DEPARTMENT OF HOMELAND SECURITY INFORMATION TECHNOLOGY MANAGEMENT CHALLENGES AND THE FUTURE OF eMERGE2

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE, AND ACCOUNTABILITY

OF THE

COMMITTEE ON GOVERNMENT REFORM

AND THE

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

OF THE

COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 29, 2006

Serial No. 109–173
Committee on Government Reform

Serial No. 109–70
Committee on Homeland Security

Printed for the use of the Committees on Government Reform and Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

29–709 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

CHRISTOPHER SHAYS, Connecticut
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
CANDICE S. MILLER, Michigan
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina
JEAN SCHMIDT, Ohio

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
BRIAN HIGGINS, New York
ELEANOR HOLMES NORTON, District of Columbia

BERNARD SANDERS, Vermont
(Independent)

DAVID MARIN, *Staff Director*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE, AND ACCOUNTABILITY

TODD RUSSELL PLATTS, Pennsylvania, *Chairman*

VIRGINIA FOXX, North Carolina
TOM DAVIS, Virginia
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
JOHN J. DUNCAN, JR., Tennessee

EDOLPHUS TOWNS, New York
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

EX OFFICIO

HENRY A. WAXMAN, CALIFORNIA

MIKE HETTINGER, *Staff Director*
TABETHA MUELLER, *Professional Staff Member*
ERIN PHILLIPS, *Clerk*
ADAM BORDES, *Minority Professional Staff Member*

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania, *Vice Chairman*
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

MIKE ROGERS, Alabama

JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
KATHERINE HARRIS, Florida
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
PETER T. KING, New York, *Ex Officio*
KENDRICK B. MEEK, Florida
EDWARD J. MARKEY, Massachusetts
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New York
BENNIE G. THOMPSON, Mississippi, *Ex Officio*

CONTENTS

	Page
Hearing held on March 29, 2006	1
Statement of:	
Williams, McCoy, Director, Financial Management and Assurance, Government Accountability Office, accompanied by Keith A. Rhodes, Chief Technologist, Applied Research and Methods, Center for Technology and Engineering; Randolph C. Hite, Director, Information Technology Architecture and Systems Issues, U.S. Government Accountability Office; Eugene Schied, Deputy Chief Financial Officer, Department of Homeland Security; and Scott Charbo, Chief Information Officer, Department of Homeland Security	5
Charbo, Scott	70
Hite, Randolph C.	28
Schied, Eugene	68
Williams, McCoy	5
Letters, statements, etc., submitted for the record by:	
Hite, Randolph C., Director, Information Technology Architecture and Systems Issues, U.S. Government Accountability Office, prepared statement of	31
Platts, Hon. Todd Russell, a Representative in Congress from the State of Pennsylvania, prepared statement of	3
Schied, Eugene, Deputy Chief Financial Officer, Department of Homeland Security; and Scott Charbo, Chief Information Officer, Department of Homeland Security, prepared statement of	72
Thompson, Hon. Bennie G., a Representative in Congress from the State of Mississippi, prepared statement of	110
Towns, Hon. Edolphus, a Representative in Congress from the State of New York, prepared statement of	108
Williams, McCoy, Director, Financial Management and Assurance, Government Accountability Office, prepared statement of	7

DEPARTMENT OF HOMELAND SECURITY INFORMATION TECHNOLOGY MANAGEMENT CHALLENGES AND THE FUTURE OF eMERGE2

WEDNESDAY, MARCH 29, 2006

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE, AND ACCOUNTABILITY, COMMITTEE ON GOVERNMENT REFORM, JOINT WITH THE SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT, COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittees met, pursuant to notice, at 3:05 p.m., in room 2247, Rayburn House Office Building, Hon. Todd Russell Platts (chairman of the Subcommittee on Government Management, Finance, and Acountability) presiding.

Present from the Committee on Government Reform, Subcommittee on Government Management, Finance, and Accountability: Representative Platts.

Present from the Committee on Homeland Security, Subcommittee on Management, Integration, and Oversight: Representatives Rogers, Meek, and Jackson Lee.

Staff present from the Committee on Government Reform, Subcommittee on Government Management, Finance, and Accountability: Mike Hettinger, staff director; Dan Daly, counsel, Tabetha Mueller, professional staff member; Erin Phillips, clerk; Adam Bordes, minority professional staff member; and Earley Green, minority chief clerk.

Mr. PLATTS. The Government Reform Subcommittee on Government Management, Finance, and Accountability, joint with the Homeland Security Subcommittee on Management, Integration, and Oversight, will come to order.

I would first like to welcome Chairman Rogers, chairman of the Homeland Security subcommittee, for joining us in this important hearing today. We will be joined shortly by ranking members of both committees as well. And if they have opening statements at that time when they join us, we will allow them to do so or submit them for the record.

I am pleased to be holding this hearing with the other subcommittee. I want to thank Chairman Rogers and his subcommittee for their important work on these issues. Sometimes management issues are overlooked in the larger policy debate, but sound management is absolutely critical to the success of any program.

One of the primary reasons for the creation of the department was to streamline processes and realize efficiencies. In short, to spend less on overhead and more on protecting America. The effective use of information technology is a key tool in reaching that goal, and today's hearing will take an important look at the initiatives now underway at the department.

The success of eMerge2 has broad implications for the department, and the shared services model that is being employed will serve as an important test case for the Government-wide Financial Management Line of Business initiative being proposed by the Office of Management and Budget.

Proper management of information technology, the eMerge2 program in particular, is a top priority for our subcommittee, something we have followed closely for the past 3 years, and it is something we will continue to focus on.

I look forward to hearing from our witnesses here today and appreciate the work that you all do in supporting DHS.

[The prepared statement of Hon. Todd Russell Platts follows:]

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE, AND ACCOUNTABILITY

TODD RUSSELL PLATTS, CHAIRMAN

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

MICHAEL D. ROGERS, CHAIRMAN

OVERSIGHT HEARING:

"Department of Homeland Security Information Technology Challenges and the Future of eMerge^2"

Wednesday, March 29, 2006, 3:00 PM
2247 Rayburn House Office Building

OPENING STATEMENT OF CHAIRMAN PLATTS

I would first like to welcome Chairman Rogers, Ranking Member Meek and the other Members of the Homeland Security Subcommittee on Management, Integration, and Oversight. Thank you for holding this joint hearing today and for your important work with these issues. Sometimes management issues are overlooked in the larger policy debate, but sound management is absolutely critical to the success of any program.

One of the primary reasons for the creation of the Department was to streamline processes and realize efficiencies – in short, to spend less on overhead and more on protecting America. The effective use of information technology is a key tool in reaching that goal, and today's hearing will take an important look at the initiatives now underway at the Department. The success of eMerge^2 has broad implications for the Department, and the shared services model that is being employed will serve as an important test case for the government-wide Financial Management Line of Business initiative being proposed by the Office of Management and Budget. Proper management of information technology – the eMerge^2 program in particular – is a top priority for our Subcommittee, something we have followed closely for the past three years and something we will continue to focus on.

I look forward to hearing from our witnesses and appreciate the work you do to support DHS.

Mr. PLATTS. I now have the pleasure of recognizing the chairman of the Homeland Security subcommittee, Chairman Rogers.

Mr. ROGERS. Thank you.

Today, we are holding a joint hearing to examine the status of the department's financial management resources and the integration of its information technology systems.

I would first like to thank Chairman Platts and Ranking Member Towns for working with us on this hearing today. Our two subcommittees do share a common goal of strengthening the department's financial management while safeguarding taxpayer dollars.

I would also like to welcome our panel of distinguished witnesses and thank them for being here today. I know you are busy, and it is very kind of you to take the time to be with us.

When the department was formed in March 2003, it inherited 19 different financial management systems. Through consolidation, that number is now down to eight. In 2004, the department announced a new initiative referred to as eMerge2. This effort would bring the entire department under one centralized financial management system.

To accomplish this, DHS has spent approximately $18 million to begin the program, which was estimated to cost over $229 million. Late last year, however, the department abruptly canceled the contract and shifted the direction of eMerge2.

