United States Government Accountability Office

GAO

Report to the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

June 2007

HOMELAND SECURITY

Departmentwide Integrated Financial Management Systems Remain a Challenge

GAO
Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-536, a report to the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Since the Department of Homeland Security (DHS) began operations in March 2003, it has faced the daunting task of bringing together 22 diverse agencies and developing an integrated financial management system to provide timely, reliable, and useful financial information. GAO was asked to determine (1) whether DHS has fully developed plans for implementing and/or migrating to an integrated departmentwide financial management system, (2) the potential usefulness of the work products received for the funds spent on the financial modernization effort, and (3) going forward, how DHS can incorporate best practices into its plans for migrating to an integrated departmentwide financial management system. GAO interviewed key DHS officials, reviewed relevant DHS policy and procedure documents, and analyzed work products related to the financial modernization effort.

What GAO Recommends

To help reduce the risks associated with a departmentwide financial management system implementation effort, GAO makes six recommendations focused on the need for DHS to define a departmentwide financial management strategy and embrace best practices to foster systems development, including key human capital practices. DHS concurred with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-536.

To view the full product, including the scope and methodology, click on the link above. For more information, contact McCoy Williams at (202) 512-9095 or Keith Rhodes at (202) 512-6412.

June 2007

HOMELAND SECURITY

Departmentwide Integrated Financial Management Systems Remain a Challenge

What GAO Found

DHS has not yet developed a financial management strategy and plan to move forward with its financial management system integration efforts. In early March 2007, DHS officials issued a plan to address existing internal control weaknesses, but this plan is at a high level and more detailed implementation strategies will be necessary to fully address the financial management systems challenges. With Office of Management and Budget (OMB) approval, DHS indicated that it has decided to migrate components to internal service providers using selected financial management systems models currently in place at two components. However, the components that DHS is considering have material financial management weaknesses.

The Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency (eMerge^2) program that was expected to integrate financial management systems across the entire department and address financial management weaknesses was halted in December 2005. DHS has stated that it had spent about $52 million in total for the eMerge^2 project, including approximately $18 million of contractor costs, but the department did not provide support for these amounts. According to DHS officials, several of the work products developed for eMerge^2 will be useful as they move forward with their financial management modernization efforts, regardless of the strategic financial management direction ultimately selected by DHS. GAO's review indicated that key work products are of limited value. The concept of operations did not contain an adequate description of the legacy systems and a clear articulation of the vision that should guide the department's improvement efforts, and key requirements developed for the project are unclear and incomplete.

Consolidation of an entity as large and diverse as DHS poses significant management challenges, including integrating a myriad of redundant financial management systems and addressing existing and newly identified weaknesses in the inherited components. In order for DHS to avoid long-standing problems that have plagued financial management system improvement efforts at other agencies and not repeat the failure of eMerge^2, it must adopt solutions that reduce the risks associated with these efforts to acceptable levels. Based on best practices, there are four key building blocks that will be critical to DHS's ability to successfully complete its financial transformation: (1) developing a concept of operations, (2) defining standard business processes, (3) developing a migration and/or implementation strategy for DHS components, and (4) defining and effectively implementing disciplined processes necessary to properly manage the specific projects. Moreover, effective human capital management is critical to the success of systems implementations. Having staff with the appropriate skills is key to achieving financial management improvements, and managing an organization's employees is essential to achieving results.

Contents

Figures

Abbreviations

AICPA	American Institute of Certified Public Accountants
BPMN	business process modeling notation
CBP	U.S. Customs and Border Protection
CFO	Chief Financial Officer
COTS	commercial-off-the-shelf
CRP	conference room pilot
DHS	Department of Homeland Security
DOT	Department of Transportation
eMerge^2	Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency
EPR	Emergency Preparedness and Response
ERP	enterprise resource planning
FEMA	Federal Emergency Management Agency
FFMIA	Federal Financial Management Improvement Act of 1996
FLETC	Federal Law Enforcement Training Center
ICE	U.S. Immigration and Customs Enforcement
ICOFR	Internal Control Over Financial Reporting
IEEE	Institute of Electrical and Electronics Engineers
INS	U.S. Immigration and Naturalization Service
IT	information technology
OCFO	Office of the Chief Financial Officer
OFM	Office of Financial Management
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OM&S	operating materials and supplies
PP&E	property, plant, and equipment
RMTO	Resource Management Transformation Office
SEI	Software Engineering Institute
TSA	Transportation Security Administration
UDO	undelivered order

G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 21, 2007

The Honorable Tom Carper
Chairman
The Honorable Tom Coburn, M.D.
Ranking Member
Subcommittee on Federal Financial Management,
Government Information, Federal Services, and
International Security
Committee on Homeland Security and
Governmental Affairs
United States Senate

Since the Department of Homeland Security (DHS) began operations in March 2003, as mandated by the Homeland Security Act of 2002,[1] it has faced the daunting task of bringing together 22 diverse agencies and developing an integrated financial management system. Since 2003, we have designated implementing and transforming DHS as high risk[2] because the agency has yet to implement a corrective action plan that includes a comprehensive transformation strategy, and because its management systems—especially related to financial, information, acquisition, and human capital management—are not yet integrated and wholly operational. DHS inherited many financial management weaknesses and vulnerabilities from 22 agencies. Auditors had identified 30 reportable

[1] Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002).

[2] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

conditions,[3] 18 of which were considered material internal control weaknesses[4] in fiscal year 2003.

DHS began implementation of the Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency (eMerge^2) program in January 2004 to integrate financial management systems across the entire department and to address the financial management weaknesses. eMerge^2 was expected to establish the strategic direction for migration, modernization, and integration of DHS financial, accounting, procurement, personnel, asset management, and travel systems, processes, and policies. DHS officials have stated that approximately $52 million in total was spent on the eMerge^2 project before it was halted in December 2005. DHS officials are considering other options to provide integrated financial management systems and are assessing the capabilities of financial management systems at various internal components. In March 2006, we reported[5] that DHS was at an important crossroads in implementing a financial management system, and we discussed the necessary building blocks that form the foundation for successful financial management system implementation efforts. As DHS moves forward, periodic independent updates on the status of financial management modernization that aligns with a comprehensive transformation strategy are important to help key congressional leaders and DHS management provide effective oversight. Moreover, DHS must be able to provide reliable, useful, and timely financial management

[3] Under standards issued by the American Institute of Certified Public Accountants (AICPA), “reportable conditions” are matters coming to the auditors’ attention relating to significant deficiencies in the design or operation of internal controls that, in the auditors’ judgment, could adversely affect the department’s ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. The AICPA recently revised its guidance for audits of financial statements beginning on or after December 15, 2006; the term “reportable condition” has been replaced by “significant deficiency.”

[4] A material weakness was previously defined as a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. The new definition of a material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

[5] GAO, *Financial Management Systems: DHS Has an Opportunity to Incorporate Best Practices in Modernization Efforts*, GAO-06-553T (Washington, D.C.: Mar. 29, 2006).

information, so that DHS leadership and the Congress are well positioned to make fully informed decisions to secure America's homeland.

You asked us to establish baseline information on DHS's financial management system modernization and to periodically update the status of these efforts. This report, our first in response to your request, provides an assessment of the status of DHS's efforts to modernize its financial management systems. Because of your concern about DHS's successful implementation of an integrated financial management system, you also asked us to determine (1) whether DHS has fully developed plans for implementing and/or migrating to an integrated departmentwide financial management system, (2) the potential usefulness of the work products received for the funds spent on eMerge^2, and (3) going forward, how DHS can incorporate key building blocks and human capital best practices into its plans for implementing and/or migrating to an integrated departmentwide financial management system.

This report incorporates lessons learned and best practices from our prior work that focused on federal government financial management system implementation efforts. We interviewed key DHS officials and reviewed their existing policies and procedures related to financial management systems. We analyzed and reviewed eMerge^2 work products as well as related current financial management initiatives under way. Our work on this report was performed in Washington, D.C., from September 2006 through April 2007 in accordance with generally accepted government auditing standards. Details on our scope and methodology are included in appendix I. Related GAO reports are listed at the end of this report.

Results in Brief

While DHS officials have recognized the need for an integrated financial management system, no financial strategy or integrated financial management systems effort that includes financial management policies and procedures, standard business processes, a human capital strategy, and effective internal controls has been developed. Moreover, DHS has experienced significant turnover in leadership, has yet to address the root causes of existing financial management problems, and still lacks a financial management strategy that includes a formal strategic financial management plan to implement or migrate to an integrated system.

In early March 2007, DHS officials issued a high-level plan with a stated purpose of addressing the existing internal control weaknesses. While a positive step, the plan has a policy and process focus and does not comprise a strategy for financial systems modernization. More detailed implementation strategies will be necessary to fully address the financial management system integration efforts. DHS recognizes that there is an urgent need for an integrated financial management system, and told us that after assessing the capabilities of existing financial management systems at several of its components, it has decided to consolidate its financial management systems. In commenting on a draft of this report, DHS indicated that it plans to leverage its current investments by migrating components to internal service providers using the financial management systems models currently in place at either the Transportation Security Administration (TSA)[6] or U.S. Customs and Border Protection (CBP). Our concern is that these components have numerous financial management weaknesses. For example, the financial statement auditors for TSA reported[7] that the agency was unable to provide sufficient evidential matter or make knowledgeable representations to support fiscal year 2005 and 2006 transactions and account balances, particularly for budgetary accounting; undelivered orders; and property, plant, and equipment, among others.

According to DHS officials, several of the work products developed for eMerge^2 will be useful as they move forward with their financial management modernization efforts, regardless of the strategic financial management direction ultimately selected by DHS. However, our review indicated that the usefulness of many of the eMerge^2 work products is questionable. The work products developed include a core set of financial management system requirements and various other qualitative financial management plans, including a concept of operations document. Our review of the core set of financial management requirements and concept of operations developed for the eMerge^2 project found that DHS had not fully incorporated best practices in this effort, and therefore it is not surprising that the results were significantly flawed and the work products were not very useful. For example, the concept of operations document lacked critical elements called for by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) standards,[8] such as providing a detailed

[6] The U.S. Coast Guard operates TSA's financial management system.

[7] Department of Homeland Security, *Performance and Accountability Report Fiscal Year 2006* (Washington, D.C.: November 2006).

[8] *IEEE Guide for Information Technology – System Definition – Concept of Operations Document*, Std.1362-1998. The IEEE is a nonprofit, technical professional association that develops standards for a broad range of global industries, including the information technology and information assurance industries, and is a leading source for defining best practices.

description of the existing system(s) that DHS planned to replace. In addition, our review of key eMerge² requirements identified requirements that were unclear and incomplete when compared with the attributes called for in the IEEE standards.[9] DHS has little to show for the $18 million in contractor costs and $52 million overall it reported to us that it spent on eMerge². DHS did not to provide documentation to support these reported costs. DHS's decision to end the project before spending an estimated $229 million on a financial management system that would not provide the expected system functionality and desired performance was prudent, and we support the decision to cut its losses. However, the agency has made little progress since that time and has missed an invaluable opportunity to address existing financial management problems.

As we previously reported,[10] consolidation of an entity as large and diverse as DHS poses significant management challenges, including integrating a myriad of redundant financial management systems and addressing existing and newly identified weaknesses in the inherited components. The federal government has long been plagued by financial management system modernization efforts that have failed to meet their cost, schedule, and performance goals. In order for DHS to avoid these long-standing problems that have plagued financial management system improvement efforts and avoid repeating the mistakes it made with eMerge², it must adopt solutions that reduce the risks associated with these efforts to acceptable levels. In our March 2006 testimony,[11] we identified four key concepts that will be critical to DHS's ability to successfully complete the implementation of an integrated financial management system or migration to shared service providers. Careful consideration of these concepts, each one building upon the next, will be integral to the success of DHS's strategy. The four building blocks are (1) developing a concept of operations, (2) defining standard business processes, (3) developing an implementation or migration strategy for DHS components, and (4) defining and effectively implementing disciplined processes necessary to properly manage the specific projects. Effective human capital

[9] *IEEE Recommended Practice for Software Requirements Specifications*, Std. 830-1998. This recommended practice is aimed at specifying requirements of software to be developed but also can be applied to assist in the selection of in-house and commercial software products.

[10] GAO, *Financial Management: Department of Homeland Security Faces Significant Financial Management Challenges*, GAO-04-774 (Washington, D.C.: July 19, 2004).

[11] GAO-06-553T.

management, such as strategic workforce planning and change management, is also identified as critical to successfully implementing a new financial management system. DHS officials recognize the importance of having sufficient staff on board to execute a financial management strategy, but because DHS does not currently have a financial management system project in place, it has not yet developed human capital plans and activities. As DHS develops a financial management plan or strategy, careful consideration of key human capital practices will be a critical success factor.

We are making six recommendations focused on the need for DHS to develop a financial management plan or strategy and to fully adopt the building blocks and human capital practices that are vital to minimizing the risk related to modernizing its financial management systems. In written comments on a draft of this report, DHS concurred with our recommendations and described the approach and steps that are planned to improve DHS's financial management systems. DHS's comments are discussed in the Agency Comments and Our Evaluation section and reprinted in appendix V. DHS also provided several technical comments, which we incorporated as appropriate.

Background

When DHS was created in March 2003 and merged 22 diverse agencies, there were many known financial management weaknesses and vulnerabilities in the inherited agencies. For 5 of the agencies that transferred to DHS—Customs Service (Customs),[12] TSA, Immigration and Naturalization Service (INS),[13] Federal Emergency Management Agency (FEMA), and Federal Law Enforcement Training Center (FLETC)—auditors had identified 30 reportable conditions, 18 of which were considered material internal control weaknesses. Further, of the four component agencies—Customs, TSA, INS, and FEMA—that had previously been subject to stand-alone financial statement audits, all four agencies' systems were found not to be in substantial compliance with the

[12] The Bureau of Customs and Border Protection is now the U.S. Customs and Border Protection component of DHS.

[13] Bureau of Immigration and Customs Enforcement is now the U.S. Immigration and Customs Enforcement component of DHS.

requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA).[14]

Most of the 22 components that transferred to DHS had not been subjected to significant financial statement audit scrutiny prior to their transfer, so the extent to which additional significant internal control deficiencies existed was unknown. For example, conditions at the Coast Guard surfaced because of its greater relative size and increased audit scrutiny at DHS as compared to its former legacy agency, the Department of Transportation (DOT). As part of DOT's financial statement audit, the Coast Guard had no specifically attributable reported weaknesses identified. However, identified weaknesses related to the Coast Guard were one of the main reasons that the independent auditors were unable to provide an opinion on DHS's consolidated balance sheets as of September 30, 2006 and 2005. The auditors identified numerous material weaknesses related to fund balance with treasury; property, plant, and equipment; and budgetary accounting. Moreover, the auditors reported that the Coast Guard did not have an organizational structure that fully supported the development and implementation of effective policies, procedures, and internal controls. The Coast Guard's personnel rotation policy, among other issues, made it difficult for the Coast Guard's Chief Financial Officer to institutionalize internal controls related to financial management and reporting.

As noted above, material internal control weaknesses have been an ongoing problem at DHS since its inception, and these material internal control weaknesses and financial reporting problems continued in fiscal year 2006. We previously reported[15] that for fiscal year 2003, the DHS financial statement auditors reported 14 total reportable conditions, 7 of which were considered to be material weaknesses. In fiscal year 2006, while the total number of reportable conditions decreased to 12, the number of reportable conditions considered to be material weaknesses increased to 10. A description of the material weaknesses as identified by the auditors in fiscal years 2003 through 2006 can be found in appendix II.

