that TSA had not demonstrated Secure Flight's operational readiness and had generally not achieved several conditions set forth in the Department of Homeland Security (DHS) Appropriations Act, 2005.[60] These conditions related to, among other things, performance of stress testing and estimation of cost and schedule. For example, we found that despite provisions for stress testing in Secure Flight test plans, stress testing had not been performed. Further, while TSA had made improvements to its life-cycle cost estimate and schedule, neither were developed in accordance with key best practices.[61] As a result, the life-cycle cost estimate did not provide a meaningful baseline from which to track

[58] GAO, *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*, GAO-08-456T (Washington, D.C.: Feb. 28, 2008).

[59]On December 19, 2008, we provided the initial results of our work to staff of the Senate and House Appropriations Committees' Subcommittees on Homeland Security, which was based on work conducted as of December 8, 2008. Section 513(b) of the Department of Homeland Security Appropriations Act, 2008, mandated that GAO report to these committees within 90 days after the DHS Secretary's certification.

[60] P.L. 108-334 118 stat. 1319, sec. 522(a)(3).

[61]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

progress, hold TSA accountable, and provide a basis for sound investment decision making.

To TSA's credit, we recently reported that it had made notable progress in developing Secure Flight, including meeting nine out of ten key legislative conditions, including conducting performance and stress testing.[62] As a result, TSA was poised at the time to begin incremental deployment of Secure Flight. Since then, Secure Flight has begun operating at selected airports and for selected airlines.

SBI*net*

SBI*net* is a multi-billion dollar program that involves the acquisition, development, integration, and deployment of surveillance systems and command, control, communications, and intelligence (C3I) technologies to create a "virtual fence" along our nation's borders. Since 2007, we have reported on a number of SBI*net* acquisition and IT management weaknesses that increased the risk that the SBI*net* system will not perform as intended and meet user needs and expectations. For example, our first report identified weaknesses in how CBP was defining system requirements and managing program risks, including risks associated with acquiring SBI*net* through a series of concurrent task orders.[63] In October 2007[64] and again in February 2008,[65] we reported that the SBI*net* pilot, known as Project 28, was almost 8 months behind schedule in part because requirements were not adequately defined, contractor oversight was limited, and testing was not sufficiently performed. Later in 2008, we again reported on limitations in how SBI*net* risks were being

[62] GAO, *Aviation Security, TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*, GAO-09-292 (Washington, D.C.: May 2009).

[63] GAO, *Secure Border Initiative: SBInet Expenditure Plan Needs to Better Support Oversight and Accountability*, GAO-07-309 (Washington, D.C.: Feb. 15, 2007).

[64] GAO, *Secure Border Initiative: Observations on Selected Aspects of SBInet Program Implementation*, GAO-08-131T (Washington, D.C.: Oct. 2007).

[65] GAO, *Secure Border Initiative: Observations on the Importance of Applying Lessons Learned to Future Projects*, GAO-08-508T (Washington, D.C.: Feb. 2008).

managed, as well as areas in which SBI*net* had yet to demonstrate alignment to DHS's enterprise architecture.

In September 2008,[66] we reported that after investing about 3 years in acquiring and developing SBI*net*, important aspects of the program remained ambiguous and were in a continued state of flux, making it unclear and uncertain what technology capabilities would be delivered, when and where they would be delivered, and how they would be delivered. Also, the program did not have an approved integrated master schedule to guide the execution of the program, and that assimilation of available information indicated that the schedule had continued to change. Further, we reiterated that the program had not effectively performed key requirements development and management practices, such as ensuring alignment between different levels of requirements. Finally, we reported that SBI*net* testing had not been effectively managed; individual system components to be deployed to the initial deployment locations had not been fully tested, a test management strategy had not yet been finalized and approved, and the draft plan contained omissions in content.

We made a series of recommendations to address these weaknesses, including assessing SBI*net* development, testing, and deployment risks and disclosing them to DHS leadership and the Congress, and defining and implementing relevant system deployment, requirements management, and testing weaknesses guidance. DHS largely agreed with our recommendations. We currently have work underway for the Chairman, House Homeland Security Committee, relative to SBI*net* risks and recommendation implementation, SBI*net* test management, planning, execution, and results, and SBI*net* contract management and oversight.

In closing, the department has made progress in establishing key institutional acquisition and IT investment management-related

[66] GAO, *Secure Border Initiative Fiscal Year 2008 Expenditure Plan Shows Improvement, but Deficiencies Limit Congressional Oversight and DHS Accountability*, GAO-08-739R (Washington D.C.: June 26, 2008).

controls and implementing them on large-scale programs, including its recent efforts to increase corporate oversight of major investments and its recent deployment and operation of Secure Flight. However, considerable work remains to be accomplished before the department can be considered a mature IT system acquirer and investor. For example, the department has yet to address longstanding challenges in, among other things, sufficiently defining its enterprise architecture and strategically managing its acquisition and IT workforce. Moreover, while program-specific weaknesses that we have identified have in many cases eventually been addressed, our concern is that these types of weaknesses were allowed to exist and in some cases took years to address, and that we continue to find them on other programs that we later review. Such a pattern of inconsistency across major programs is indicative of institutional acquisition and IT management immaturity. Unless this changes, ongoing and future DHS major acquisitions will likely fall short in delivering promised capabilities and benefits on time and on budget.

Our existing recommendations continue to provide the department with a framework for maturation, and thus we encourage the department to move swiftly in implementing both our institutional and program-specific recommendations. To this end, we look forward to working constructively with the department in doing so and thereby maximizing the role that IT can play in DHS's mission performance and transformation.

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

Contacts and Acknowledgements

For future information regarding this testimony, please contact Randolph C. Hite, Director, Information Technology Architecture and Systems Issues, at (202) 512-3439, or hiter@gao.gov. Other individuals who made key contributions to this testimony were Kathleen Agatone, Mathew Bader, Justin Booth, James Crimmer, Deborah Davis, Elena Epps, Ash Huda, John P. Hutton, Tonia Johnson, Neela Lakhmani, Anh Le, Anne McDonough-Hughes, Gary

Mountjoy, Sabine Paul, Tomas Ramirez, Jr., Amelia Shachoy, and Teresa Smith.