Today, we hope to hear what went wrong with the contract, what, if anything, the department received for its $18 million, and what the department plans for the future of eMerge2. We also will examine the steps the department is taking to integrate its information systems.

I was disappointed to see, for example, that the department had recently received an "F" on the Government Reform Committee's annual computer security scoreboard for the 3rd year. Today, I hope we will find out why that grade hasn't improved.

And with that, I will be happy to yield back to Chairman Platts, and thank you again for this joint hearing.

Mr. PLATTS. Thank you, Chairman Rogers.

And we will proceed to our witnesses. We are pleased to have four distinguished guests with us today as part of this hearing. As part of our process here of the subcommittee, we would ask all four of you to first stand and be sworn in.

[Witnesses sworn.]

Mr. PLATTS. Thank you. You may be seated.

A clerk will note that the witnesses affirmed the oath.

We are pleased to have with us, first, Mr. McCoy Williams, Director of Financial Management and Assurance, the Government Accountability Office; Mr. Randy Hite, Director, Information Technology Architecture and Systems, Government Accountability Office; Mr. Eugene Schied, Acting Chief Financial Officer, Department of Homeland Security; and Mr. Scott Charbo, Chief Information Officer, Department of Homeland Security.

All four of your written testimonies have been submitted for the record. And again, we appreciate you being here with us.

Mr. Williams, we are going to start with you, if you would like to proceed with your opening statement?

STATEMENTS OF McCOY WILLIAMS, DIRECTOR, FINANCIAL MANAGEMENT AND ASSURANCE, GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY KEITH A. RHODES, CHIEF TECHNOLOGIST, APPLIED RESEARCH AND METHODS, CENTER FOR TECHNOLOGY AND ENGINEERING; RANDOLPH C. HITE, DIRECTOR, INFORMATION TECHNOLOGY ARCHITECTURE AND SYSTEMS ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; EUGENE SCHIED, DEPUTY CHIEF FINANCIAL OFFICER, DEPARTMENT OF HOMELAND SECURITY; AND SCOTT CHARBO, CHIEF INFORMATION OFFICER, DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF McCOY WILLIAMS

Mr. WILLIAMS. Thank you.

Mr. Chairmen, it is a pleasure to be here today to participate in this joint oversight hearing on the Department of Homeland Security's ongoing efforts to effectively manage its information technology projects.

Today, we would like to provide our perspectives on the importance of DHS following best practices in developing and implementing its new financial management systems.

Specifically, we would like to discuss the recurring problems we and others have identified in agencies' financial management systems development and implementation efforts, point out key financial management system modernization challenges at DHS, highlight the building blocks that form the foundation for successful financial management system implementation efforts.

First, our work and that of the IGs over the years has shown that agencies have failed to employ accepted best practices and systems development and implementation that can collectively reduce the risk associated with implementing financial systems. These are commonly referred to as disciplined processes.

In our recently issued report, we identified key causes of failures related to disciplined processes, such as requirements management, testing, and project management. As a case in point, we recently reported that the initial deployment of a $1 billion Army system intended to improve depot operations was still not meeting users' needs. One reason was a breakdown in the requirements management process.

Agencies have also faced challenges in implementing financial management systems due to human capital management issues related to strategic work force planning, human resources, and change management. By not identifying the right people with the right skills, agencies reduce their chances of successfully implementing and operating new financial management systems. For example, we identified human capital problems in systems projects at IRS, HHS, and VA.

Second, DHS faces unique challenges in attempting to develop integrated financial management systems across the breadth of such a large and diverse department. DHS inherited a number of redundant financial management systems from 22 diverse agencies. Among the weaknesses identified in prior financial audits were insufficient internal controls or processes to reliably report basic financial information.

According to DHS officials, they recently decided to change the direction of eMerge2 project, which was supposed to consolidate and integrate the department's financial accounting and reporting systems. DHS's revised shared services approach will allow DHS components to choose from existing financial management service providers, mainly from within DHS.

Third, based on industry best practices, we have identified four key concepts that we believe will be critical to DHS's ability to successfully complete its planned migration to financial management shared services providers.

The four concepts are developing a concept of operations, defining standard business processes, developing a strategy for implementing DHS's approach across the department, and defining and effectively implementing disciplined processes. Careful consideration of these four concepts, each one building upon the next, will be integral to the success of DHS's strategy.

In closing, with DHS at an important crossroads in implementing financial management systems, it has an excellent opportunity to use these building blocks to form a solid foundation on which to base its efforts and avoid the problems that have plagued so many other Federal agencies.

This concludes our statement. We will be pleased to answer any questions.

Thank you.

[The prepared statement of Mr. Williams follows:]

United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees

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

FINANCIAL MANAGEMENT SYSTEMS

DHS Has an Opportunity to Incorporate Best Practices in Modernization Efforts

Statement of McCoy Williams
Director, Financial Management and Assurance

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

GAO-06-553T

March 29, 2006

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-06-553T, a testimony before congressional subcommittees

FINANCIAL MANAGEMENT SYSTEMS

DHS Has an Opportunity to Incorporate Best Practices in Modernization Efforts

Why GAO Did This Study

Over the years, GAO has reported on various agencies' financial management system implementation failures. GAO's recent report (GAO-06-184) discusses some of the most significant problems previously identified with agencies' financial management system modernization efforts. For today's hearing, GAO was asked to provide its perspectives on the importance of the Department of Homeland Security (DHS) following best practices in developing and implementing its new financial management systems and avoiding the mistakes of the past. GAO's testimony (1) discusses the recurring problems identified in agencies' financial management systems development and implementation efforts, (2) points out key financial management system modernization challenges at DHS, and (3) highlights the building blocks that form the foundation for successful financial management system implementation efforts.

www.gao.gov/cgi-bin/getrpt?GAO-06-553T.

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.

What GAO Found

GAO's work and that of agency inspectors general over the years has shown that agencies have failed to employ accepted best practices in systems development and implementation (commonly referred to as disciplined processes) that can collectively reduce the risk associated with implementing financial management systems. GAO's recent report identified key causes of failures within several recurring themes including (1) disciplined processes, such as requirements management, testing, and project management; and (2) human capital management, such as workforce planning, human resources, and change management. Prior reports have identified costly systems implementation failures attributable to problems in these areas at agencies across the federal government.

DHS faces unique challenges in attempting to develop integrated financial management systems across the breadth of such a large and diverse department. DHS inherited a myriad of redundant financial management systems from 22 diverse agencies and about 100 resource management systems. Among the weaknesses identified in prior component financial audits were insufficient internal controls or processes to reliably report financial information such as revenue, accounts receivable, and accounts payable; significant system security deficiencies; financial systems that required extensive manual processes to prepare financial statements; and incomplete policies and procedures necessary for conducting basic financial management activities. In August 2003, DHS began a program to consolidate and integrate DHS financial accounting and reporting systems. DHS officials said they recently decided to develop a new strategy for the planned financial management systems integration program, referred to as eMerge^2, because the prior strategy was not meeting its performance goals and timeline. DHS's revised strategy will allow DHS components to choose from an array of existing financial management shared service providers.

Based on industry best practices, GAO identified four key concepts that will be critical to DHS's ability to successfully complete its planned migration to shared service providers. Careful consideration of these four concepts, each one building upon the next, will be integral to the success of DHS's strategy. The four concepts are

- developing a concept of operations,
- defining standard business processes,
- developing a strategy for implementing DHS's shared services approach across the department, and
- defining and effectively implementing disciplined processes necessary to properly manage the specific projects.

With DHS at an important crossroads in implementing financial management systems, it has an excellent opportunity to use these building blocks to form a solid foundation on which to base its efforts and avoid the problems that have plagued so many other federal agencies.