[14] Federal Financial Management Improvement Act of 1996, Pub. L. No. 104-208, div. A, § 101(f), title VIII, 110 Stat. 3009, 3009-389 (Sept. 30, 1996), requires agencies to implement financial management systems that substantially comply with (1) federal financial management systems requirements, (2) federal accounting standards, and (3) the *U.S. Standard General Ledger* at the transaction level.

[15] GAO-04-774.

Some of the more recent material weaknesses identified by the auditors include problems with fund balance with treasury, budgetary accounting, and intergovernmental balances.

The DHS Financial Accountability Act of 2004[16] made DHS subject to the Chief Financial Officers Act of 1990 (CFO Act),[17] which requires DHS to issue audited financial statements, among other things. In fiscal year 2006, the DHS financial statement auditors issued a disclaimer of opinion because the scope of their work was not sufficient to express an opinion given the seriousness of DHS's financial management problems. DHS's Inspector General engaged the auditors to audit the balance sheet and statement of custodial activity for the fiscal year that ended September 30, 2006. The auditors were not engaged to audit DHS's statements of net costs, changes in net position, budgetary resources, and financing for the years ended September 30, 2006 and 2005, because the Office of Financial Management, Coast Guard, TSA, FEMA, U.S. Immigration and Customs Enforcement (ICE), and the Management Directorate were unable to provide sufficient evidence to support account balances presented in the financial statements. In fiscal year 2006, DHS's financial statement auditors also reported[18] that DHS was not in compliance with the CFO Act as well as other key financial management reform legislation, such as the Federal Managers' Financial Integrity Act of 1982[19] and FFMIA. Resolving all reported internal control weaknesses, addressing serious financial management systems deficiencies, and complying with financial management reform legislation are key to DHS's ability to produce relevant and reliable financial information that will enable it to better manage the department and provide accountability.

[16] The Department of Homeland Security Financial Accountability Act of 2004, Pub. L. No. 108-330 § 3, 118 Stat. 1275, 1276 (Oct. 16, 2004), added DHS to the list of CFO Act agencies.

[17] Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990).

[18] Department of Homeland Security, *Performance and Accountability Report Fiscal Year 2006* (Washington, D.C.: November 2006).

[19] Pub. L. No. 97-255, 96 Stat. 814 (Sept. 8, 1982) (codified at 31 U.S.C. § 3512 (c), (d)).

DHS Lacks a Fully Developed Financial Management Strategy and Plan

The eMerge[2] program that was expected to integrate financial management systems across the entire department and address financial management weaknesses was a failure, and DHS wisely halted the project in December 2005. Since that time and 4 years after the creation of the agency, DHS is still contemplating various financial management options. DHS has yet to clearly define a financial management strategy and plan to move forward with its financial management system modernization efforts. Such a plan is needed to address the fundamental financial management problems that have existed since the agency was created. In early March 2007, DHS officials issued a high level plan, which DHS stated was intended to address existing internal control weaknesses. While a first step, more detailed implementation strategies and plans will be necessary to fully address the financial management systems challenges.

DHS officials told us they have decided to consolidate the department's financial management systems. DHS and Office of Management and Budget (OMB) officials told us that OMB approved DHS's decision to rely on its in-house core financial management operations. DHS officials within the Office of the Chief Financial Officer stated that they were performing an internal assessment of the financial management systems being used by the components and revisiting current internal financial service providers, such as the Coast Guard, to determine whether they can leverage those resources. The systems used by TSA and CBP were some of the internal DHS systems being considered. Recent plans call for the Coast Guard to move to the TSA systems model. In accordance with this approach, DHS officials told us that they have plans to develop three or four shared service providers using the existing component financial management systems. Some of the services may include information technology (IT) hosting,[20] business process services,[21] and application management services.[22] However, DHS did not provide documentation or evidence of the internal assessment that it was conducting or when it would be completed. In commenting on a draft of this report, DHS indicated that it

[20] IT hosting involves providing secure facility space, networks, and hardware to host software applications and providing the necessary personnel to operate this secure environment.

[21] Business process services involve services ranging from transaction processing to financial management services. The range of services may include general ledger reconciliation, budget formulation, and audit support.

[22] Application management services include services for running and managing access to business software applications and the feeder systems that provide data to the financial management software.

was focusing on two current systems already in use at TSA and CBP and how to migrate other DHS components to those systems.

The components that DHS is considering as systems models have material financial management weaknesses and consequently do not appear to be good candidates to be the models used by an entity with an annual budget in excess of $40 billion. While DHS has corrective action plans under way to address identified weaknesses, most of the component core financial management systems are unable to produce reliable, useful, and timely financial information. The auditors have not been able to issue an opinion on DHS's financial statements since the agency was created in 2003. For example, in fiscal year 2006, TSA, one of the proposed internal systems models, was unable to provide sufficient evidential matter or make knowledgeable representation of facts and circumstances to the DHS financial statement auditors to support transactions and account balances of TSA for amounts reported on DHS's balance sheet. Specifically, TSA was unable to support transactions related to property and equipment, accrued unfunded employee leave, accounts payable, and components of net position. In addition, the auditors reported that TSA did not have sufficient processes and procedures to enable the successful completion of a financial statement audit in fiscal years 2005 and 2006. In commenting on a draft of this report, DHS officials stated that TSA's audit shortcomings were centered on policies and procedures, not systems-oriented problems. However, our analysis of the auditor's report indicated that the problems were broad based. As DHS pointed out in its comments, success in financial management rests upon a comprehensive framework of people, policy, process, systems, and assurance. Accordingly, it is imperative that DHS understand the policy and procedure weaknesses at TSA in order to prevent such weaknesses from affecting subsequent users.

Further, the Coast Guard, TSA's current shared service provider, was unable to provide sufficient evidential matter or make knowledgeable representations of facts and circumstances to the DHS financial statement auditors, to support transactions and account balances of the Coast Guard for amounts reported on DHS's balance sheet. The Coast Guard was unable to support transactions related to fund balance with treasury; accounts receivable; actuarially-derived liabilities; environmental and legal liabilities; operating materials and supplies; certain categories of property, plant, and equipment; undelivered orders and changes in net position; and adjustments, both manual and automated, made as part of the Coast Guard's financial reporting process. The Coast Guard was also unable to complete corrective actions, and make adjustments, as necessary, to these and other balance sheet amounts, prior to the completion of the DHS 2006

Performance and Accountability Report. The total assets of the Coast Guard, as reported on the DHS balance sheet as of September 30, 2006, were $12.5 billion, or 16 percent of total DHS consolidated assets. In addition, the auditors reported that the Coast Guard does not have an organizational structure that fully supports the development and implementation of effective policies, procedures, and internal controls. Consequently, to the extent that the shared service approach is sustained, it will be critical for DHS to avoid replicating these weaknesses and ineffective policies and procedures at other components.

According to DHS officials, migration is only one component of an improvement program and can be costly, risky, and very disruptive. We agree that implementation of any financial management system brings a degree of risk. This is magnified when an organization has a range of serious problems as is the case with DHS. Our report[23] summarizing financial management systems implementation problems at other federal agencies established that failure to effectively follow best practices was a key shortcoming that lead to failure to meet cost, schedule, and performance goals. Later in this report, we offer our perspective on how DHS can embrace these best practices to minimize these risks as it moves forward.

Managing the transformation of an organization of the size and complexity of DHS requires comprehensive planning, integration of key management functions across the department, and partnering with stakeholders across the public and private sectors. On September 13, 2006, the department's CFO testified before the Congress that DHS's goals for improving its financial systems have not changed and a major effort remains to improve all of its resource management systems. Rather than focus only on systems, the CFO testified that the department was currently developing an overarching strategy to address challenges in the areas of people, process, policy, systems, and assurances to achieve the department's goals of obtaining a clean audit opinion, establishing sound internal controls, and improving the efficiency of financial operations. The CFO stated that DHS understands that some systems are aging; that some fail to meet all user requirements; and that some are not fully integrated with finance, procurement, and asset management. To meet these needs, the DHS CFO reported that DHS is building a financial management framework. The

[23] GAO, *Financial Management Systems: Additional Efforts Needed to Address Key Causes of Modernization Failures*, GAO-06-184 (Washington, D.C.: Mar. 15, 2006).

CFO said that the centerpiece of the effort to improve agency financial processes and address the existing financial management problems is DHS's *Internal Controls Over Financial Reporting (ICOFR) Playbook*, released in March 2007. DHS officials have reported that the *ICOFR Playbook* draws from internal control best practices to establish a management control program that measures performance and provides accountability for improvement. DHS officials expect the *ICOFR Playbook* to guide DHS ahead for the next several years through fundamental financial management improvement across the spectrum of financial activities supporting the agency's mission.

We found that the *ICOFR Playbook* does not contain adequate detail to clarify the approach that DHS plans to take to modernize its financial management systems. For example, the *ICOFR Playbook* focuses on financial statement preparation and only includes two tracks. The first track focuses on corrective action strategies for material weaknesses, and the second track focuses on building support for the Secretary's internal control over financial reporting assurance statement. In its comments on a draft of this report, DHS officials acknowledged that the *ICOFR Playbook* is at the policy and process level and does not comprise a specific strategy for financial systems modernization. Much more detail is needed to provide a financial management strategy or plan for integrating and modernizing DHS's financial management systems. While there continues to be much focus on agency and governmentwide audit opinions, getting a clean audit opinion, though important in itself, is not the end goal. The end goal is the establishment of a fully functioning CFO operation that includes (1) modern financial management systems that provide reliable, timely, and useful information to support day-to-day decision-making and oversight and for the systematic measurement of performance; (2) a cadre of highly qualified senior level and supporting staff; and (3) sound internal controls that safeguard assets and ensure proper accountability.

eMerge^2 Costs Are Unknown and Work Products Have Limited Usefulness

Although DHS stated that it had spent about $52 million in agency costs for the eMerge^2 project, including approximately $18 million of contractor costs, it did not provide adequate support for these amounts. Moreover, DHS believes that the eMerge^2 funds spent will benefit its future financial management modernization efforts since a number of the work products can still be used. However, our review of two key items—a concept of operations document and system requirements—found that they have significant deficiencies and will be of little use for future efforts. Specifically, the concept of operations does not contain an adequate description of the legacy systems and a clear articulation of the vision that should guide the department's improvement efforts, while key requirements developed for the project are unclear and incomplete. Based on best practices that form the foundation for successful financial management systems implementation, DHS will have little assurance that its future efforts will meet their cost, schedule, and performance goals. These issues are discussed in greater detail later in this report.

Actual Costs of eMerge^2 Are Unknown

DHS officials told us they ended the eMerge^2 program because (1) the project fell behind schedule and (2) the contactor could not meet established performance goals. We were unable to confirm the estimated $52 million in eMerge^2 program costs because DHS officials did not provide adequate supporting evidence to document this amount after repeated GAO requests. eMerge^2 was expected to establish the strategic direction for migration, modernization, and integration of DHS financial, accounting, procurement, personnel, asset management, and travel systems, processes, and policies. DHS officials began working on the project in late fiscal year 2003. DHS contracted with Bearing Point, Inc. (Bearing Point) to develop the functional and technical eMerge^2 requirements. These requirements were approved by all DHS components in May 2004. Based on these requirements, DHS developed a Request for Quotation for the acquisition and implementation of eMerge^2.

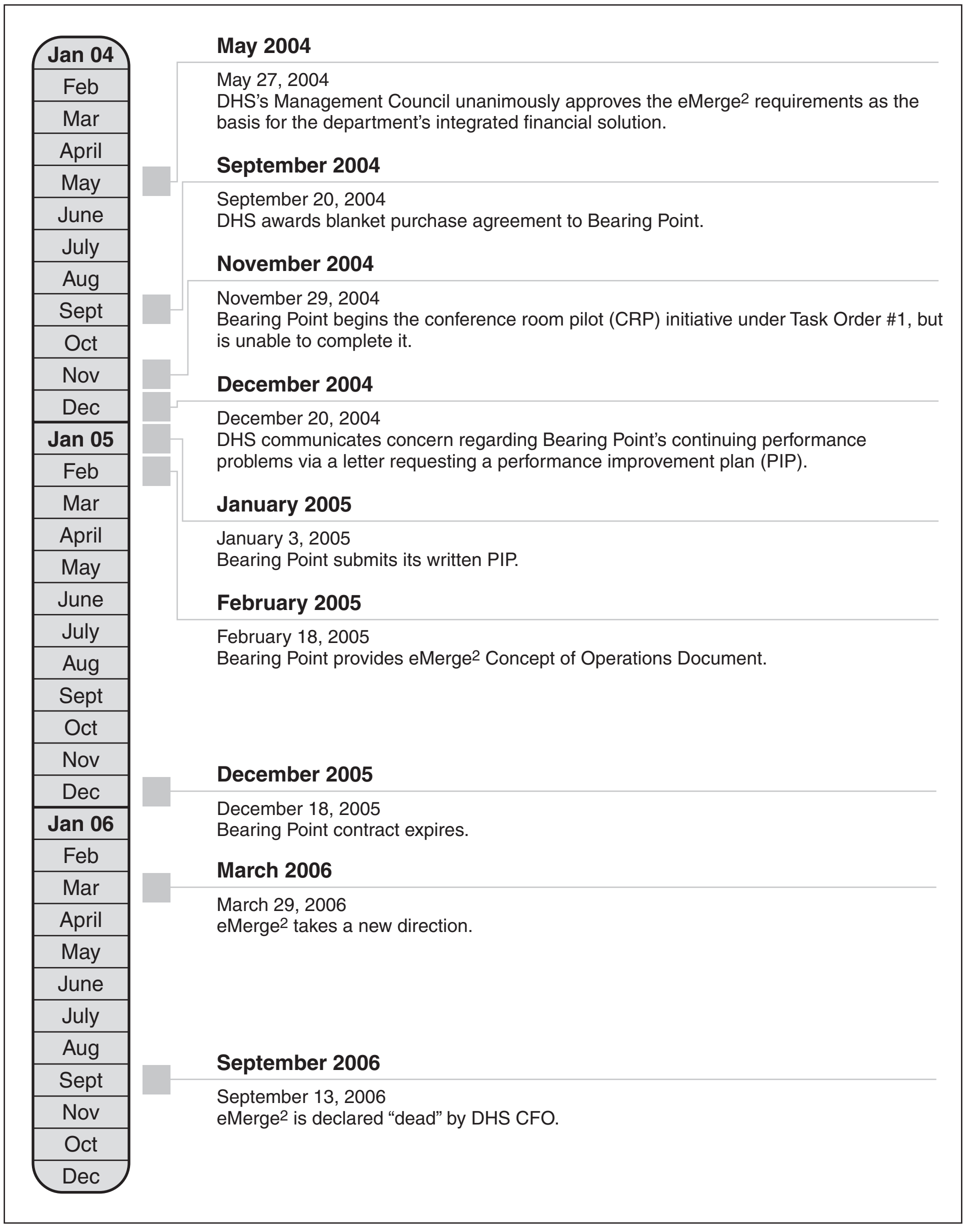
In September 2004, after a competitive acquisition process, Bearing Point was awarded a blanket purchase agreement with a ceiling of about $229 million to acquire and implement the eMerge^2 solution. The first task order was issued under the agreement for solution development and conference room pilot (CRP) testing.[24] Bearing Point began the CRP initiative in November 2004, and soon into work on this task order, concerns began to arise regarding the extent to which there was a clear understanding between DHS and Bearing Point on exactly what was to be delivered. In December 2004, DHS officials formally communicated their concerns to Bearing Point by requesting a performance improvement plan. In January 2005, Bearing Point submitted a performance improvement plan. According to DHS officials, Bearing Point missed deadlines, and some products presented to the eMerge^2 project team were deemed unacceptable. In February 2005, the DHS CFO conducted a review of the

[24] CRP is a configured solution ready for the execution of scenarios. The solution is measured against its capability to satisfy the eMerge^2 requirements. The CRP was not executed.

eMerge^2 effort. DHS chose not to exercise the next contract option, and the Bearing Point contract to acquire and implement eMerge^2 expired in December 2005. See figure 1 for a summary of the eMerge^2 timeline. In March 2006, DHS's Deputy CFO testified[25] that eMerge^2 was taking a new direction in that the department was going to perform an internal assessment of existing financial management systems at the component level to determine whether resources could be leveraged. DHS officials also reported that they were going to review the OMB Financial Management Line of Business initiative to assess whether migration to a shared service provider was a feasible option. Finally, in September 2006, the newly appointed CFO stated that eMerge^2 was officially "dead."

[25] Department of Homeland Security - March 29, 2006, testimony before the House Government Reform Subcommittee on Government Management, Finance, and Accountability and the House Homeland Security Subcommittee on Management, Integration, and Oversight.

Figure 1: eMerge[2] Project Timeline



May 2004

May 27, 2004
DHS's Management Council unanimously approves the eMerge[2] requirements as the basis for the department's integrated financial solution.

September 2004

September 20, 2004
DHS awards blanket purchase agreement to Bearing Point.

November 2004

November 29, 2004
Bearing Point begins the conference room pilot (CRP) initiative under Task Order #1, but is unable to complete it.

December 2004

December 20, 2004
DHS communicates concern regarding Bearing Point's continuing performance problems via a letter requesting a performance improvement plan (PIP).

January 2005

January 3, 2005
Bearing Point submits its written PIP.

February 2005

February 18, 2005
Bearing Point provides eMerge[2] Concept of Operations Document.

December 2005

December 18, 2005
Bearing Point contract expires.

March 2006

March 29, 2006
eMerge[2] takes a new direction.

September 2006

September 13, 2006
eMerge[2] is declared "dead" by DHS CFO.

Source: GAO.

eMerge^2 Work Products Have Limited Future Usefulness

According to DHS officials, several of the work products developed during eMerge^2 will benefit its future financial management modernization efforts. These products included a concept of operations and over 7,000 requirements. A review of these two critical products found that they will not provide much assistance to future efforts since they do not contain the attributes normally associated with such documents. The concept of operations document we reviewed did not include all the important elements and the requirements did not flow from the concept of operations. Moreover, key requirements (1) lacked the IEEE characteristics associated with good requirements; (2) did not incorporate the functionality associated with inventories, supplies, and materials; and (3) did not consider appropriate internal control. Accordingly, these documents will have to undergo significant rework before they can be used in future efforts.

The Concept of Operations Document Is Flawed

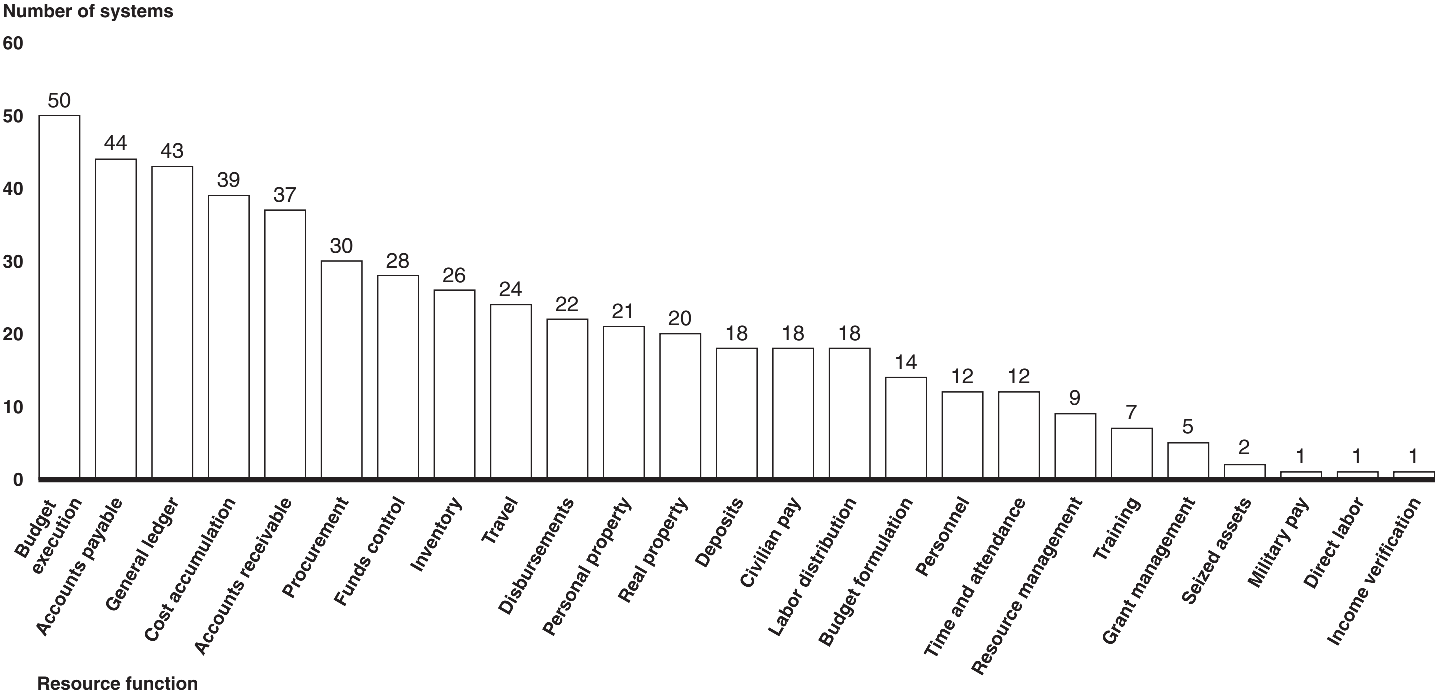
Our review of the DHS concept of operations found that it did not have the types of information expected when compared to best practices. As we noted in March 2006, a concept of operations defines how an organization's day-to-day operations are (and will be) carried out to meet mission needs. The concept of operations includes high-level descriptions of information systems, their interrelationships, and information flows. It also describes the operations that must be performed, who must perform them, and where and how the operations will be carried out. Further, it provides the foundation on which requirements definitions and the rest of the systems planning process are built. Normally, a concept of operations document is one of the first documents to be produced during a disciplined development effort and flows from both the vision statement and the enterprise architecture. According to IEEE standards,[26] a concept of operations is a user-oriented document that describes the characteristics of a proposed system from the users' viewpoint. The key elements that should be included in a concept of operations are major system components, interfaces to external systems, and performance characteristics, such as speed and volume.

Our review of the DHS concept of operations found that it lacked several key attributes called for by best practices. For example, DHS officials stated that the guiding principles of the functional vision for the eMerge^2 program focused on the "to-be" state and that they did not attempt to document the "as-is" state. As noted in the IEEE standard, the "as-is"

[26] IEEE Std. 1362-1998.

environment is normally captured or depicted in the concept of operations document. In the case of DHS this is especially important since when the eMerge[2] project began, DHS had identified over 500 financial management and related systems in operation and much of its operational history was contained in legacy systems data files. Figure 2 provides a summary of DHS's systems inventory by resource functions.

Figure 2: DHS Systems Inventory



Source: DHS.

Due to the large number of systems, DHS needs to define in its concept of operations (1) which legacy systems will be migrated to the new environment and (2) conceptually how this transition is envisioned to occur in order to achieve an integrated environment. As we noted in our March 2006 testimony,[27] the transition strategy outlined in the concept of operations is useful for developing an understanding of how and when changes will occur. Not only is this needed from an investment

[27] GAO-06-553T.

management point of view, it is a key element in addressing human capital problems relating to change management strategies. Simply saying "all systems will be migrated to the new environment" does not provide an understanding of how this transition will take place or provide the necessary specificity to help the concept of operations serve as the foundation for the requirements management process. For example, should DHS decide to develop and implement a standard budget system that includes both formulation and execution, it would need to ensure that the new budget system achieved the functionality associated with over 60 existing budget legacy systems.

eMerge^2 System Requirements Are Deficient

Although DHS officials told us that they expected the requirements developed for eMerge^2 to be salvageable and provide a foundation for its future efforts, our review found that key requirements did not have attributes associated with good requirements developed using best practices. Requirements are specifications that system developers and program managers use to design, develop, and acquire a system. They need to be carefully defined, consistent with one another, verifiable, and directly traceable to higher level business or functional requirements. Most importantly, the eMerge^2 requirements were not based on (1) a good concept of operations, (2) reengineered business processes, and (3) an appropriate internal control structure.

In our March 2006 report,[28] we noted that business process models provide a way of expressing the procedures, activities, and behaviors needed to accomplish an organization's mission and are helpful tools to document and understand complex systems. Business processes are the various steps that must be followed to perform a certain activity. For example, the procurement process would start when the agency defines its needs and issues a solicitation for goods or services, and would continue through contract award and receipt of goods and services, and would end when the vendor properly receives payment. The identification of preferred business processes is critical for the standardization of applications and training and portability of staff.

DHS officials reportedly developed approximately 33 business processes across five business domains[29] using Business Process Modeling Notation

[28] GAO-06-184.

[29] The DHS five business domains are (1) accounting and reporting, (2) acquisition and grants, (3) asset management, (4) budget, and (5) cost and revenue performance management.

(BPMN)[30] during the eMerge[2] effort. While DHS officials stated that they placed an emphasis on business processes when capturing requirements, their business process emphasis focused on the “to-be” state versus the “as-is” state. However, industry standards suggest that it is important to model the processes currently in operation (“as-is”) because it allows an organization to discover the existing core business processes. An organization needs to be fully aware of its existing core business processes because reassessment of those processes is necessary to ensure continued value and capability in a new system. In order to maximize the success of a new system, redesigning the current business processes while promoting consistency through the development of standard business processes is essential for a large and complex agency like DHS. Identifying or developing preferred business processes for standardization of applications and training and portability of staff also helps when selecting the appropriate software that best reflects the preferred business processes.

Since DHS has not defined its standard business processes, it is unclear whether the requirements are valid because some of the requirements are process specific and we were unable to test the linkage between requirements and DHS business processes. DHS developed over 7,000 external requirements and derived requirements. The external requirements were compiled based upon externally mandated laws and regulations. The derived requirements were compiled based upon business process modeling that incorporated external requirements, business rules, leading practices, known deficiencies, roles, data objects, and interface requirements. The derived requirements were also organized by the five functional domains noted above. However, even assuming that the requirements were “linked” to the processes that DHS would like to employ, many of the key requirements did not have the attributes associated with good requirements. The following are examples of the requirements problems we noted.

[30] BPMN defines a Business Process Diagram, which is based on a flowcharting technique tailored for creating graphical models of business process operations. A business process model, then, is a network of graphical objects, which are activities (i.e., work) and the flow controls that define their order of performance.

- One requirement stated that "the system must calculate gross pay, deductions, net pay, employee, and employer contributions for each employee on an effective pay period basis." The requirement is unnecessary because all of DHS's components have migrated payroll processing functions to the Department of Agriculture's National Finance Center. Moreover, the requirement does not address basic questions, such as (1) which payroll system will perform this function, (2) how is the gross pay amount defined, and (3) what deductions must be supported (taxes, retirement, employee allotments, etc.).
- Another requirement stated that "the bottom line of this reconciliation would be the net cost of operations defined." It is unclear what reconciliation is being performed and how the net cost of operations is defined or which other requirement provided this formula.
- We were unable to identify critical requirements relating to inventory. According to DHS's fiscal year 2006 statements, the department held about $677 million in inventory and supplies. Basic requirements, such as determining the inventory valuation method and ensuring that inventory items transferred between DHS locations retain their historical cost basis, were not included. These are critical items for maintaining visibility of assets and the financial presentation process.
- All requirements were considered "equal." For example, some requirements were simply the language used in a given law or regulation while other requirements appeared to be intended to provide additional specificity to those requirements. However, these related requirements were not "linked" in such a manner that made these relationships clear. One approach that can be used is to provide a hierarchal structure. Under this concept, the general requirements are at one level while the more specific requirements are at a lower level and linked to the higher level requirements. This process maintains the necessary traceability (another best practice concept) between the requirements.[31]

DHS officials have stated that the eMerge^2 requirements did not consider the internal control structure. OMB's *Core Financial System Requirements*[32] have several mandatory requirements that must be

[31] Requirements for projects can be expressed at various levels depending on user needs. They range from agencywide business requirements to increasingly detailed functional requirements that eventually permit the software project managers and other technicians to design and build the required functionality in the new system. Adequate traceability ensures that a requirement in one document is consistent with and linked to applicable requirements in another document.

[32] OMB's Office of Federal Financial Management, *Core Financial System Requirements*, OFFM-NO-0106, January 2006.

considered when migrating or implementing the system management function in federal financial management systems. Some of these requirements include accounting classification, document and transaction control, system generated transactions, and audit trails. OMB Circular No. A-123, *Management's Responsibility for Internal Control*, requires agencies to operate systems with appropriate internal controls to ensure accuracy of data, completeness and consistency of transaction processing, and adequate reporting. Automatic internal control capabilities needed to meet the provisions of Circular No. A-123 are expected to be integrated into financial management systems. For example, requirements that specify validations to be performed on invoice data before they can be certified as ready for payment and system-enforced separation of duties are some of the basic control activities that are expected to be integrated into a financial management system. As we have noted in numerous reports, requirements management problems are a leading cause of systems that do not meet their cost, schedule, and functionality objectives. (See our related GAO products section at the end of this report).

Four Key Building Blocks and Effective Human Capital Management Must Drive DHS's Financial Management Transformation Efforts

Based on industry best practices, we have identified four key building blocks that will be critical to DHS's ability to successfully complete its financial transformation. Our March 2006 testimony[33] pointed out that careful consideration of these four concepts, each one building upon the former, will be integral to the success of DHS's strategy. The four concepts are (1) developing a concept of operations, (2) defining standard business processes, (3) developing a migration and/or implementation strategy for DHS components, and (4) defining and effectively implementing disciplined processes necessary to properly manage the specific projects. Fully embracing these four building blocks and human capital best practices will be critical to the success of any future financial management plan or strategy that addresses implementing and/or migrating to an integrated departmentwide financial management system at DHS. DHS also has an opportunity to reap substantial benefits by reengineering business processes and standardizing those processes so that productivity gains and staff portability across the various components are realized. In addition, identifying staff with the requisite skills to implement such systems and identifying gaps in needed staff skills and filling them are necessary to successfully implement and operate a new financial management system. Any financial management plan or strategy

[33] GAO-06-553T.

implemented by DHS will be complex and challenging, making the adoption of best practices even more important for this undertaking. We will now highlight the key issues to be considered for each of the four areas and human capital. Moreover, detailed key questions for DHS to consider related to each concept can be found in appendix III.

Concept of Operations Provides Foundation

As we discussed previously, a concept of operations defines how an organization's day-to-day operations are (or will be) carried out to meet mission needs. The concept of operations includes high-level descriptions of information systems, their interrelationships, and information flows. It also describes the operations that must be performed, who must perform them, and where and how the operations will be carried out. Further, it provides the foundation on which requirements definitions and the rest of the systems planning process are built. Normally, a concept of operations document is one of the first documents to be produced during a disciplined development effort and flows from both the vision statement and the enterprise architecture. According to the IEEE standards,[34] a concept of operations is a user-oriented document that describes the characteristics of a proposed system from the users' viewpoint. The key elements that should be included in a concept of operations are major system components, interfaces to external systems, and performance characteristics, such as speed and volume.