Mr. Chairmen and Members of the Subcommittees:

It is a pleasure to be here today to participate in this joint oversight hearing[1] on the Department of Homeland Security's (DHS) ongoing efforts to effectively manage its information technology (IT) projects. Modern financial management systems are a critical component to instituting strong financial management as called for by the Chief Financial Officers (CFO) Act of 1990, the Federal Financial Management Improvement Act of 1996 (FFMIA), and other legislation. As we testified[2] in November 2005, agencies continue to struggle with developing and implementing integrated systems that achieve expected functionality within cost and timeliness goals. While most CFO Act agencies have obtained clean (or unqualified) audit opinions on their financial statements, the underlying financial systems remain a serious problem. Hearings such as this one today foster meaningful financial management reform.

Over the years, we have reported on various agencies' financial management system implementation failures. Our recent report,[3] which was prepared at the request of the Subcommittee on Government Management, Finance, and Accountability, House Committee on Government Reform, discusses some of the most significant problems and observations we identified with agencies' financial management system modernization efforts. Today, we would like to provide our perspectives on the importance of DHS following best practices in developing and implementing its new financial management systems. Specifically, we would like to

- discuss the recurring problems we and others have identified in agencies' financial management systems development and implementation efforts,
- point out key financial management system modernization challenges at DHS, and

[1]Joint hearing held by the Subcommittee on Government Management, Finance, and Accountability, House Committee on Government Reform and the Subcommittee on Management, Integration, and Oversight, House Committee on Homeland Security.

[2]GAO, *CFO Act of 1990: Driving the Transformation of Federal Financial Management*, GAO-06-242T (Washington, D.C.: Nov. 17, 2005).

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

- highlight the building blocks that form the foundation for successful financial management system implementation efforts.

Our statement is based upon our recently issued report,[4] as well as our previous reports and testimonies, which were performed in accordance with U.S. generally accepted government auditing standards. We have not performed a detailed review of DHS's financial management transformation efforts.

Lessons Learned in Recurring Failures of Federal Agency Financial Management System Implementations

In our recent report,[5] we summarize many of the agencies' financial management system implementation failures that have been previously reported by us and inspectors general (IG). Our work and that of the IGs over the years has shown that agencies have failed to employ accepted best practices in systems development and implementation (commonly referred to as disciplined processes) that can collectively reduce the risk associated with implementing financial management systems. In our report, we identified key causes of failures within several recurring themes, including disciplined processes and human capital management. DHS would be wise to study the lessons learned through other agencies' costly failures and consider building a strong foundation for successful financial management system implementation, as we will discuss later in our testimony.

Disciplined Processes Have Not Been Fully Employed

From our review of over 40 prior reports, we identified weaknesses in the following areas of disciplined processes.

- **Requirements management.** Ill-defined or incomplete requirements have been identified by many system developers and program managers as a root cause of system failure.[6] It is critical that requirements—functions the system must be able to perform—be carefully defined and flow from the concept of operations (how the organization's day-to-day operations are or will be carried out to meet mission needs). In our previous work, we have found agencies with a lack of a concept of operations, vague and

[4]GAO-06-184.

[5]GAO-06-184.

[6]Requirements are the blueprint that system developers and program managers use to design and develop a system.

ambiguous requirements, and requirements that are not traceable or linked to business processes.

- **Testing**. Complete and thorough testing is essential to provide reasonable assurance that new or modified systems will provide the capabilities in the requirements. 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. Industry best practices indicate that the sooner a defect is recognized and corrected, the cheaper it is to fix. In our work, we have found flawed test plans, inadequate timing of testing, and ineffective systems testing.

- **Data conversion**. In its white paper[8] on financial system data conversion,[9] the Joint Financial Management Improvement Program (JFMIP)[10] identified data conversion as one of the critical tasks necessary to successfully implement a new financial system. JFMIP also noted that if data conversion is done right, the new system has a much greater opportunity for success. On the other hand, converting data incorrectly or entering unreliable data from a legacy system has lengthy and long-term repercussions. The adage "garbage in, garbage out" best describes the adverse impact. Examples of problems we have reported on include agencies that have not properly developed and implemented good data conversion plans, have planned the data conversion too late in the project, and have not reconciled account balances.

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

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

[9]Data conversion is defined as the modification of existing data to enable it to operate with similar functional capability in a different environment.

[10]JFMIP was originally formed under the authority of the Budget and Accounting Procedures Act of 1950 and was a joint and cooperative undertaking of GAO, the Department of the Treasury, the Office of Management and Budget (OMB), and the Office of Personnel Management (OPM), working in cooperation with each other to improve financial management practices in the federal government. In a December 2004 memorandum, OMB announced a realignment of JFMIP's responsibilities for financial management policy and oversight in the federal government. JFMIP ceased to exist as a separate organization, although the Principals will continue to meet at their discretion.

- **Risk management**. According to leading systems acquisition organizations, risk management is a process for identifying potential problems before they occur and adjusting the acquisition to decrease the chance of their occurrence. Risks should be identified as early as possible and a risk management process should be developed and put in place. Risks should be identified, analyzed, mitigated, and tracked to closure. Effectively managing risks is one way to minimize the chances of project cost, schedule, and performance problems from occurring. We have reported that agencies have not fully implemented effective risk management practices, including shortcomings in identifying and tracking risks.

- **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. We have reported on a number of project management problems including inadequate project management structure, schedule-driven projects, and lack of performance metrics and oversight.

- **Quality assurance**. Quality assurance provides independent assessments of whether management process requirements are being followed and whether product standards and requirements are being satisfied. This process includes, among other things, the use of independent verification and validation (IV&V). We and others have reported on problems related to agencies' use of IV&V including specific functions not being performed by the IV&V, the IV&V contractor not being independent, and IV&V recommendations not being implemented.

Inadequate implementation of disciplined processes can manifest itself in many ways when implementing a financial management system. While full deployment has been delayed at some agencies, specific functionality has been delayed or flawed at other agencies. The following examples illustrate some of the recurring problems related to the lack of disciplined processes in implementing financial management systems.

- In May 2004, we reported[11] significant flaws in requirements management and testing that adversely affected the initial development and implementation of the Army's Logistics Modernization Program (LMP), in which the Army estimated that it would invest about $1 billion. These flaws also hampered efforts to correct the operational difficulties experienced at the Tobyhanna Army Depot. In June 2005, we reported[12] that the Army had not effectively addressed its requirements management and testing problems, and data conversion weaknesses had hampered the Army's ability to address the problems that needed to be corrected before the system could be fielded to other locations. The Army lacked reasonable assurance that (1) system problems experienced during the initial deployment and causing the delay of future deployments had been corrected and (2) LMP was capable of providing the promised system functionality. Subsequent deployments of the system have been delayed.

- We reported[13] in February 2005 that our experience with major systems acquisitions, such as the Office of Personnel Management's (OPM) Retirement Systems Modernization (RSM) program, has shown that having sound disciplined processes in place increases the likelihood of the acquisitions meeting cost and schedule estimates as well as performance requirements. However, we found that many of the processes in these areas for RSM were not sufficiently developed, were still under development, or were planned for future development. For example, OPM lacked needed processes for developing and managing requirements, planning and managing project activities, managing risks, and providing sound information to investment decision makers. Without these processes in place, RSM was at increased risk of not being developed and delivered on time and within budget and falling short of promised capabilities.

[11]GAO, *DOD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability*, GAO-04-615 (Washington, D.C.: May 27, 2004).

[12]GAO, *Army Depot Maintenance: Ineffective Oversight of Depot Maintenance Operations and System Implementation Efforts*, GAO-05-441 (Washington, D.C.: June 30, 2005).

[13]GAO, *Office of Personnel Management: Retirement Systems Modernization Program Faces Numerous Challenges*, GAO-05-237 (Washington, D.C.: Feb. 28, 2005).

- In August 2004, the Department of Veterans Affairs (VA) IG reported[14] that the effect of transferring inaccurate data to VA's new core financial system at a pilot location interrupted patient care and medical center operations. This raised concerns that similar conversion problems would occur at other VA facilities if the conditions identified were not addressed and resolved nationwide prior to roll out. Some of the specific conditions the IG noted were that contracting and monitoring of the project were not adequate, and the deployment of the new system encountered multiple problems, including those related to software testing, data conversion and system interfaces, and project management. As a result of these problems, patient care was interrupted by supply outages and other problems. The inability to provide sterile equipment and needed supplies to the operating room resulted in the cancelation of 81 elective surgeries for a week in both November 2003 and February 2004. In addition, the operating room was forced to operate at two-thirds of its prior capacity. Because of the serious nature of the problems raised with the new system, VA management decided to focus on transitioning back to the previous financial management software at the pilot location and assembled a senior leadership team to examine the results of the pilot and make recommendations to the VA Secretary regarding the future of the system.