Another key element of a concept of operations is a transition strategy that is useful for developing an understanding of how and when changes will occur. Not only is this needed from an investment management point of view, it is a key element in the human capital problems discussed previously that revolved around change management strategies. Describing how to execute DHS's approach for implementing a new system or migrating to shared service providers, as well as the processes that will be used to deactivate legacy systems that will be replaced or interfaced with a new financial management system, are key aspects that need to be addressed in a transition strategy.

[34] IEEE Std. 1362-1998.

Standard Business Processes Promote Consistency

Business process models provide a way of expressing the procedures, activities, and behaviors needed to accomplish an organization's mission and are helpful tools to document and understand complex systems. In our view, an agency's mission must drive the business processes and the resulting financial information is a derivative of these processes. Moreover, business processes are the various steps that must be followed to perform a certain activity. For example, the procurement process would start when the agency defines its needs and issues a solicitation for goods or services, and would continue through contract award and receipt of goods and services, and would end when the vendor properly receives payment. As we discussed earlier in this report, the identification of preferred business processes would be critical for standardization of applications and training and portability of staff.

To maximize the success of a new system acquisition, organizations need to consider the redesign of current business processes. As we noted in our *Executive Guide: Creating Value Through World-class Financial Management*,[35] leading finance organizations have found that productivity gains typically result from more efficient processes, not from simply automating old processes. Moreover, the Clinger-Cohen Act of 1996 requires agencies to analyze the missions of the agency and, based on the analysis, revise mission-related and administrative processes, as appropriate, before making significant investments in IT used to support those missions.[36] Another benefit of what is often called business process modeling is that it generates better system requirements, since the business process models drive the creation of information systems that fit in the organization and will be used by end users. Other benefits include providing a foundation for agency efforts to describe the business processes needed for unique missions and developing subprocesses to support those at the departmentwide level.

Strategy for Consolidating and Migrating Financial Management Systems Will Be Key

Although DHS officials have stated that they plan to consolidate their financial management systems, the department has not yet articulated a detailed plan for achieving this goal. In the context of consolidating financial management operations, which will include migrating to a selected systems model, critical activities include (1) developing specific

[35] GAO, *Executive Guide: Creating Value Through World-class Financial Management*, GAO/AIMD-00-134 (Washington, D.C.: April 2000).

[36] See 40 U.S.C. §11303(b)(2)(C).

criteria for requiring component agencies to migrate to one of the providers rather than attempting to develop and implement their own stove-piped business systems; (2) providing the necessary information for a component agency to select a DHS-approved financial management system; (3) defining and instilling new values, norms, and behaviors within component agencies that support new ways of doing work and overcoming resistance to change; (4) building consensus among customers and stakeholders on specific changes designed to better meet their needs; and (5) planning, testing, and implementing all aspects of the transition from one organizational structure and business process to another.

Regardless of the strategy DHS takes, sustained leadership will be key to a successful migration strategy for moving DHS toward a consolidated financial management system. In our *Executive Guide: Creating Value Through World-class Financial Management*, we found that leading organizations made financial management improvement an entitywide priority by, among other things, providing clear, strong executive leadership. We also reported that making financial management a priority throughout the federal government involves changing the organizational culture of federal agencies. Although the views about how an organization can change its culture can vary considerably, leadership (executive support) is often viewed as the most important factor in successfully making cultural changes. Top management, such as the Secretary, must be totally committed in both words and actions to changing the culture, and this commitment must be sustained and demonstrated to staff. As pressure mounts to do more with less, to increase accountability, and to reduce fraud, waste, abuse, and mismanagement, and efforts to reduce federal spending intensify, sustained and committed leadership will be a key factor in the successful migration of DHS's financial management systems.

Disciplined Processes Will Help Ensure Successful Implementation

Once the concept of operations and standard business processes have been defined and a migration or implementation strategy is in place, the use of disciplined processes will be a critical factor in helping to ensure that the implementation is successful. The key to avoiding long-standing implementation problems is to provide specific guidance to component agencies for financial management system implementations, incorporating the best practices identified by the Software Engineering Institute, the IEEE, the Project Management Institute, and other experts that have been proven to reduce risk in implementing systems. Such guidance should include the various disciplined processes, such as requirements management, testing, data conversion and system interfaces, risk and project management, and related activities, which have been problematic in the financial systems implementation projects we and others have reviewed.

Disciplined processes have been shown to reduce the risks associated with software development and acquisition efforts to acceptable levels and are fundamental to successful system implementations. The principles of disciplined IT systems development and acquisition apply to shared services implementation, such as that contemplated by DHS. A disciplined software implementation process can maximize the likelihood of achieving the intended results (performance) within established resources (costs) on schedule. For example, disciplined processes should be in place to address the areas of data conversion and interfaces, two of the many critical elements necessary to successfully implement a new system—the lack of which has contributed to the failure of previous agency efforts. Further details on disciplined processes can be found in appendix IV. Inadequate implementation of disciplined processes can manifest itself in many ways when implementing a financial management system. Full deployment has been delayed at some agencies and specific functionality has been delayed or flawed at other agencies.

Strong Human Capital Management Needed at DHS

Effective human capital management is critical to the success of systems implementations. As we reported in our *Executive Guide: Creating Value Through World-class Financial Management*,[37] having staff with the appropriate skills is key to achieving financial management improvements, and managing an organization's employees is essential to achieving results. The independent public accountants that conducted DHS's fiscal year 2006 audit have stated that many of the department's difficulties in financial management and reporting can be attributed to the original stand-up of a large, new, and complex executive branch agency without adequate organizational expertise in financial management and accounting. Moreover, DHS's Resource Management Transformation Office (RMTO) officials have stated that outside contractors are currently performing some of the financial management activities or duties that internal DHS staff would normally perform because of staffing shortages. Having adequate and sufficient human resources with the requisite training and experience to successfully implement a financial management system is a critical success factor.

[37] GAO/AIMD-00-134.

Our work[38] has identified significant human capital issues, including the lack of IT expertise, that have affected financial systems implementation at other agencies. Some of the human capital problems we identified that have hampered the implementation of new financial management systems include incomplete strategic workforce planning and ongoing staff shortages as well as untrained staff. By not identifying staff with the requisite skills to implement such systems and by not identifying gaps in needed skills and filling them, agencies reduce their chances of successfully implementing and operating a new financial management system. Further, OMB guidance[39] requires agencies to have qualified project managers for major IT investments.

Strategic human capital management for financial management projects includes organizational planning, staff acquisition, and team development. Human capital planning is necessary for all stages of the system implementation. It is important that agencies incorporate strategic workforce planning by (1) aligning an organization's human capital programs with its current and emerging mission and programmatic goals and (2) developing long-term strategies for acquiring, developing, and retaining an organization's total workforce to meet the needs of the future. As we have recently testified,[40] some of the most pressing human capital challenges at DHS include (1) successfully completing its ongoing transformation; (2) forging a unified results-oriented culture across the department; (3) obtaining, developing, providing incentives to, and retaining needed talent; and (4) most importantly, leadership at the top, to include a chief operating officer or chief management officer. The federal government has always faced the challenge of sustaining the momentum of transformation because of the limited tenure of key administration officials, and managing the transformation of an organization of the size and complexity of DHS requires comprehensive planning and integration of key management functions across the department.

Conclusions

GAO and others have found that the key to implementing systems that meet cost, schedule, and performance objectives is to have effectively

[38] GAO-06-184.

[39] See OMB, *Information Technology Project Manager Qualification Guidance*, M-04-19 (Washington, D.C.: July 21, 2004), and OMB Circular No. A-11, § 300.

[40] GAO, *Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security*, GAO-07-398T (Washington, D.C.: Feb. 6, 2007).

implemented the disciplined processes necessary to reduce risks to acceptable levels. DHS has not yet taken the first step, which is to define a formal financial management strategy that addresses the fundamental financial management problems that have existed since the agency's creation. Ending eMerge^2 was a judicious decision; however, we are concerned that DHS still lacks a clearly defined financial management strategy or financial management systems implementation effort to even begin to address DHS's integration and transformation issues as reported in our most recent high-risk report. Furthermore, because DHS is one of the largest and most complex executive branch agencies in the federal government, developing, operating, maintaining, and modernizing its financial management systems represent a monumental challenge. This challenge is compounded by DHS's newness and the poor condition of the range of legacy financial and related business systems it inherited. To that end, critical success factors include utilizing the four building blocks and human capital best practices to provide reasonable assurance that the risks associated with implementing a departmentwide integrated financial management system are minimized. Otherwise, DHS runs the risk of repeating the failure of eMerge^2.

Recommendations for Executive Action

To help reduce the risks associated with a departmentwide financial management system implementation effort, we recommend that the Secretary of DHS demonstrate commitment to integrating DHS's financial management systems and direct the Undersecretary for Management and Chief Financial Officer to take the following six actions. This would entail placing a high priority on fully integrating into its approach the following concepts and underlying key issues, which are related to the fundamental disciplined processes typically utilized in systems implementation.

- Clearly define and document a departmentwide financial management strategy and plan to move forward with its financial management system integration efforts.
- Fully embrace the four building blocks and best practices when developing and documenting the strategy and plan to foster the development of an integrated financial management system that meets expected performance and functionality targets. This would include the following:
  - Developing a comprehensive concept of operations document
  - Reengineering business processes and standardizing them across the department, including applicable internal control

- Developing a detailed plan for consolidating and migrating various DHS components to an internal shared services approach if this approach is sustained
- Utilizing and implementing the specific disciplined processes below to minimize project risk

  1. Requirements management
  2. Testing
  3. Data conversion and system interfaces
  4. Risk management
  5. Configuration management
  6. Project management
  7. Quality assurance

- Carefully consider key human capital practices as DHS moves forward with its financial management transformation efforts so that the right people with the right skills are in place at the right time.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from DHS, which are reprinted in appendix V. DHS concurred with our recommendations and described the actions it has taken or plans to take to improve financial management systems and departmentwide financial accountability. As DHS moves forward to address the recommendations in our report, it is important that it prioritize its efforts and focus on the concepts and key issues we discussed, such as clearly documenting and defining a departmentwide financial management systems integration strategy and implementing disciplined processes. We are encouraged that DHS has recognized that attention is needed and is developing plans to address these financial management systems issues. It is critical that the departmentwide financial management strategy is documented and stresses the importance of a standard set of business processes. We continue to believe that careful consideration of all the building blocks and key issues we identified will be integral to the success of DHS's financial management systems integration efforts. DHS also provided technical comments, which we incorporated as appropriate.

As arranged with your offices, unless you announce the contents of this report earlier, we will not distribute it until 30 days from its date. Then we will send copies of this report to interested congressional committees. We will also send copies to the Secretary of Homeland Security, the DHS Under Secretary for Management, and the DHS Chief Financial Officer. Copies will be made available to others upon request. In addition, this report will also be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact McCoy Williams, Director, Financial Management and Assurance, who may be reached at (202) 512-9095 or by e-mail at williamsm1@gao.gov, or Keith A. Rhodes, Chief Technologist, Applied Research and Methods, who may be reached at (202) 512-6412 or by e-mail at rhodesk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VI.

McCoy Williams

McCoy Williams
Director
Financial Management and Assurance

Keith A. Rhodes
Chief Technologist
Applied Research and Methods
Center for Technology and Engineering

Appendix I: Scope and Methodology

To determine whether the Department of Homeland Security (DHS) has developed plans for implementing and/or migrating to an integrated departmentwide financial management system, we interviewed key DHS officials, reviewed relevant DHS's Resource Management Transformation Office's (RMTO) policy and procedure documents, and analyzed the Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency (eMerge^2) work products related to the financial modernization effort. We reviewed DHS performance and accountability reports, particularly the Management Discussion and Analysis section, to determine whether there were any financial management system modernization initiatives under way. We also reviewed the Office of Management and Budget (OMB) Exhibit 300, and relevant contractor files and procurement data.

To assess the potential usefulness of work products received for funds spent on eMerge^2 efforts, we interviewed DHS officials and analyzed relevant DHS eMerge^{2}planning documents, the eMerge^2 requirements database, and RMTO policy and procedure documents. We evaluated the key information in the requirements database by selecting requirements that focused on accounting and financial reporting issues. Based on our analysis, we concluded that the requirements we reviewed were unclear and incomplete. As a result, we determined it would not be useful for DHS's future efforts to integrate financial management systems. We also reviewed Bearing Point, Inc.'s contractor files to determine the nature and scope of contractual services provided by the systems integrator. We requested but did not receive invoices and other documents to support amounts spent on eMerge^2. Accordingly we were unable to test amounts DHS officials told us were spent on the project. As a result we are unable to provide any assurance on the accuracy of these amounts.

To provide our views on how DHS can incorporate key building blocks and human capital best practices into its plans for migrating to an integrated departmentwide financial management system going forward, we reviewed our prior reports and material from key industry groups and national experts to identify any potential solutions posed by those groups, lessons learned, and relevant best practices.

We conducted our work in Washington, D.C., from September 2006 through April 2007, in accordance with U.S. generally accepted government auditing standards. We did not evaluate the federal government's overall information technology strategy or whether DHS selected the most appropriate financial management systems approach. We are making recommendations to DHS in this report. We requested comments on a draft of this report from the Secretary of DHS or his designee. Written comments from the Department of Homeland Security are reprinted in appendix V and evaluated in the "Agency Comments and Our Evaluation" section.

Appendix II: Material Weaknesses/Reportable Conditions at DHS for Fiscal Years 2003 through 2006

Number	Material weakness/reportable conditions	2003	2004	2005	2006
1	**Financial management and oversight:** DHS's Office of the Chief Financial Officer (OCFO) needs to establish financial reporting roles and responsibilities, assess critical needs, and establish standard operating procedures for the department. These conditions were not unexpected for a newly created organization, especially one as large and complex as DHS. The Coast Guard and the Strategic National Stockpile had weaknesses in financial oversight that have led to reporting problems.	√	√	√	√
2	**Financial reporting:** Key controls to ensure reporting integrity were not in place, and inefficiencies made the process more error prone. At the Coast Guard, the financial reporting process was complex and labor-intensive. Several DHS bureaus lacked clearly documented procedures, making them vulnerable if key people leave the organization.	√	√	√	√
3	**Financial systems security:** The auditors found weaknesses across DHS in its entitywide security program management and in controls over system access, application software development, system software, segregation of duties, and service continuity. Many bureau systems lacked certain functionality to support the financial reporting requirements.	√	√	√	√
4	**Property, plant, and equipment (PP&E):** The Coast Guard was unable to support the recorded value of $2.9 billion in PP&E due to insufficient documentation provided prior to the completion of audit procedures, including documentation to support its estimation methodology. The Transportation Security Administration lacked a comprehensive property management system and adequate policies and procedures to ensure the accuracy of its PP&E records.	√	√	√	√
5	**Operating materials and supplies (OM&S) and seized property:** Internal controls over physical counts of OM&S were not effective at the Coast Guard. As a result, the auditors were unable to verify the recorded value of $497 million in OM&S. The Coast Guard also had not recently reviewed its OM&S capitalization policy, leading to a material adjustment to its records when an analysis was performed. The Coast Guard Inventory Control Point physical inventory procedures lacked key elements of an effective physical inventory.	√	√	√	√
6	**Actuarial liabilities:** The Secret Service did not record the pension liability for certain employees and retirees, and when corrected, the auditors had insufficient time to audit the amount recorded. The Coast Guard does not have adequate policies, procedures, and controls to ensure the completeness and accuracy of the data necessary for the calculation of actuarial liabilities.	√		√	√
7	**Transfers of funds, assets, and liabilities to DHS:** DHS lacked controls to verify that monthly financial reports and transferred balances from legacy agencies were accurate and complete.	√			
8	**Fund Balance with Treasury:** The Coast Guard has not designed and implemented policies, procedures, and internal controls, including effective reconciliations and the use of a financial system that complies with Federal Financial System Requirements, as defined in OMB No. Circular A-127 and the requirements published by the Joint Financial Management Improvement Program.		√	√	√

Number	Material weakness/reportable conditions	2003	2004	2005	2006
9	**Legal and other liabilities:** The Office of Financial Management (OFM), in association with the Office of the General Counsel (OGC), has not implemented adequate policies and procedures to ensure that OFM is provided with sufficient information to accurately and completely present legal liabilities and related disclosures in the financial statements throughout the year.				√
10	**Intragovernmental and intradepartmental balances:** Immigration and Customs Enforcement (ICE), Emergency Preparedness and Response (EPR) and Coast Guard have not developed and adopted effective standard operating procedures, or established systems, to completely track, confirm, and reconcile intra-DHS balances and/or transactions with trading partners in a timely manner.		√	√	√
11	**Undelivered orders (UDO), accounts and grants payable, and disbursements:** ICE had difficulty maintaining accurate records relating to obligations and UDOs and did not establish sufficient controls to prevent duplicate payments.		√	√	
12	**Financial management structure:** OCFO has not provided the DHS bureaus with sufficient management oversight and timely policy guidance to address accounting and reporting issues that cross multiple bureaus and affect the efficiency of bureau financial accounting and reporting operations.		√		
13	**Budgetary accounting:** DHS lacked effective internal controls for validation and verification of UDO balances to ensure that recorded obligations were valid, and recorded in a timely manner, and that proper approval and supporting documentation is maintained.		√	√	√

Source: GAO based on DHS performance and accountability report(s).

Appendix III: Key Questions for the Department of Homeland Security to Consider Based on the Four Building Blocks

Building block	Key questions
Concept of operations	• What is considered a financial management system? Are all the components using a standard definition? • Who will be responsible for developing a DHS-wide financial management concept of operations, and what process will be used to ensure that the resulting document reflects the departmentwide solution rather than individual component agency stove-piped efforts? • How will DHS's concept of operations be linked to its enterprise architecture? • How can DHS obtain reliable information on the costs of its financial management systems investments?
Standard business process	• Who will be responsible for developing DHS-wide standard business processes that meet the needs of its component agencies? • How will the component agencies be encouraged to adopt new processes, rather than selecting other methods that result in simply automating old ways of doing business? • How will the standard business processes be implemented by DHS components or the shared service providers to provide consistency across DHS? • What process will be used to determine and validate the processes needed for DHS components that have unique needs?
Strategy for implementing the shared service approach	• What guidance will be provided to assist DHS and its component agencies in adopting a change management strategy that reduces the risks of consolidating systems and migrating to a shared service provider that uses the selected financial management systems models? • What processes will be put in place to ensure that individual component agency financial management system investment decisions focus on the benefits of standard processes and shared service providers? • What process will be used to facilitate the decision-making by component agencies to a given systems model? • How will component agencies incorporate strategic workforce planning in the migration approach and consolidation of financial management systems?
Disciplined Processes	• How can existing industry standards and best practices be incorporated into DHS-wide guidance related to financial management system implementation efforts, including migrating to shared service providers? • What actions will be taken to reduce the risks and costs associated with data conversion and interface efforts? • What oversight process will be used to ensure that modernization efforts effectively implement the prescribed policies and procedures?

Source: GAO.

Appendix IV: Disciplined Processes

Disciplined Processes Are Key to Successful Financial Management System Implementation Efforts

Disciplined processes have been shown to reduce the risks associated with software development and acquisition efforts to acceptable levels and are fundamental to successful system implementations. A disciplined software implementation process can maximize the likelihood of achieving the intended results (performance) within established resources (costs) on schedule. Although a standard set of practices that will guarantee success does not exist, several organizations, such as the Software Engineering Institute (SEI) and the Institute of Electrical and Electronic Engineers (IEEE), and individual experts have identified and developed the types of policies, procedures, and practices that have been demonstrated to reduce development time and enhance effectiveness. The key to having a disciplined system development effort is to have disciplined processes in multiple areas, including requirements management, testing, data conversion and system interfaces, configuration management, risk management, project management, and quality assurance.

Requirements Management

Requirements are the specifications that system developers and program managers use to design, develop, and acquire a system. They need to be carefully defined, consistent with one another, verifiable, and directly traceable to higher-level business or functional requirements. It is critical that they flow directly from the organization's concept of operations (how the organization's day-to-day operations are or will be carried out to meet mission needs).[1]

According to the IEEE,[2] a leader in defining the best practices for such efforts, good requirements have several characteristics, including the following:

- The requirements fully describe the software functionality to be delivered. Functionality is a defined objective or characteristic action of a system or component. For example, for grants management, a key functionality

[1] According to IEEE Std. 1362-1998, a concept of operations document is normally one of the first documents produced during a disciplined development effort since it describes system characteristics for a proposed system from the user's viewpoint. This is important since a good concept of operations document can be used to communicate overall quantitative and qualitative system characteristics to the user, developer, and other organizational elements. This allows the reader to understand the user organizations, missions, and organizational objectives from an integrated systems point of view.

[2] IEEE Std. 830-1998.

includes knowing (1) the funds obligated to a grantee for a specific purpose, (2) the cost incurred by the grantee, and (3) the funds provided in accordance with federal accounting standards.

- The requirements are stated in clear terms that allow for quantitative evaluation. Specifically, all readers of a requirement should arrive at a single, consistent interpretation of it.
- Traceability among various requirement documents is maintained. Requirements for projects can be expressed at various levels depending on user needs. They range from agencywide business requirements to increasingly detailed functional requirements that eventually permit the software project managers and other technicians to design and build the required functionality in the new system. Adequate traceability ensures that a requirement in one document is consistent with and linked to applicable requirements in another document.
- The requirements document contains all of the requirements identified by the customer, as well as those needed for the definition of the system.

Studies have shown that problems associated with requirements definition are key factors in software projects that do not meet their cost, schedule, and performance goals. Examples include the following:

- A 1988 study found that getting a requirement right in the first place costs 50 to 200 times less than waiting until after the system is implemented to get it right.[3]
- A 1994 survey of more than 8,000 software projects found that the top three reasons that projects were delivered late, over budget, and with less functionality than desired all had to do with requirements management.[4]
- A 1994 study found that, on average, there is about a 25-percent increase in requirements over a project's lifetime, which translates into at least a 25-percent increase in the schedule.[5]
- A 1997 study noted that between 40 and 60 percent of all defects found in a software project could be traced back to errors made during the requirements development stage.[6]

[3] Barry W. Boehm and Philip N. Papaccio, "Understanding and Controlling Software Costs," *IEEE Transactions on Software Engineering*, vol. 14, no. 10 (1988).

[4] The Standish Group, *Charting the Seas of Information Technology* (Dennis, Mass.: The Standish Group, 1994).

[5] Caper Jones, *Assessment and Control of Software Risks* (Englewood Cliffs, N.J.: Yourdon Press, 1994).

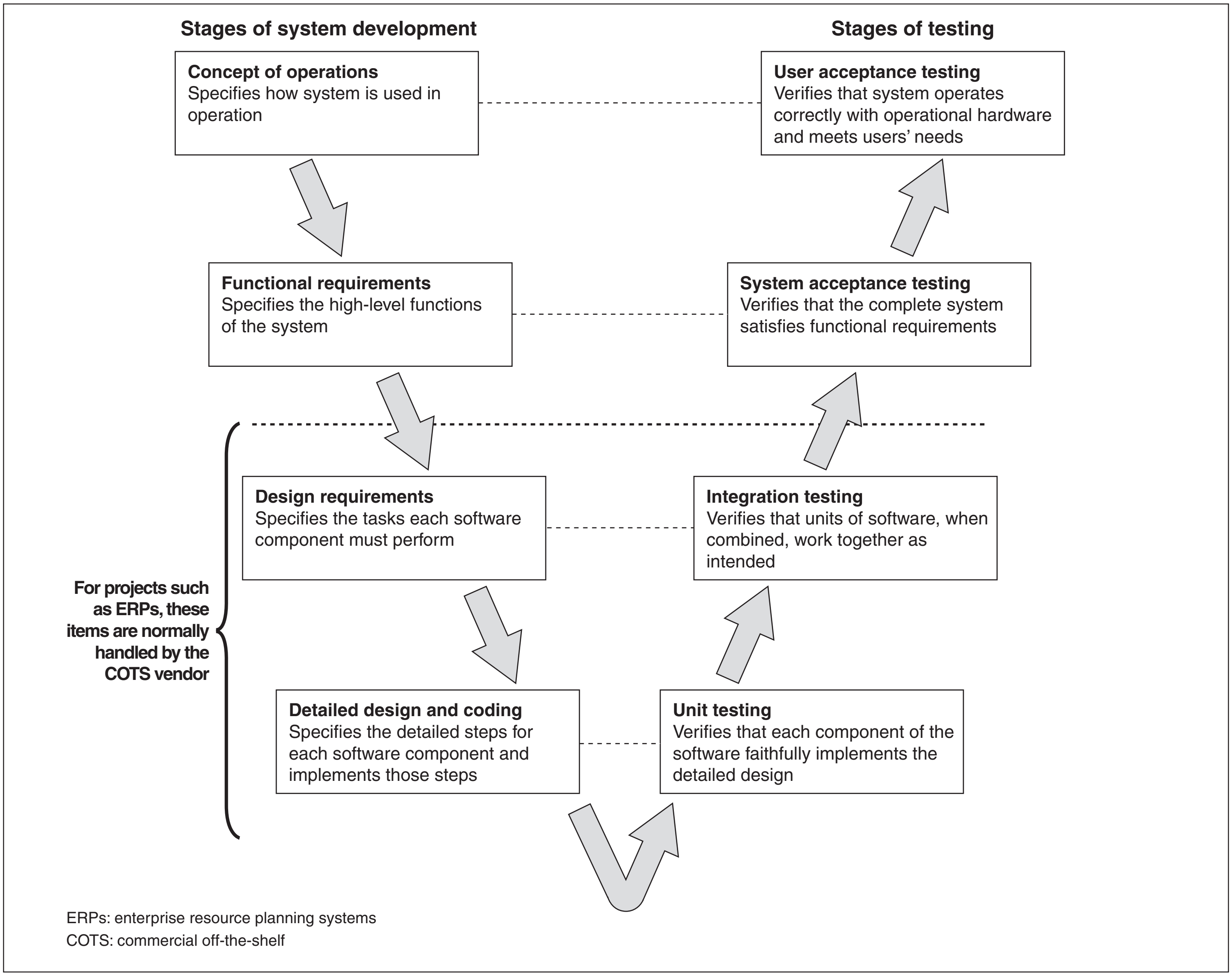
[6] Dean Leffingwell, "Calculating the Return on Investment from More Effective Requirements Management," *American Programmer* (1997).

Testing

Testing is the process of executing a program with the intent of finding errors.[7] Because requirements provide the foundation for system testing, they must be complete, clear, and well documented to design and implement an effective testing program. Absent this, an organization is taking a significant risk that substantial defects will not be detected until after the system is implemented. As shown in figure 3, there is a direct relationship between requirements and testing.

[7] Glenford J. Myers, *The Art of Software Testing* (New York: John Wiley & Sons, Inc., 1979).

Figure 3: Relationship between Requirements Development and Testing


Stages of system development
Stages of testing
Concept of operations
Specifies how system is used in operation
User acceptance testing
Verifies that system operates correctly with operational hardware and meets users' needs
Functional requirements
Specifies the high-level functions of the system
System acceptance testing
Verifies that the complete system satisfies functional requirements
For projects such as ERPs, these items are normally handled by the COTS vendor
Design requirements
Specifies the tasks each software component must perform
Integration testing
Verifies that units of software, when combined, work together as intended
Detailed design and coding
Specifies the detailed steps for each software component and implements those steps
Unit testing
Verifies that each component of the software faithfully implements the detailed design
ERPs: enterprise resource planning systems
COTS: commercial off-the-shelf

Source: GAO.

Although the actual testing occurs late in the development cycle, test planning can help disciplined activities reduce requirements-related defects. For example, developing conceptual test cases based on the requirements derived from the concept of operations and functional requirements stages can identify errors, omissions, and ambiguities long before any code is written or a system is configured. Disciplined organizations also recognize that planning the testing activities in coordination with the requirements development process has major benefits.

Although well-defined requirements are critical for implementing a successful testing program, disciplined testing efforts for projects have several characteristics,[8] which include the following:

- Testers who assume that the program has errors are likely to find a greater percentage of the defects present in the system. This is commonly called the testing mindset.
- Test plans and scripts that clearly define what the expected results should be when the test case is properly executed and the program does not have a defect that would be detected by the test case. This helps to ensure that defects are not mistakenly accepted.
- Processes that ensure test results are thoroughly inspected.
- Test cases that include exposing the system to invalid and unexpected conditions as well as the valid and expected conditions. This is commonly referred to as boundary condition testing.
- Testing processes that determine if a program has unwanted side effects. For example, a process should update the proper records correctly but should not delete other records.
- Systematic gathering, tracking, and analyzing statistics on the defects identified during testing.

Although these processes may appear obvious, they are often overlooked in testing activities.[9]

Data Conversion and System Interfaces

Data conversion is defined as the modification of existing data to enable them to operate with similar functional capability in a different environment.[10] It is one of the many critical elements necessary to successfully implement a new system. Because of the difficulty and

[8] Testing covers a variety of activities. The discussion of the testing processes in this appendix has been tailored to selected aspects of system implementation efforts and is not intended to provide a comprehensive discussion of all the processes that are required or the techniques that can be used to accomplish a disciplined testing process.

[9] Glendford J. Myers, *The Art of Software Testing.*

[10] Joint Financial Management Improvement Program, *White Paper: Financial Systems Data Conversion–Considerations* (Washington, D.C.: Dec. 20, 2002).

complexity associated with financial systems data conversion, highly skilled staff are needed. There are three primary phases in a data conversion:

(1) **Pre-conversion** activities prior to and leading up to the conversion, such as determining the scope and approach or method, developing the conversion plan, performing data cleanup and validation, ensuring data integrity, and conducting necessary analysis and testing.

(2) **Cutover** activities to convert the legacy data to the new system, such as testing system process and data edits, testing system interfaces (both incoming and outgoing), managing the critical path, supervising workload completion, and reconciliation.

(3) **Post-installation** activities such as verifying data integrity, conducting final disposition of the legacy system data, and monitoring the first reporting cycle.

There are also specific issues that apply uniquely to converting data as part of the replacement of a financial system, including

- identifying specific open transactions and balances to be established,
- analyzing and reconciling transactions for validation purposes, and
- establishing transactions and balances in the new system through an automated or manual process.