Human Capital Management Problems Impede Financial Systems Development and Deployment

We are concerned that federal agencies' human capital problems are eroding the ability of many agencies—and threatening the ability of others—to perform their IT missions economically, efficiently, and effectively. For example, we found[15] that in the 1990s, the initial rounds of downsizing were set in motion without considering the longer-term effects on agencies' IT performance capacity. Additionally, a number of individual agencies drastically reduced or froze their hiring efforts for extended periods. Consequently, following a decade of downsizing and curtailed investments in human capital, federal agencies currently face skills, knowledge, and experience imbalances, especially in their IT workforces. Without corrective action, these imbalances will worsen, especially in light of the numbers of federal civilian workers becoming eligible to retire in the coming years. In this regard, we are emphasizing the need for

[14]Department of Veterans Affairs Office of Inspector General, *Issues at VA Medical Center Bay Pines, Florida and Procurement and Deployment of the Core Financial and Logistics System*, Report 04-01371-177 (Washington, D.C.: Aug. 11, 2004).

[15]GAO, *Human Capital: Building the Information Technology Workforce to Achieve Results*, GAO-01-1007T (Washington, D.C.: July 31, 2001).

additional focus on the following three key elements of human capital management.

- **Strategic workforce planning**. Having staff with the appropriate skills is key to achieving financial management improvements, and managing an organization's employees is essential to achieving results. It is important that agencies incorporate strategic workforce planning by (1) aligning an organization's human capital program 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. This incorporates a range of activities from identifying and defining roles and responsibilities, to identifying team members, to developing individual competencies that enhance performance. We have reported on agencies without a sufficient human capital strategy or plan, skills gap analysis, or training plans.

- **Human resources**. Having sufficient numbers of people on board with the right mix of knowledge and skills can make the difference between success and failure. This is especially true in the IT area, where widespread shortfalls in human capital have contributed to demonstrable shortfalls in agency and program performance. We have found agency projects with significant human resource challenges, including addressing personnel shortages, filling key positions, and developing and retaining staff with the required competencies.

- **Change management**. According to leading IT organizations, organizational change management is the process of preparing users for the business process changes that will accompany implementation of a new system. An effective organizational change management process includes project plans and training that prepare users for impacts the new system might have on their roles and responsibilities and a process to manage those changes. We have reported on various problems with agencies' change management, including transition plans not being developed, business processes not being reengineered, and customization not being limited.

The following examples illustrate some of the recurring problems related to human capital management in implementing financial management systems.

- We first reported in February 2002[16] that the Internal Revenue Service (IRS) had not defined or implemented an IT human capital strategy for its Business Systems Modernization (BSM) program and recommended that IRS address this weakness. In June 2003, we reported[17] that IRS had made important progress in addressing our recommendation, but had yet to develop a comprehensive multiyear workforce plan. IRS also had not hired, developed, or retained sufficient human capital resources with the required competencies, including technical skills, in specific mission areas. In September 2003, the Treasury Inspector General for Tax Administration reported[18] that IRS's Modernization and IT Services organization had made significant progress in developing its human capital strategy but had not yet (1) identified and incorporated human capital asset demands for the modernized organization, (2) developed detailed hiring and retention plans, or (3) established a process for reviewing the human capital strategy development and monitoring its implementation. We most recently reported in July 2005[19] that IRS had taken some steps in the right direction. However, until IRS fully implements its strategy, it will not have all of the necessary IT knowledge and skills to effectively manage the BSM program or to operate modernized systems. Consequently, the risk of BSM program and project cost increases, schedule slippages, and performance problems is increased.

- We reported, in September 2004,[20] that staff shortages and limited strategic workforce planning resulted in the Department of Health and Human Services (HHS) not having the resources needed to effectively design and operate its new financial management system. HHS had taken the first

[16]GAO, *Business Systems Modernization: IRS Needs to Better Balance Management Capacity with Systems Acquisition Workload*, GAO-02-356 (Washington, D.C.: Feb. 28, 2002).

[17]GAO, *Business Systems Modernization: IRS Has Made Significant Progress in Improving Its Management Controls, but Risks Remain*, GAO-03-768 (Washington, D.C.: June 27, 2003).

[18]Treasury Inspector General for Tax Administration, *The Modernization, Information Technology and Security Services Organization Needs to Take Further Action to Complete Its Human Capital Strategy*, Reference Number 2003-20-209 (Washington, D.C.: Sept. 22, 2003).

[19]GAO, *Business Systems Modernization: Internal Revenue Service's Fiscal Year 2005 Expenditure Plan*, GAO-05-774 (Washington, D.C.: July 22, 2005).

[20]GAO, *Financial Management Systems: Lack of Disciplined Processes Puts Implementation of HHS's Financial System at Risk*, GAO-04-1008 (Washington, D.C.: Sept. 23, 2004).

steps in strategic workforce planning. For example, the Centers for Disease Control and Prevention (CDC), where the first deployment was scheduled, was the only operating division that had prepared a competency report, but a skills gap analysis and training plan for CDC had not been completed. In addition, many government and contractor positions on the implementation project were not filled as planned. While HHS and the systems integrator had taken measures to acquire additional human resources for the implementation of the new financial management system, we concluded that scarce resources could significantly jeopardize the project's success and lead to several key deliverables being significantly behind schedule. In September 2004, HHS decided to delay its first scheduled deployment at CDC by 6 months in order to address these and other issues.

DHS Faces Serious Financial Management Challenges

DHS faces unique challenges in attempting to develop integrated financial management systems across the breadth of such a large and diverse department. DHS was established by the Homeland Security Act of 2002,[21] as the 15th Cabinet Executive Branch Department of the United States government. DHS inherited a myriad of redundant financial management systems from 22 diverse agencies along with 180,000 employees, about 100 resource management systems, and 30 reportable conditions[22] identified in prior component financial audits. Of the 30 reportable conditions, 18 were so severe they were considered material weaknesses.[23] Among these weaknesses were insufficient internal controls or processes to reliably report financial information such as revenue, accounts receivable, and accounts payable; significant system security deficiencies; financial systems that required extensive manual processes to prepare financial statements; and incomplete policies and procedures necessary to complete basic financial management activities.

[21]Pub. L. No. 107-296, § 101(a), 116 Stat. 2135, 2142 (Nov. 25, 2002) (*codified at* 6 U.S.C. § 111(a)).

[22]Under standards issued by the American Institute of Certified Public Accountants, "reportable conditions" are matters coming to the auditors' attention relating to significant deficiencies in the design or operation of internal control 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.

[23]Material weaknesses are reportable conditions 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 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.

DHS received a disclaimer of opinion on its financial statements for fiscal year 2005,[24] and the independent auditors also reported that DHS's financial management systems did not substantially comply with the requirements of FFMIA. The disclaimer was primarily due to financial reporting problems at five components. The five components include Immigration and Customs Enforcement (ICE), the United States Coast Guard (Coast Guard), State and Local Government Coordination and Preparedness (SLGCP),[25] the Transportation Security Administration (TSA), and Emergency Preparedness and Response (EPR). Further, ICE is an accounting service provider for other DHS components, and it failed to adequately maintain both its own accounting records and those of other DHS components during fiscal year 2005.

The auditors' fiscal year 2005 report discusses 10 material weaknesses, two other reportable conditions in internal control, and instances of noncompliance with seven laws and regulations. Among the 10 material weaknesses were inadequate financial management and oversight at DHS components, primarily ICE and Coast Guard; decentralized financial reporting at the component level; significant general IT and application control weaknesses over critical financial and operational data; and the lack of accurate and timely reconciliation of fund balance with treasury accounts. The results of the auditors' tests of fiscal year 2005 compliance with certain provisions of laws, regulations, contracts, and grant agreements disclosed instances of noncompliance. The DHS auditors reported instances of noncompliance with

- 31 U.S.C. § 3512(c),(d), commonly known as the Federal Managers' Financial Integrity Act of 1982 (FMFIA);
- the Federal Financial Management Improvement Act of 1996 (FFMIA), Pub. L. No. 104-208, div. A, § 101(f), title VIII, 110 Stat. 3009, 3009-389 (Sept. 30, 1996);
- the Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (Dec. 17, 2002);

[24]Office of Inspector General, *Independent Auditors' Report on DHS' FY 2005 Financial Statements* (Nov. 15, 2005).

[25]SLGCP has since been succeeded by the Office of Grants and Training (G&T) within the DHS Preparedness Directorate.

- the Single Audit Act, as amended (*codified at* 31 U.S.C. §§ 7501-7507), and other laws and regulations related to OMB Circular No. A-50, *Audit Follow-up*, as revised (Sept. 29, 1982);
- the Improper Payments Information Act of 2002, Pub. L. No. 107-300, 116 Stat. 2350 (Nov. 26, 2002);
- the Department of Homeland Security Financial Accountability Act of 2004, Pub. L. No. 108-330, 118 Stat. 1275 (Oct. 16, 2004); and
- the Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285 (Aug. 3, 1993).

Although DHS inherited many of the reportable conditions and noncompliance issues discussed above, the department's top management, including the CFO, is ultimately responsible for ensuring that progress is made in the area of financial management.

In August 2003, DHS began the "electronically Managing enterprise resources for government effectiveness and efficiency" (eMerge^2) program at an estimated cost of $229 million. The eMerge^2 program was supposed to provide DHS with the financial system functionality to consolidate and integrate the department's financial accounting and reporting systems, including budget, accounting and reporting, cost management, asset management, and acquisition and grants functions. According to DHS officials, a systems integrator was hired in December 2003, and the project was expected to be fully deployed and operational in 2006. In July 2004, we reported[26] that the acquisition of eMerge^2 was in the early stages and continued focus and follow through, among other things, would be necessary for it to be successful.

According to DHS officials, because the project was not meeting its performance goals and timeline, DHS officials began considering whether to continue the project and in Spring 2005 started looking at another strategy. DHS officials told us they decided to change the strategy for its eMerge^2 program in October 2005, and focus on leveraging the systems already in place. The revised strategy will allow DHS components to choose from an array of existing financial service providers. DHS officials said that by January 2006, after spending a reported $15.2 million,

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

acquisition and development activities on eMerge[2] had stopped and the blanket purchase agreement with the systems integrator expired. DHS officials added that the eMerge[2] project would not be renamed. However, DHS plans to continue eMerge[2] using a shared services approach, which allows its components to choose among three DHS providers of financial management services[27] and the Department of the Treasury's Bureau of the Public Debt, which was identified by OMB as a governmentwide financial management center of excellence. DHS officials told us that although a departmentwide concept of operations and migration plan were still under development, they expected progress to be made in the next 5 years. As we will discuss later, a departmentwide concept of operations document would help DHS and others understand such items as how DHS will migrate the various entities to these shared service providers and how it will obtain the departmental information necessary to manage the agency from these disparate operations. DHS officials acknowledged that they needed to first address the material weaknesses at the proposed shared service providers before component agencies migrate to them.

The Building Blocks of Successful Financial Management System Implementations

The key for federal agencies, including DHS, to avoid the long-standing problems that have plagued financial management system improvement efforts is to address the foremost causes of those problems and adopt solutions that reduce the risks associated with these efforts to acceptable levels. Although it appears that DHS will adopt a shared services approach to meet its needs for integrated financial management systems, implementing this approach will be complex and challenging, making the adoption of best practices even more important for this undertaking. Based on industry best practices, we identified four key concepts that will be critical to DHS's ability to successfully complete its planned migration to shared service providers. Careful consideration of these four concepts, each one building upon the next, 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 strategy for DHS components, and (4) defining and effectively implementing disciplined processes necessary to properly manage the specific projects. We will now highlight the key issues to be considered for each of the four areas.

[27]The three proposed DHS shared service providers are Customs and Border Protection, Coast Guard, and Federal Law Enforcement Training Center.

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 Institute of Electrical and Electronic Engineers (IEEE) standards,[28] 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 implement DHS's approach for using shared service providers for its financial management systems, as well as the process 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.

[28]IEEE Std. 1362-1998. The IEEE is a nonprofit, technical professional association that develops standards for a broad range of global industries, including the IT and information assurance industries and is a leading source for defining best practices.

Key Issues for DHS to Consider

- What is considered a financial management system? Are all the components using a standard definition?
- Who will be responsible for developing a DHS-wide 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 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. 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, receipt of goods and services, and would end when the vendor properly receives payment. 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*,[29] 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.[30] 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

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

[30]See 40 U.S.C. § 11303(b)(2)(C).

processes needed for unique missions, or developing subprocesses to support those at the departmentwide level.

Key Issues for DHS to Consider

- 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 the shared service providers to provide consistency across DHS?
- What process will be used to determine and validate the processes needed for DHS agencies that have unique needs?

Strategy for Implementing the Financial Management Shared Services Approach Will Be Key

Although DHS has a goal of migrating agencies to a limited number of shared service providers, it has not yet articulated a clear and measurable strategy for achieving this goal. In the context of migrating to shared service providers, critical activities include (1) developing specific 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 make a selection of a shared service provider for financial management; (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.

Finally, sustained leadership will be key to a successful strategy for moving DHS components towards consolidated financial management systems. 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 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 implementation of DHS's financial management systems.

Key Issues for DHS to Consider

- What guidance will be provided to assist DHS component agencies in adopting a change management strategy that reduces the risks of moving to a shared service provider?
- 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 process used by component agencies to select a provider?
- How will component agencies incorporate strategic workforce planning in the implementation of the shared service provider approach?

Disciplined Processes Will Help Ensure Successful Implementation

Once the concept of operations and standard business processes have been defined and a migration strategy is in place, the use of disciplined processes, as discussed previously, 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 have contributed to the failure of previous agency efforts. Further details on disciplined processes can be found in appendix III of our recently issued report.[31]

Key Issues for DHS to Consider

- 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?

Concluding Observations

In closing, the best practices we identified are interrelated and interdependent, collectively providing an agency with a better outcome for its system deployment—including cost savings, improved service and product quality, and ultimately, a better return on investment. The predictable result of DHS and other agencies not effectively addressing these best practices is projects that do not meet cost, schedule, and performance objectives. There will never be a 100 percent guarantee that a new system will be fully successful from the outset. However, risk can be managed and reduced to acceptable levels through the use of disciplined processes, which in short represent best practices that have proven their value in the past. We view the application of disciplined processes to be essential for DHS's systems modernization efforts. Based on industry best practices, the following four concepts would help ensure a sound foundation for developing and implementing a DHS-wide solution for the complex financial management problems it currently faces: (1) developing a concept of operations that expresses DHS's view of financial management and how that vision will be realized, (2) defining standard business processes, (3) developing an implementation strategy, and (4) defining and effectively implementing applicable disciplined processes. If properly implemented, the best practices discussed here today and in our recently issued report[32] will help reduce the risk associated with a project of this magnitude and importance to an acceptable level. With DHS at an important crossroads in the implementation of the eMerge^2 program, it has the perfect opportunity to use these building blocks to form a solid

[31]GAO-06-184.

[32]GAO-06-184.

foundation on which to base its efforts and avoid the problems that have plagued so many other federal agencies faced with the same challenge.

Mr. Chairmen, this concludes our prepared statement. We would be happy to respond to any questions you or other Members of the Subcommittees may have at this time.

Contacts and Acknowledgments

For information about this testimony, please contact McCoy Williams, Director, Financial Management and Assurance, at (202) 512-9095 or at williamsm1@gao.gov, or Keith A. Rhodes, Chief Technologist, Applied Research and Methods, who may be reached at (202) 512-6412 or at rhodesk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony. Individuals who made key contributions to this testimony include Kay Daly, Assistant Director; Chris Martin, Senior-Level Technologist; Francine DelVecchio; Mike LaForge; and Chanetta Reed. Numerous other individuals made contributions to the GAO reports cited in this testimony.