Further, consideration of various data conversion approaches and implications are important. Some considerations to be taken into account for the system conversion are the timing of the conversion (beginning-of-the-year, mid-year, or incremental) and other options such as direct or flash conversions, parallel operations, and pilot conversions. In addition, agencies should consider different data conversion options for different categories of data when determining the scope and timelines, such as

- opting not to conduct a data conversion,
- processing new transactions and activity only,
- establishing transaction balances in the new system for reporting purposes,
- converting open transactions from the legacy system, and
- recording new activity on closed prior year transactions.

Validation and adjustment of open transactions and data in the legacy system are essential prerequisites to the conversion process and have often been problematic. When data conversion is done right, the new system can flourish. However, converting data incorrectly has lengthy and long-term repercussions.

System interfaces operate on an ongoing basis, linking various systems and providing data that are critical to day-to-day operations, such as obligations, disbursements, purchase orders, requisitions, and other procurement activities. Testing the system interfaces in an end-to-end manner is necessary so agencies can have reasonable assurance that the system will be capable of providing the intended functionality. Systems that lack appropriate system interfaces often rely on manual reentry of data into multiple systems, convoluted systems, or both. According to the SEI, a widely recognized model for evaluating the interoperability of systems is the Levels of Information System Interoperability. This model focuses on the increasing levels of sophistication of system interoperability. Efforts at the highest level of this model—enterprise-based interoperability—are systems that can provide multiple users access to complex data simultaneously, data and applications are fully shared and distributed, and data have a common interpretation regardless of format. This is in contrast to the traditional interface strategies that are more aligned with the lowest level of the SEI model. Data exchanged at this level rely on electronic links that result in a simple electronic exchange of data.

Configuration Management

According to the SEI, configuration management is defined as a discipline applying technical and administrative direction and surveillance to (1) identify and document the functional and physical characteristics of a configuration item, (2) control changes to those characteristics, (3) record and report change processing and implementation status, and (4) verify compliance with specified requirements.[11] The purpose of configuration management is to establish and maintain the integrity of work products. Configuration management involves the processes of

- identifying the configuration of selected work products that compose the baselines at given points in time,
- controlling changes to configuration items,
- building or providing specifications to build work products from the configuration management system,

[11] IEEE Std. 610-1990.

- maintaining the integrity of baselines, and
- providing accurate status and current configuration data to developers, integrators, and end users.

The work products placed under configuration management include the products that are delivered to the customer, designated internal work products, acquired products, tools, and other items that are used in creating and describing these work products.

For commercial off-the-shelf (COTS) systems, configuration management focuses on ensuring that changes to the requirements or components of a system are strictly controlled to ensure the integrity and consistency of system requirements or components. Two of the key activities for configuration management include ensuring that (1) project plans explicitly provide for evaluation, acquisition, and implementation of new, often frequent, product releases[12] and (2) modification or upgrades to deployed versions of system components are centrally controlled, and unilateral user release changes are precluded. Configuration management recognizes that when using COTS products, it is the vendor, not the acquisition or implementing organization, that controls the release of new versions and that new versions are frequently released.

Risk Management

Risk and opportunity are inextricably related. Although developing software is a risky endeavor, risk management processes should be used to manage the project's risks to acceptable levels by taking the actions necessary to mitigate the adverse effects of significant risks before they threaten the project's success. If a project does not effectively manage its risks, then the risks will manage the project.

Risk management is a set of activities for identifying, analyzing, planning, tracking, and controlling risks. Risk management starts with identifying the risks before they can become problems. If this step is not performed well, then the entire risk management process may become a useless exercise since one cannot manage something that one does not know anything about. As with the other disciplined processes, risk management is designed to eliminate the effects of undesirable events at the earliest possible stage to avoid the costly consequences of rework.

[12] Donald J. Reifer, Victor R. Basili, Barry W. Boehm, and Betsy Clark, "COTS-Based Systems—Twelve Lessons Learned about Maintenance." (Presentation, 3rd International Conference on COTS-Based Software Systems, Redondo Beach, Calif., Feb. 4, 2004.)

After the risks are identified, they need to be analyzed so that they can be better understood and decisions can be made about what actions, if any, will be taken to address them. Basically, this step includes activities such as evaluating the impact on the project if the risk does occur, determining the probability of the event occurring, and prioritizing the risk against the other risks. Once the risks are analyzed, a risk management plan is developed that outlines the information known about the risks and the actions, if any, which will be taken to mitigate those risks. Risk monitoring is a continuous process because both the risks and actions planned to address identified risks need to be monitored to ensure that the risks are being properly controlled and that new risks are identified as early as possible. If the actions envisioned in the plan are not adequate, then additional controls are needed to correct the deficiencies identified.

Project Management

Effective project management is the process for planning and managing all project-related activities, such as defining how components are interrelated, defining tasks, estimating and obtaining resources, and scheduling activities. Project management allows the performance, cost, and schedule of the overall program to be continually measured, compared with planned objectives, and controlled. Project management activities include planning, monitoring, and controlling the project.

Project planning is the process used to establish reasonable plans for carrying out and managing the software project. This includes (1) developing estimates of the resources needed for the work to be performed, (2) establishing the necessary commitments, and (3) defining the plan necessary to perform the work. Effective planning is needed to identify and resolve problems as soon as possible, when it is the cheapest to fix them. According to one author, the average project expends about 80 percent of the time on unplanned rework—fixing mistakes that were made earlier in the project. Recognizing that mistakes will be made in a project is an important part of planning. According to this author, successful system development activities are designed so that the project team makes a carefully planned series of small mistakes to avoid making large, unplanned mistakes. For example, spending the time to adequately analyze three design alternatives before selecting one results in time spent analyzing two alternatives that were not selected. However, discovering that a design is inadequate after development can result in code that must be rewritten, at a cost greater than analyzing the three alternatives in the first place. This same author notes that a good rule of thumb is that each hour a developer spends reviewing project requirements and architecture saves 3 to 10 hours later in the project.[13]

Project monitoring and control help to understand the progress of the project and determine when corrective actions are needed based on the project's performance. Best business practices indicate that a key facet of project management and oversight is the ability to effectively monitor and evaluate a project's actual performance, cost, and schedule against what was planned.[14] In order to perform this critical task, the accumulation of quantitative data or metrics is required and can be used to evaluate a project's performance. An effective project management and oversight process uses quantitative data or metrics to understand matters such as (1) whether the project plan needs to be adjusted and (2) oversight actions that may be needed to ensure that the project meets its stated goals and complies with agency guidance. For example, an earned value management system is one metric that can be employed to better manage and oversee a system project.[15] An earned value management system attempts to compare the value of work accomplished during a given period with the work scheduled for that period. With ineffective project oversight, management can only respond to problems as they arise.

Agency management can also perform oversight functions, such as project reviews and participation in key meetings, to help ensure that the project will meet the agency needs. Management can use independent verification and validation reviews to provide it with assessments of the project's

[13] Steve McConnell, *Software Project Survival Guide* (Redmond, Wash.: Microsoft Press, 1998).

[14] GAO, *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722 (Washington, D.C.: July 30, 2004).

[15] According to Office of Management and Budget Circular No. A-11 § 300.4, earned value management is a project (investment) management tool that effectively integrates the investment scope of work with schedule and cost elements for optimum investment planning and control. Agencies must demonstrate use of an earned value management system that meets American National Standards Institute/ Electronic Industries Alliance Standard 748, for both government and contractor costs, for those parts of the total investment that require development efforts (e.g., prototypes and testing in the planning phase and development efforts in the acquisition phase) and show how close the investment is to meeting the approved cost, schedule, and performance goals. In addition, agencies must provide an explanation for any cost or schedule variances that are more than plus or minus 10 percent.

software deliverables and processes. Although independent of the developer, verification and validation is an integral part of the overall development program and helps management mitigate risks. This core element involves having an independent third party—such as an internal audit function or a contractor that is not involved with any of the system implementation efforts—verify and validate that the systems were implemented in accordance with the established business processes and standards. Doing so provides agencies with needed assurance about the quality of the system, which is discussed in more detail in the following section.

Quality Assurance

Quality assurance is defined as a set of procedures designed to ensure that quality standards and processes are adhered to and that the final product meets or exceeds the required technical and performance requirements. Quality assurance is a widely used approach in the software industry to improve upon product delivery and the meeting of customer requirements and expectations. The SEI indicates that quality assurance should begin in the early phases of a project to establish plans, processes, standards, and procedures that will add value to the project and satisfy the requirements of the project and the organizational policies. Quality assurance provides independent assessments, typically performed by an independent verification and validation or internal audit team, of whether management process requirements are being followed and whether product standards and requirements are being satisfied. Some of the widely used quality assurance activities include defect tracking, technical reviews, and system testing.

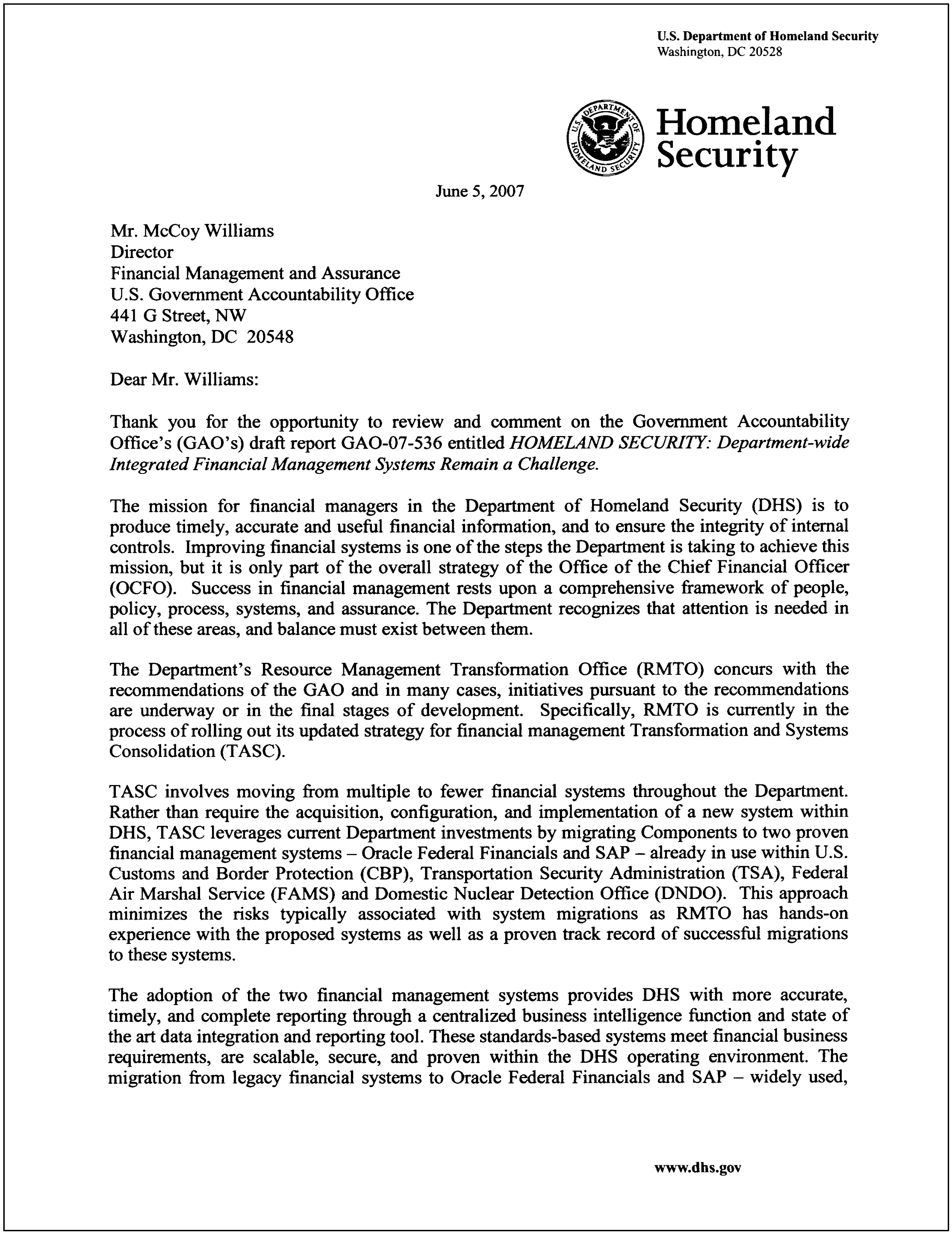
- Defect tracking---keeping a record of each defect found, its source, when it was detected, when it was resolved, how it was resolved (fixed or not), and so on.
- Technical reviews---reviewing user interface prototypes, requirements specifications, architecture, designs, and all other technical work products.
- System testing---executing software for the purpose of finding defects, typically performed by an independent test organization or quality assurance group.

According to one author, quality assurance activities might seem to result in a lot of overhead, but in actuality, exactly the opposite is true.[16] If defects can be prevented or removed early, a significant schedule benefit can be realized. For example, studies have shown that reworking defective requirements, design, and code typically consumes 40 to 50 percent of the total costs of software development projects.[17] An effective quality assurance approach is to detect as many defects as possible as early as possible to keep the costs of corrections down. However, enormous amounts of time can be saved by detecting defects earlier than during system testing.

[16] Steve McConnell, *Software Project Survival Guide.*

[17] Steve McConnell, *Rapid Development: Taming Wild Software Schedules* (Redmond, Wash.: Microsoft Press, 1996).

Appendix V: Comments from the Department of Homeland Security



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

Homeland
Security

June 5, 2007

Mr. McCoy Williams
Director
Financial Management and Assurance
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Williams:

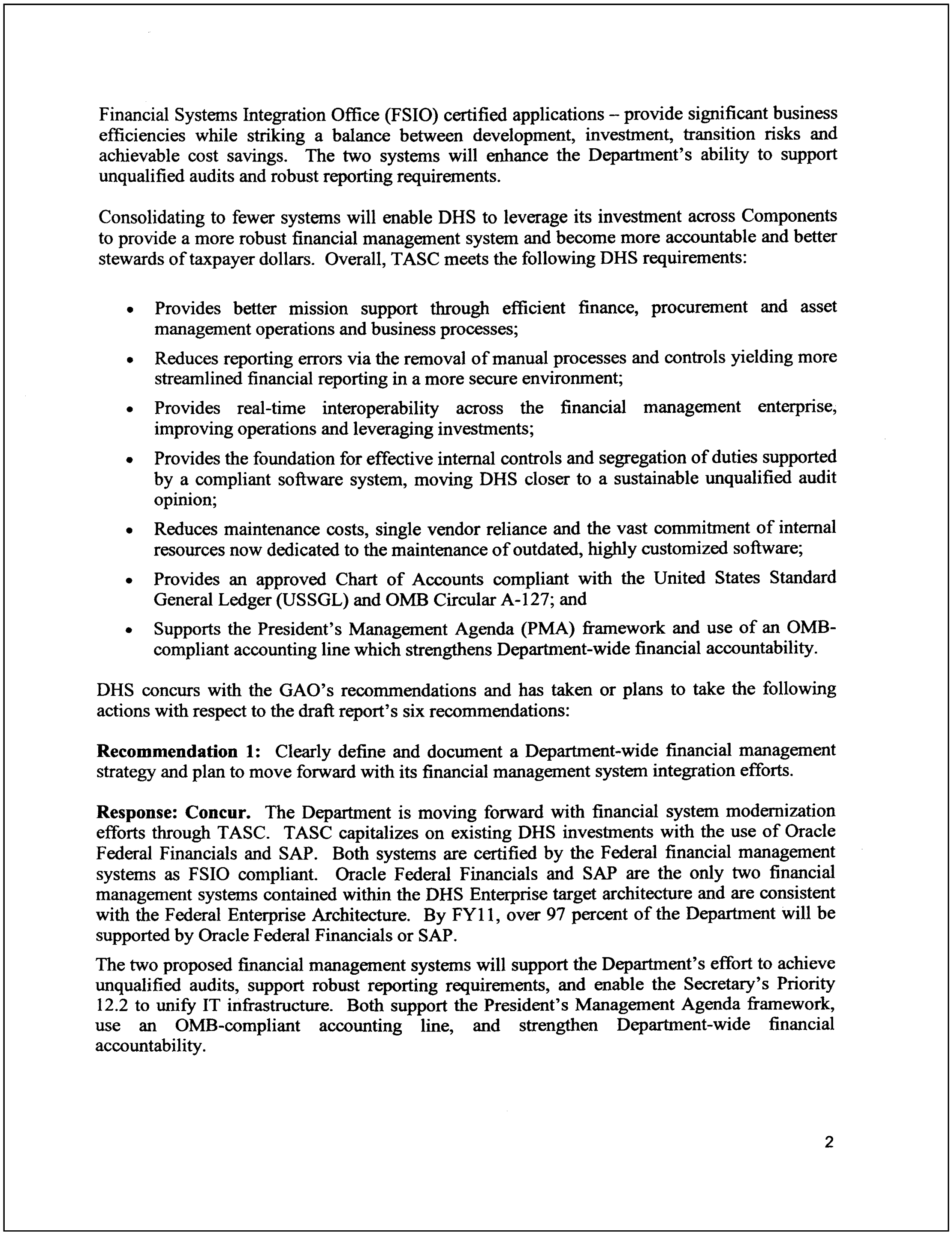
Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO's) draft report GAO-07-536 entitled *HOMELAND SECURITY: Department-wide Integrated Financial Management Systems Remain a Challenge.*

The mission for financial managers in the Department of Homeland Security (DHS) is to produce timely, accurate and useful financial information, and to ensure the integrity of internal controls. Improving financial systems is one of the steps the Department is taking to achieve this mission, but it is only part of the overall strategy of the Office of the Chief Financial Officer (OCFO). Success in financial management rests upon a comprehensive framework of people, policy, process, systems, and assurance. The Department recognizes that attention is needed in all of these areas, and balance must exist between them.