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

Mr. PLATTS. Thank you, Mr. Williams.

Before we move to Mr. Hite, we are pleased to be joined by the Homeland Security subcommittee ranking member, the gentleman from Florida, Mr. Meek. And I believe you would like to make an opening statement?

Mr. MEEK. Thank you, Mr. Chairman.

I will make some brief comments, and I will enter the rest of my statement for the record.

I am glad that both of our subcommittees have come together to have this hearing. This is the first time the Homeland Security and Government Reform Committees have had an oversight joint hearing as far as we know here, here at this level.

But the fact that these two committees have come together today says a lot about the level of concern for Department of Homeland Security. I can tell you, as the ranking member of the oversight committee, the Homeland Security subcommittee, I am becoming more and more concerned with these kinds of hearings after the incident has happened and after the taxpayers' money has been wasted.

I am also very concerned about the fact there is so much attrition over at the Department of Homeland Security, so that once you set the plan to recover or to make sure it never happens again, you have a whole other set of players in place. I am interested in learning today at this hearing how the corrections to make sure that the incident that has happened never happens again and jeopardize national security is put into place so that we don't have to have another hearing such as this one.

This has very serious consequences for our national security, and I agree with many of the points that were made in the GAO report. Looking forward to hearing more about it.

And with that, Mr. Chairman, I would like to just enter the rest of my comments for the record so that we can get the testimony, and we will have time for question and answers, sir.

Thank you. Yield back.

Mr. PLATTS. Thank you, Mr. Meek.

And without objection, the rest of your testimony is entered into the record.

And we will proceed, Mr. Hite, if you would like to proceed with your opening statement?

STATEMENT OF RANDOLPH C. HITE

Mr. HITE. Thank you, Chairman Platts, Chairman Rogers, Ranking Member Meek.

Let me begin by commending this subcommittee—or both subcommittees for holding this hearing on IT management at DHS, a subject that is, without question, as challenging for the department as it is important. Suffice it to say that while effective IT management is not the end all and be all when it comes to transforming the department, this transformation cannot occur without it.

My statement today addresses the state of IT management at DHS and what I view as two interrelated planes. The first is establishing institutional or corporate-level IT management controls, and the second is actually managing individual IT programs in accordance with these controls.

In effect, this collection of control mechanisms can be viewed as providing the means to desired end, that is, delivering systems that are on time and on budget and produce required capabilities and promised benefits.

My bottom-line message is there has been mixed progress on these fronts. But overall, the department is not yet where it needs to be.

To expand on this bottom line, let me first set the stage by identifying some of these institutional controls that I am referring to, all of which are spelled out in my written statement, and then focus on the department's performance thus far in implementing them, using key system investments as examples.

One control is having and using an enterprise architecture, which can be viewed as a department-wide operational and technological blueprint that provides an authoritative frame of reference to guide and constrain the structure and the content of IT investments.

Another is applying engineering and acquisition discipline and rigor when defining and designing and developing and testing and deploying and maintaining these IT systems.

A third is having people with the right knowledge, skills, and abilities to execute all of these disciplines. And transcending each of these controls is an empowered Chief Information Officer to make it all happen.

Over the last 3 years, we have reported on varying levels of progress in these areas. For example, we pointed out that the department's first version of its enterprise architecture provided a foundation upon which to build, but it was missing important content which limited its utility.

Since then, the department has improved its approach to managing the architecture and has issued updated versions of it. The latest version includes some of the missing scope, and the department plans to keep building on this.

We also found the department has introduced a standard template for capturing information about investments alignment with the architecture, although it has yet to document a methodology with explicit criteria for determining the degree of alignment.

As another example, the department continues to recruit, hire, and train IT professionals, but has yet to develop a strategic approach to IT human capital management that provides for, first, understanding the current and needed work force numbers and qualifications and then pursuing explicit strategies for filling current and projected gaps in these capabilities.

Now, concurrent with its ongoing efforts to strengthen corporate IT governance, the department has continued to invest heavily in new and enhanced systems, including IT infrastructure, such as shared networks, consolidated data centers, and IT systems better known for their catchy titles, such as ACE and US-VISIT and Secure Flight, to name a few.

To the department's credit, some of these investments have resulted in increments of capabilities to assist DHS employees in doing their jobs. Examples include the initial core of a department-wide sensitive, but unclassified network known as OneNet, the entry side of US-VISIT, and the first four releases of ACE.

However, other capabilities, such as the Atlas infrastructure initiative, the exit side of US-VISIT, and Secure Flight as a whole, are not operational after years of work.

We have also reported that these and other IT investments have suffered from management weaknesses that both have caused problems and increased the risk of future problems.

Examples include poor requirements definition, inadequate testing, limited program planning, unreliable cost and schedule estimating, poor security management, limited staffing, inadequate risk management, absence of independent verification validation, limited earned value, to name more than a few. Some of these weaknesses have been corrected on some programs, but others have not.

So having said all of this, what needs to be done? Part of the answer lies in the litany of recommendations that we have made to address each of these institutional and program-specific areas. To the department's credit, it has largely agreed with these recommendations, and some have been implemented. However, most are still works in process.

In my view, our recommendations provide a comprehensive framework for strengthening DHS's IT management and increasing the chances that its investments will successfully play their roles in transforming how the department operates and how well it performs. We look forward to working constructively with the department in implementing them.

This concludes my statement. I would be happy to answer any questions whenever you choose.

[The prepared statement of Mr. Hite follows:]

United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees

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

HOMELAND SECURITY

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

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

GAO-06-598T

March 29, 2006

GAO
Accountability · Integrity · Reliability
Highlights

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

HOMELAND SECURITY

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

Why GAO Did This Study

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

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

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

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

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

What GAO Found

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

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

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

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

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

Mr. Chairmen and Members of the Subcommittees,

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

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

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

[1] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003); *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

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

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

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

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

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

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

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

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

Background

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

Created in March 2003, DHS has assumed operational control of about 209,000 civilian and military positions from 22 agencies and

offices specializing in one or more aspects of homeland security.[4] The intent behind DHS's merger and transformation was to improve coordination, communication, and information sharing among the multiple federal agencies responsible for protecting the homeland. Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. As we reported before the department was created,[5] such a transformation is critically important and poses significant management and leadership challenges. For these reasons, we designated the implementation of the department and its transformation as high risk; we also pointed out that failure to effectively address DHS's management challenges and program risks could have serious consequences for our national security.

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

DHS Components and IT Spending

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

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

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

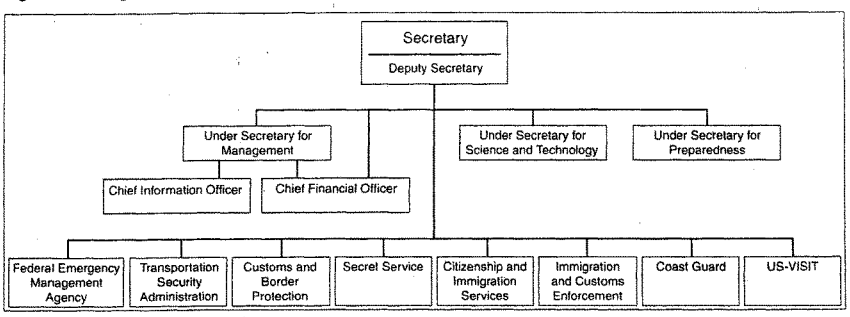
Table 1: DHS's Principal Organizations and Their Missions

Principal organizations*	Missions
Citizenship and Immigration Services	Responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities.
Coast Guard	Protects the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, and in any maritime region as required to support national security.
Customs and Border Protection	Responsible for protecting the nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.
Federal Emergency Management Agency	Prepares the nation for hazards, manages federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.
Immigration and Customs Enforcement	The largest investigative arm of the department, responsible for identifying and shutting down vulnerabilities in the nation's border, economic, transportation, and infrastructure security.
Management Directorate	Responsible for department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. This directorate includes the offices of the Chief Financial Officer and the Chief Information Officer.
Preparedness Directorate	Works with state, local, and private sector partners to identify threats, determine vulnerabilities, and target resources where risk is greatest, thereby safeguarding borders, seaports, bridges and highways, and critical information systems.
Science and Technology Directorate	Serves as the primary research and development arm of the department, responsible for providing federal, state, and local officials with the technology and capabilities to protect the homeland.
Secret Service	Protects the President and other high-level officials and investigates counterfeiting and other financial crimes (including financial institution fraud, identity theft, and computer fraud) and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.
Transportation Security Administration	Protects the nation's transportation systems to ensure freedom of movement for people and commerce.
US-VISIT	Responsible for developing and implementing a governmentwide program to record the entry into and exit from the United States of selected individuals, verify their identity, and confirm their compliance with the terms of their admission into and stay in this country.