The Department's Resource Management Transformation Office (RMTO) concurs with the recommendations of the GAO and in many cases, initiatives pursuant to the recommendations are underway or in the final stages of development. Specifically, RMTO is currently in the process of rolling out its updated strategy for financial management Transformation and Systems Consolidation (TASC).

TASC involves moving from multiple to fewer financial systems throughout the Department. Rather than require the acquisition, configuration, and implementation of a new system within DHS, TASC leverages current Department investments by migrating Components to two proven financial management systems – Oracle Federal Financials and SAP – already in use within U.S. Customs and Border Protection (CBP), Transportation Security Administration (TSA), Federal Air Marshal Service (FAMS) and Domestic Nuclear Detection Office (DNDO). This approach minimizes the risks typically associated with system migrations as RMTO has hands-on experience with the proposed systems as well as a proven track record of successful migrations to these systems.

The adoption of the two financial management systems provides DHS with more accurate, timely, and complete reporting through a centralized business intelligence function and state of the art data integration and reporting tool. These standards-based systems meet financial business requirements, are scalable, secure, and proven within the DHS operating environment. The migration from legacy financial systems to Oracle Federal Financials and SAP – widely used,



Financial Systems Integration Office (FSIO) certified applications – provide significant business efficiencies while striking a balance between development, investment, transition risks and achievable cost savings. The two systems will enhance the Department's ability to support unqualified audits and robust reporting requirements.

Consolidating to fewer systems will enable DHS to leverage its investment across Components to provide a more robust financial management system and become more accountable and better stewards of taxpayer dollars. Overall, TASC meets the following DHS requirements:

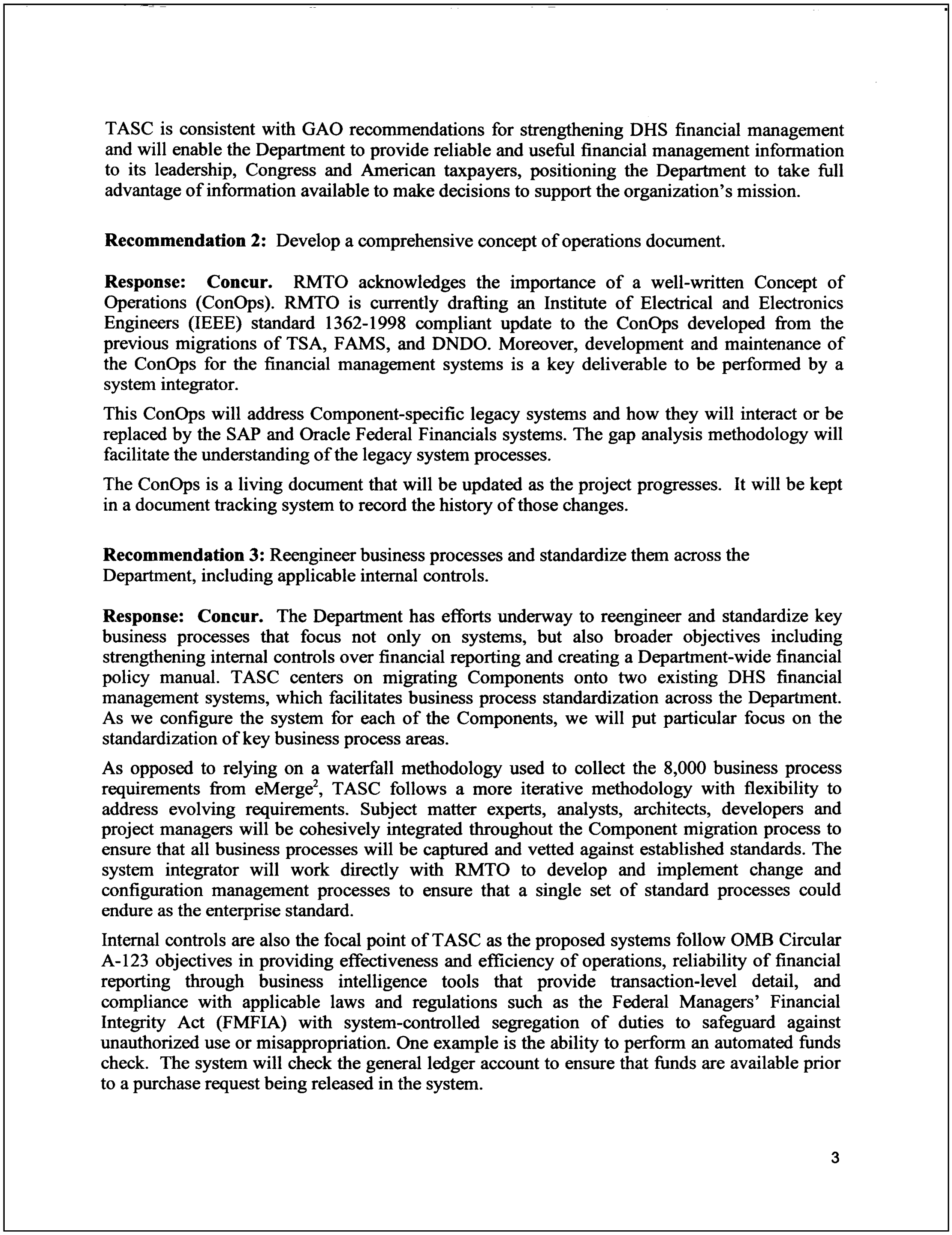
- Provides better mission support through efficient finance, procurement and asset management operations and business processes;
- Reduces reporting errors via the removal of manual processes and controls yielding more streamlined financial reporting in a more secure environment;
- Provides real-time interoperability across the financial management enterprise, improving operations and leveraging investments;
- Provides the foundation for effective internal controls and segregation of duties supported by a compliant software system, moving DHS closer to a sustainable unqualified audit opinion;
- Reduces maintenance costs, single vendor reliance and the vast commitment of internal resources now dedicated to the maintenance of outdated, highly customized software;
- Provides an approved Chart of Accounts compliant with the United States Standard General Ledger (USSGL) and OMB Circular A-127; and
- Supports the President's Management Agenda (PMA) framework and use of an OMB-compliant accounting line which strengthens Department-wide financial accountability.

DHS concurs with the GAO's recommendations and has taken or plans to take the following actions with respect to the draft report's six recommendations:

Recommendation 1: Clearly define and document a Department-wide financial management strategy and plan to move forward with its financial management system integration efforts.

Response: Concur. The Department is moving forward with financial system modernization efforts through TASC. TASC capitalizes on existing DHS investments with the use of Oracle Federal Financials and SAP. Both systems are certified by the Federal financial management systems as FSIO compliant. Oracle Federal Financials and SAP are the only two financial management systems contained within the DHS Enterprise target architecture and are consistent with the Federal Enterprise Architecture. By FY11, over 97 percent of the Department will be supported by Oracle Federal Financials or SAP.

The two proposed financial management systems will support the Department's effort to achieve unqualified audits, support robust reporting requirements, and enable the Secretary's Priority 12.2 to unify IT infrastructure. Both support the President's Management Agenda framework, use an OMB-compliant accounting line, and strengthen Department-wide financial accountability.



TASC is consistent with GAO recommendations for strengthening DHS financial management and will enable the Department to provide reliable and useful financial management information to its leadership, Congress and American taxpayers, positioning the Department to take full advantage of information available to make decisions to support the organization's mission.

Recommendation 2: Develop a comprehensive concept of operations document.

Response: Concur. RMTO acknowledges the importance of a well-written Concept of Operations (ConOps). RMTO is currently drafting an Institute of Electrical and Electronics Engineers (IEEE) standard 1362-1998 compliant update to the ConOps developed from the previous migrations of TSA, FAMS, and DNDO. Moreover, development and maintenance of the ConOps for the financial management systems is a key deliverable to be performed by a system integrator.

This ConOps will address Component-specific legacy systems and how they will interact or be replaced by the SAP and Oracle Federal Financials systems. The gap analysis methodology will facilitate the understanding of the legacy system processes.

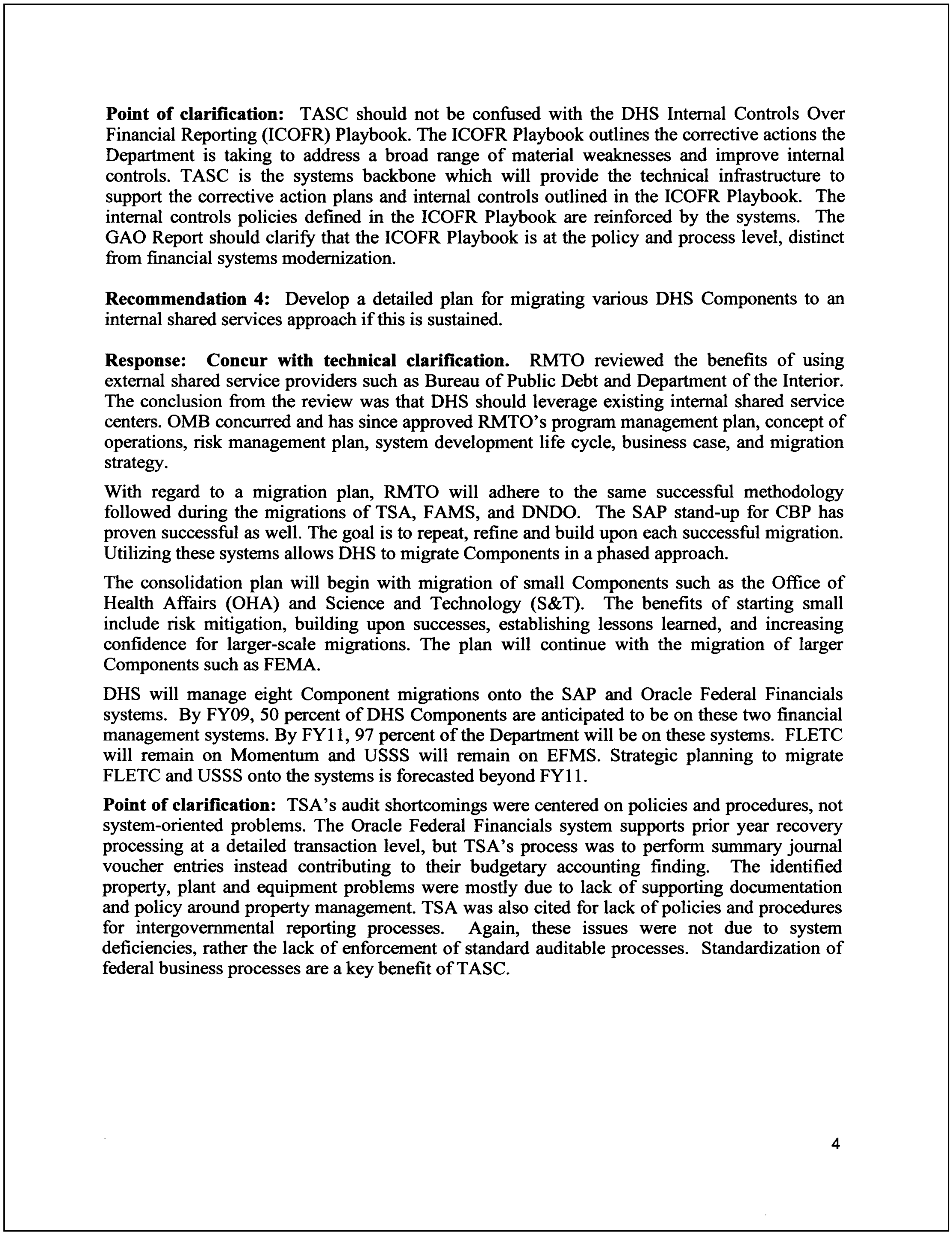
The ConOps is a living document that will be updated as the project progresses. It will be kept in a document tracking system to record the history of those changes.

Recommendation 3: Reengineer business processes and standardize them across the Department, including applicable internal controls.

Response: Concur. The Department has efforts underway to reengineer and standardize key business processes that focus not only on systems, but also broader objectives including strengthening internal controls over financial reporting and creating a Department-wide financial policy manual. TASC centers on migrating Components onto two existing DHS financial management systems, which facilitates business process standardization across the Department. As we configure the system for each of the Components, we will put particular focus on the standardization of key business process areas.

As opposed to relying on a waterfall methodology used to collect the 8,000 business process requirements from eMerge[2], TASC follows a more iterative methodology with flexibility to address evolving requirements. Subject matter experts, analysts, architects, developers and project managers will be cohesively integrated throughout the Component migration process to ensure that all business processes will be captured and vetted against established standards. The system integrator will work directly with RMTO to develop and implement change and configuration management processes to ensure that a single set of standard processes could endure as the enterprise standard.

Internal controls are also the focal point of TASC as the proposed systems follow OMB Circular A-123 objectives in providing effectiveness and efficiency of operations, reliability of financial reporting through business intelligence tools that provide transaction-level detail, and compliance with applicable laws and regulations such as the Federal Managers' Financial Integrity Act (FMFIA) with system-controlled segregation of duties to safeguard against unauthorized use or misappropriation. One example is the ability to perform an automated funds check. The system will check the general ledger account to ensure that funds are available prior to a purchase request being released in the system.



Point of clarification: TASC should not be confused with the DHS Internal Controls Over Financial Reporting (ICOFR) Playbook. The ICOFR Playbook outlines the corrective actions the Department is taking to address a broad range of material weaknesses and improve internal controls. TASC is the systems backbone which will provide the technical infrastructure to support the corrective action plans and internal controls outlined in the ICOFR Playbook. The internal controls policies defined in the ICOFR Playbook are reinforced by the systems. The GAO Report should clarify that the ICOFR Playbook is at the policy and process level, distinct from financial systems modernization.

Recommendation 4: Develop a detailed plan for migrating various DHS Components to an internal shared services approach if this is sustained.

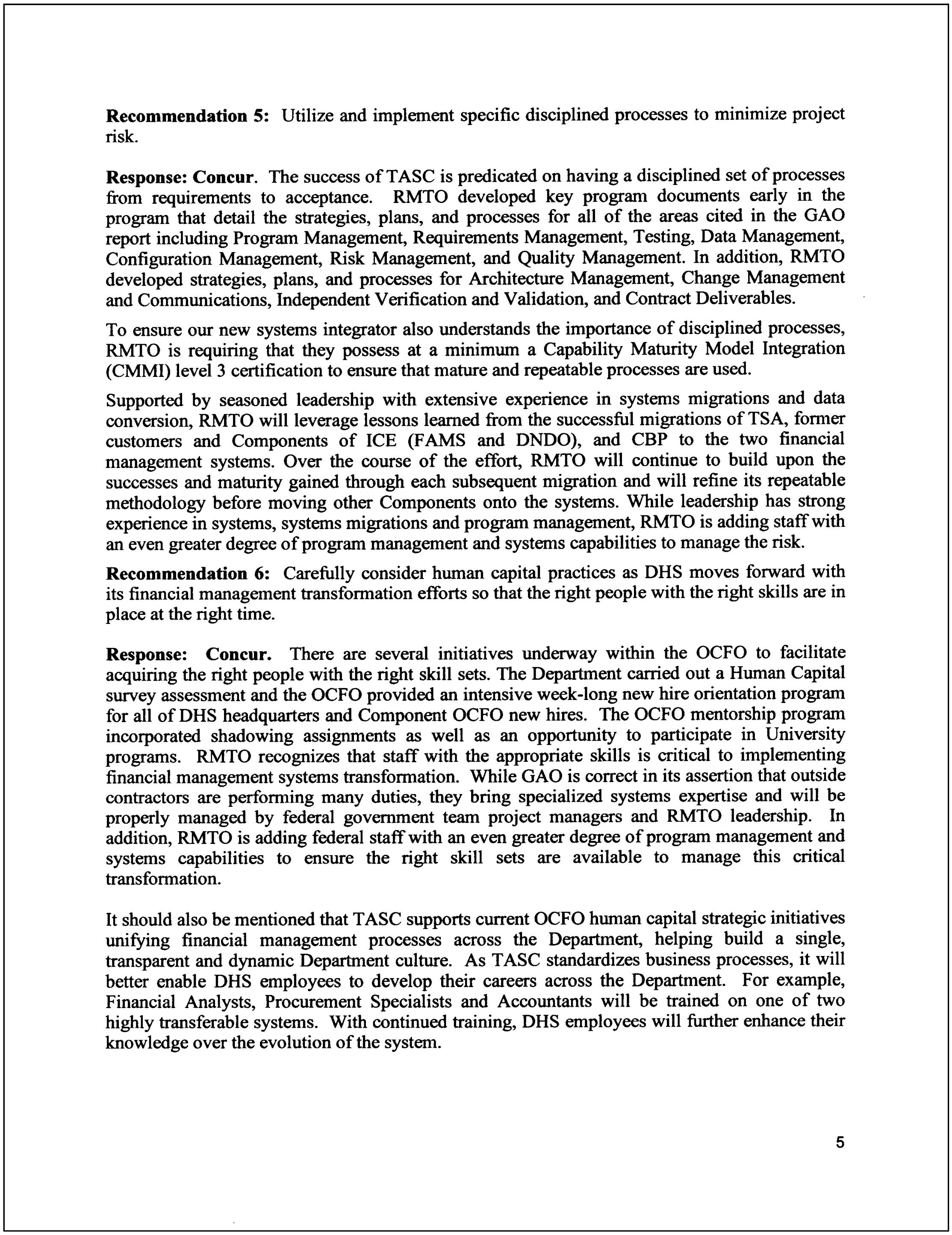
Response: Concur with technical clarification. RMTO reviewed the benefits of using external shared service providers such as Bureau of Public Debt and Department of the Interior. The conclusion from the review was that DHS should leverage existing internal shared service centers. OMB concurred and has since approved RMTO's program management plan, concept of operations, risk management plan, system development life cycle, business case, and migration strategy.

With regard to a migration plan, RMTO will adhere to the same successful methodology followed during the migrations of TSA, FAMS, and DNDO. The SAP stand-up for CBP has proven successful as well. The goal is to repeat, refine and build upon each successful migration. Utilizing these systems allows DHS to migrate Components in a phased approach.

The consolidation plan will begin with migration of small Components such as the Office of Health Affairs (OHA) and Science and Technology (S&T). The benefits of starting small include risk mitigation, building upon successes, establishing lessons learned, and increasing confidence for larger-scale migrations. The plan will continue with the migration of larger Components such as FEMA.

DHS will manage eight Component migrations onto the SAP and Oracle Federal Financials systems. By FY09, 50 percent of DHS Components are anticipated to be on these two financial management systems. By FY11, 97 percent of the Department will be on these systems. FLETC will remain on Momentum and USSS will remain on EFMS. Strategic planning to migrate FLETC and USSS onto the systems is forecasted beyond FY11.

Point of clarification: TSA's audit shortcomings were centered on policies and procedures, not system-oriented problems. The Oracle Federal Financials system supports prior year recovery processing at a detailed transaction level, but TSA's process was to perform summary journal voucher entries instead contributing to their budgetary accounting finding. The identified property, plant and equipment problems were mostly due to lack of supporting documentation and policy around property management. TSA was also cited for lack of policies and procedures for intergovernmental reporting processes. Again, these issues were not due to system deficiencies, rather the lack of enforcement of standard auditable processes. Standardization of federal business processes are a key benefit of TASC.



Recommendation 5: Utilize and implement specific disciplined processes to minimize project risk.

Response: Concur. The success of TASC is predicated on having a disciplined set of processes from requirements to acceptance. RMTO developed key program documents early in the program that detail the strategies, plans, and processes for all of the areas cited in the GAO report including Program Management, Requirements Management, Testing, Data Management, Configuration Management, Risk Management, and Quality Management. In addition, RMTO developed strategies, plans, and processes for Architecture Management, Change Management and Communications, Independent Verification and Validation, and Contract Deliverables.

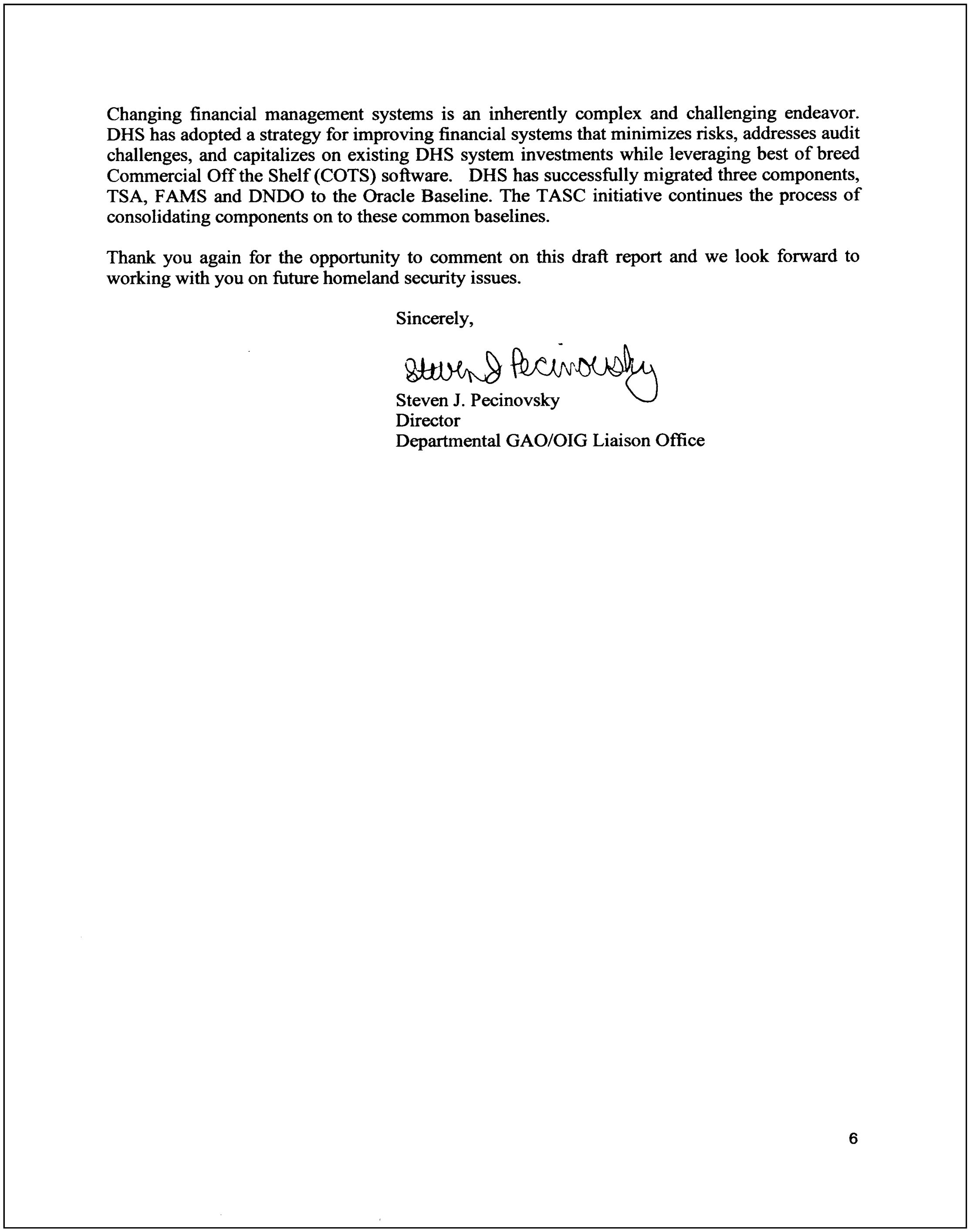
To ensure our new systems integrator also understands the importance of disciplined processes, RMTO is requiring that they possess at a minimum a Capability Maturity Model Integration (CMMI) level 3 certification to ensure that mature and repeatable processes are used.

Supported by seasoned leadership with extensive experience in systems migrations and data conversion, RMTO will leverage lessons learned from the successful migrations of TSA, former customers and Components of ICE (FAMS and DNDO), and CBP to the two financial management systems. Over the course of the effort, RMTO will continue to build upon the successes and maturity gained through each subsequent migration and will refine its repeatable methodology before moving other Components onto the systems. While leadership has strong experience in systems, systems migrations and program management, RMTO is adding staff with an even greater degree of program management and systems capabilities to manage the risk.

Recommendation 6: Carefully consider human capital practices as DHS moves forward with its financial management transformation efforts so that the right people with the right skills are in place at the right time.

Response: Concur. There are several initiatives underway within the OCFO to facilitate acquiring the right people with the right skill sets. The Department carried out a Human Capital survey assessment and the OCFO provided an intensive week-long new hire orientation program for all of DHS headquarters and Component OCFO new hires. The OCFO mentorship program incorporated shadowing assignments as well as an opportunity to participate in University programs. RMTO recognizes that staff with the appropriate skills is critical to implementing financial management systems transformation. While GAO is correct in its assertion that outside contractors are performing many duties, they bring specialized systems expertise and will be properly managed by federal government team project managers and RMTO leadership. In addition, RMTO is adding federal staff with an even greater degree of program management and systems capabilities to ensure the right skill sets are available to manage this critical transformation.

It should also be mentioned that TASC supports current OCFO human capital strategic initiatives unifying financial management processes across the Department, helping build a single, transparent and dynamic Department culture. As TASC standardizes business processes, it will better enable DHS employees to develop their careers across the Department. For example, Financial Analysts, Procurement Specialists and Accountants will be trained on one of two highly transferable systems. With continued training, DHS employees will further enhance their knowledge over the evolution of the system.



Changing financial management systems is an inherently complex and challenging endeavor. DHS has adopted a strategy for improving financial systems that minimizes risks, addresses audit challenges, and capitalizes on existing DHS system investments while leveraging best of breed Commercial Off the Shelf (COTS) software. DHS has successfully migrated three components, TSA, FAMS and DNDO to the Oracle Baseline. The TASC initiative continues the process of consolidating components on to these common baselines.

Thank you again for the opportunity to comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,

Steven J Pecinovsky

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

McCoy Williams (202) 512-9095 or williamsm1@gao.gov
Keith A. Rhodes (202) 512-6412 or rhodesk@gao.gov

Acknowledgments

In addition to the contacts named above, Kay Daly, Assistant Director; Chris Martin, Senior-Level Technologist; Chanetta Reed; Francine DelVecchio; and Felicia Brooks made key contributions to this report.

Related GAO Products

Federal Financial Management: Critical Accountability and Fiscal Stewardship Challenges Facing Our Nation. GAO-07-542T. Washington, D.C.: March 1, 2007.

Homeland Security: Applying Risk Management Principles to Guide Federal Investments. GAO-07-386T. Washington, D.C.: February 7, 2007.

Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security. GAO-07-398T. Washington, D.C.: February 6, 2007.

High-Risk Series: An Update. GAO-07-310. Washington, D.C.: January 2007.

Financial Management: Improvements Underway But Serious Financial Systems Problems Persist. GAO-06-970. Washington, D.C.: September 26, 2006.

Information Technology: Improvements Needed to More Accurately Identify and Better Oversee Risky Projects Totaling Billions of Dollars. GAO-06-1099T. Washington, D.C.: September 7, 2006.

Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation. GAO-06-831. Washington, D.C.: August 14, 2006.

Homeland Security: Progress Continues, but Challenges Remain on Department's Management of Information Technology. GAO-06-598T. Washington, D.C.: March 29, 2006.

Financial Management Systems: DHS Has an Opportunity to Incorporate Best Practices in Modernization Efforts. GAO-06-553T. Washington, D.C.: March 29, 2006.

Financial Management Systems: Additional Efforts Needed to Address Key Causes of Modernization Failures. GAO-06-184. Washington, D.C.: March 15, 2006.

CFO Act of 1990: Driving the Transformation of Federal Financial Management. GAO-06-242T. Washington, D.C.: November 17, 2005.

Information Technology: OMB Can Make More Effective Use of Its Investment Reviews. GAO-05-276. Washington, D.C.: April 15, 2005.

Financial Management: Effective Internal Control Is Key to Accountability. GAO-05-321T. Washington, D.C.: February 16, 2005.

Financial Management: Improved Financial Systems Are Key to FFMIA Compliance. GAO-05-20. Washington, D.C.: October 1, 2004.

Financial Management Systems: Lack of Disciplined Processes Puts Implementation of HHS' Financial Systems at Risk. GAO-04-1008. Washington, D.C.: September 23, 2004.

Financial Management: Department of Homeland Security Faces Significant Financial Management Challenges. GAO-04-774. Washington, D.C.: July 19, 2004.

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

Executive Guide: Creating Value Through World-class Financial Management. GAO/AIMD-00-134. Washington, D.C.: April 2000.

Standards for Internal Control in the Federal Government. GAO/AIMD-00-21.3.1. Washington, D.C.: November 1999.

(195096)

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

PRINTED ON RECYCLED PAPER