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

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

Figure 1: DHS Organizational Structure (Simplified and Partial)



Source: GAO analysis of DHS data.

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

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

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

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

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

Table 2: IT Funding for Fiscal Year 2006

Dollars in millions

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

Source: GAO analysis of DHS data.

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

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

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

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

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

[f]HR IT includes the set of DHS enterprisewide systems to support the personnel regulations such as MaxHR.

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

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

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

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

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

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

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

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

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

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

IT Management Controls and Capabilities Are Important

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

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

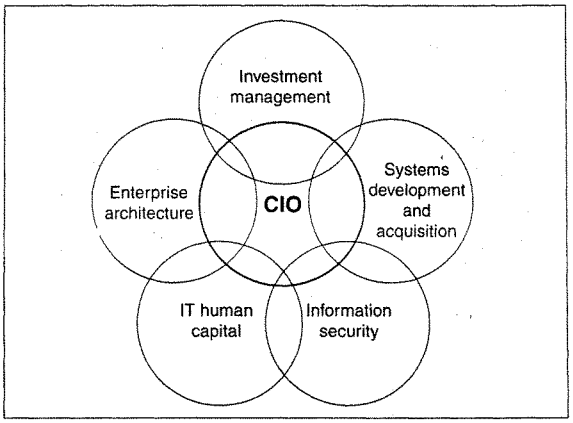
[7] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001); *Architect of the Capitol: Management and Accountability Framework Needed for Organizational Transformation*, GAO-03-231 (Washington, D.C.: Jan. 17, 2003).

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

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

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

Figure 2: Interrelated Keys to Successful IT Management



Source: GAO.

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

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

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

Enterprise Architecture

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

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

[9] See for example, GAO, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458, (Washington, D.C.: Feb. 28, 2003); *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

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

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

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

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

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

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

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

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

IT Investment Management

Through IT investment management, organizations define and follow a corporate process to help senior leadership make informed decisions on competing options for investing in IT. Such investments, if managed effectively, can have a dramatic impact on

performance and accountability. If mismanaged, they can result in wasteful spending and lost opportunities for improving delivery of services.

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

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

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

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

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

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

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

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

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

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

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

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

Systems Development and Acquisition Management

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

Best practices in systems development and acquisition include following a disciplined life cycle management process, in which key activities and phases of the project are conducted in a logical and

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

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

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

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

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

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

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

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

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

Information Security Management

Effective information security management depends on establishing a comprehensive program to protect the information and information systems that support an organization's operations and

assets. The overall framework for ensuring the effectiveness of federal information security controls is provided by the Federal Information Security Management Act of 2002.[18] In addition, OMB Circular No. A-130 requires agencies to provide information and systems with protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to these assets or their loss, misuse, or modification.

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

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

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

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

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

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

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

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

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

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

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

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

IT Human Capital Management

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

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

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

[24] GAO-02-373SP.

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

[26] GAO-04-39.

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

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

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

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

CIO Leadership

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

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

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

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

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

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

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

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

DHS Is Making Some Progress in Implementing IT Systems and Infrastructure

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

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

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

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

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

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

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

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

Key IT Programs Reflect Mixed Use of Effective IT Management Practices

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

IT investment alignment with the enterprise architecture. An important element of enterprise architecture management is ensuring that IT investments comply with the architecture. However, in several of the programs that we have reviewed, investments have been approved without documented analysis to support these judgments and to permit the judgments to be independently verified. For example, DHS approved the ACE program's alignment with the department's architecture on the recommendation of its Enterprise Architecture Center of Excellence and Enterprise Architecture Board. However, the Center's evaluators did not provide a documented analysis that would allow independent verification. According to DHS officials, they do not have a documented methodology for evaluating programs' architecture compliance, and instead rely on the professional expertise of Center staff. In contrast, the ASI program provides an example of an instance in which the reviews required to ensure

architecture alignment resulted in the discovery of a significant problem: the program had not adequately defined its relationships and dependencies with other department programs.[33] As a result, the program was reconsidered and later subsumed within the new Secure Border Initiative, the department's broader strategy for border and interior enforcement.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For several IT programs, security and privacy has been a challenge. For example, we reported[36] in September 2003 and again in May 2004 that the US-VISIT program office had yet to develop a security plan as required by OMB and other federal guidance, although the program later developed a plan that was generally consistent with applicable guidance. However, the program office had not conducted a security risk assessment or included in the plan when such an assessment would be completed. OMB and other federal guidance specifies that security plans should describe the methodology that is used to identify system threats and vulnerabilities and to assess the risks, and include the date the assessment was completed.

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

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

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

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

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

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

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

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

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

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

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

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

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

Contacts and Acknowledgments

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

Mr. PLATTS. Thank you, Mr. Hite.
Mr. Schied.

STATEMENT OF EUGENE SCHIED

Mr. SCHIED. Thank you, Chairman Platts, Chairman Rogers, Ranking Member Meek, for allowing me this opportunity to testify before you regarding the Department of Homeland Security's plans for its financial management systems and the future of the eMerge2 program.

The Department of Homeland Security continues to make progress in improving financial management, but the progress admittedly does not come easy or quick.

Our accomplishments to date reflect the rigorous effort of our financial management personnel and are evidenced by things such as the timely completion this past November of DHS's consolidated financial statements for the first time and the submission of those statements for audit, the unqualified opinion on the balance sheet this past year by the Customs and Border Protection, our work on internal controls to date, and OMB's A–123 implementation and implementation of the OMB A–123 requirements, including the completion this past year of the GAO assessment tool used by DHS components to support the assertion made by the Secretary at the end of the year.

And financial systems and accounting service successes to date that include, as mentioned by Chairman Rogers, the reduction of the number of financial service providers to date from 18 down to 8, a CBP and Secret Service implementation successful of new financial management systems, and the U.S. Coast Guard and FLETC becoming financial service providers to other components within the Department of Homeland Security.

Particularly regarding systems, and specifically the department's eMerge2 program, it did not progress as we had originally planned, and DHS still needs to improve greatly its resource management systems. We have some systems that are aging. Others that fail to meet user requirements. Some that are not fully integrated between finance, procurement, and asset management.

To meet these needs, rather than acquiring, configuring, and implementing a new system solution, as we initially started with the eMerge2 program, we are now looking to leverage investments that have already been made, both inside DHS and outside.

By closely monitoring contract performance under the initial attempt at the eMerge2 solution implementation, we were able to determine really within several weeks of letting the initial eMerge2 task order that we had issues with how the project was progressing.

We determined that the project had veered unacceptably off schedule, and we worked with the contractor in an attempt to get the project back on track. But when the risks ultimately were deemed to be too great, we chose to allow the blanket purchase agreement to expire and to retool our approach to meet our systems needs.

Specifically, the primary reasons we decided to stop with the effort to build the new system solution include contractor performance issues; the challenge of undertaking a major change while still

building the basic organizational capabilities within DHS to manage a project of this magnitude; consideration of the overall financial management issues faced by DHS, such as those cited in the annual financial audits; and recognition that recent DHS component financial systems and servicing successes, such as those I have just mentioned, presented viable alternatives to standing up a new system.

We are now in the replanning effort of our eMerge2 effort to improve financial systems. We are looking at leveraging system investments that have been made to date, not only those within DHS, but also at the OMB financial management centers of excellence. And we are developing a 5-year plan not only for the improvement of financial management, but also how improvements in financial management services have to tie in with systems including internal controls and financial reporting.

The eMerge2 program is an important element of improving financial management in DHS, but it is vital as DHS moves forward that the eMerge2 program not be viewed as separate from the larger context of financial management, which includes not only systems, but people and processes.

Our efforts to fix audit weaknesses, improve financial management, strengthen internal controls, and modernize financial systems are all interrelated activities. Accordingly, before jumping headlong into further systems and service provider changes, DHS has to make sure that the prerequisite steps of solidifying financial management are taken.

Central to eliminating all of DHS's reported material weaknesses and obtaining a clean financial statement audit opinion is a credible and enforceable corrective action and remediation process. This year, DHS is entirely revamping the corrective action process. It will be more standardized, and it will be more disciplined.

Among our changes for this year are identifying root causes and underlying issues of our pervasive material weaknesses, particularly those involving fund balance with Treasury and financial reporting; formalizing a corrective action process through a management directive, through guidance, through training, then utilizing the authority from the Office of the Secretary to overcome cultural shifts and secure management commitment; leveraging an automated tool to help us track our corrective action process.

We will also be partnering with the inspector general's office to ensure that our progress is monitored and that management is held accountable for the progress.

In conclusion, while the eMerge2 program did not progress along the path we had originally envisioned, we managed the project in such a way that enabled us to minimize our risk and make course corrections before substantial sums of taxpayer dollars were expended.

We are now moving along a path that will enable us to achieve our original goals of providing decisionmakers with critical resource management information, but at less risk to the Government. The new approach will also enable us to better incorporate needed improvements in DHS financial management practices into the design and rollout strategy of our new approach.

Thank you again for the opportunity to testify here today, and I especially thank you for your leadership and continuing support in Homeland Security and its management programs. And I would be happy to answer any questions.

Mr. PLATTS. Thank you, Mr. Schied.

Mr. Charbo.

STATEMENT OF SCOTT CHARBO

Mr. CHARBO. Thank you, Chairmen Platts and Rogers, Ranking Member Meek.

I would like to focus my comments on capital control processes and IT governance within the Department of Homeland Security.

Currently at DHS, the IT Strategic Plan and Enterprise Architecture are developed from the DHS Strategic Plan, the Future Years Homeland Security Program [FYHSP], and the Secretary's Planning Priorities. These assist in framing our governance processes as we manage IT programs.

The department's current IT budget is controlled and invested by the Capital Planning and Investment Control [CPIC] process. The department's enterprise architecture process, coupled to our CPIC process, ensures the department optimally invests and manages its annual budget.

The investment strategy at the department is taking a review of the systems via portfolio view. These portfolios are managed through a Joint Resource Council [JRC], of the department leadership, then an IRB board, which reviews for major investments by each of those portfolios.

Portfolio investments must meet specific criteria in order to be continuously funded. They must align to the DHS mission, have clear performance metrics. They must meet program and project control criteria as measured by earned value and demonstrate delivery of discrete technical capability at key milestones throughout the life cycle of the investment.

In addition, the investment performance is assessed against the entire portfolio to ensure that budget dollars are allocated to initiatives that are delivering the most value to the mission.

Our strategy of alignment, integration, and architecture is centered on the Technical Reference Model of the enterprise architecture. The TRM is used to establish standards and initial integration throughout DHS. These standards are enforced through the EA governance process.

The eventual goal is to align requirements and reduce the number of products being used for particular functions to the standard products laid out in the TRM. We feel this will enhance information sharing as well.

The department has the proper IT governance for its programs through the CPIC process and the Enterprise Architecture Board for the enterprise architecture. A strong part of this governance is the CIO Council. This consists of the department CIOs and the CIOs of the major components. This council provides a collaborative forum for DHS-wide IT decisionmaking, allows for the socialization of these decisions, and acts as the architecture board that is chaired by myself.

The benefits of the council finalizing and disseminating the EA and CPIC processes are many fold. It aligns the investment decisions to the FYHSP goals and objectives, balances DHS resources across transformational portfolios and objectives, identifies redundancies in integration opportunities across DHS, and it maintains enterprise-level OMB, PMA, and congressional compliance.

As the department moves forward with eMerge2 to achieve a clean financial opinion, standardization of DHS accounting structure and financial management business rules, processes, and procedures, those same principles mentioned—of proper program management, requirements alignment, IT governance, and risk mitigation—will be applied.

Thank you. I look forward to your questions.

[The prepared statement of Messrs. Schied and Charbo follows:]

Statement by

Scott Charbo

Chief Information Officer

Department of Homeland Security

and

Eugene Schied

Deputy Chief Financial Officer

Department of Homeland Security

Before the

House Government Reform Subcommittee on

Government Management, Finance, and Accountability

and the

House Homeland Security Subcommittee on

Management, Integration, and Oversight

Hearing on

Thank you Chairman Platts, Chairman Rogers and members of the Subcommittees, for allowing us this opportunity to testify before you regarding the Department of Homeland Security's (DHS) Information Technology investments, its plans for its financial management systems, and the future of the ***eMerge²*** Program.

Information Technology (IT) Governance and Investment Control

The IT Strategic Plan and Enterprise Architecture (EA) for DHS are developed from the DHS Strategic Plan, the DHS Future Years Homeland Security Program (FYHSP) and the Secretary's Planning Priorities. These assist in framing our governance processes.

The Department's current IT budget is controlled and invested by the Capital Planning and Investment Control (CPIC) process. The Department's Enterprise Architecture (EA) process coupled with our CPIC process ensures the Department optimally invests and manages its annual budget.

DHS reviews critical systems investments in two ways: (1) we look at proposed investments from a portfolio perspective where investments are assessed cross-programmatically for gaps, redundancies and interoperability; (2) we conduct in-depth reviews of investments periodically and at milestone decision points to assess risk and management of the program's cost, schedule and performance. These reviews are conducted by senior DHS leadership through the Joint Requirements Council (JRC) and the final decisions rest with the Investment Review Board (IRB). The JRC is comprised of the Department's Chief Information Officer, Chief Financial Officer, Chief Procurement Officer, Chief Human Capital Officer, Chief Administrative Services Officer and the Chief Operating Officers of the Components. The IRB is chaired by the Deputy Secretary and is comprised of the Under Secretary for Management, the CFO, CIO, Assistant Secretary for Policy, and other DHS Component heads as appropriate. Additionally, the Integrated Project Review Team (IPRT) conducts integrated reviews in support of the IRB, JRC, Enterprise Architecture Board, and Asset and Services Management Board. The IPRT is comprised of subject matter experts and representatives from various organizations within DHS. The IPRT develops an integrated review plan for investments that reflects the cost, complexity, and risk of the investment. The Department's investment review process is governed by a Department Management Directive that is designed to reduce risk and provide appropriate investment oversight. This directive is part of an ongoing Department focus on continuously improving mission effectiveness.

Portfolio investments must meet specific criteria for continuous funding. They must align to the DHS mission, have clear performance metrics, meet program and project control criteria as measured by Earned Value Management and Operational Analysis, and demonstrate delivery of discrete technical capability at key milestones throughout the lifecycle of the investment. In addition, investment performance is assessed against the entire portfolio to ensure that budget dollars are allocated to initiatives that are delivering the most value to the mission.

The Technical Reference Model (TRM) of the DHS Enterprise Architecture is used to establish standards throughout DHS. These standards are enforced through the EA governance process. The eventual goal is to align requirements and reduce the number of products being used for particular functions to the standard products laid out in the TRM. This enhances information sharing since the TRM standards facilitate information sharing.

The Department ensures proper IT governance of its programs through the CPIC process and the Enterprise Architecture Board (EAB) for the EA. A strong part of this governance is the CIO Council, which consists of the CIOs from DHS HQ and its components. This Council, which is chaired by the Department's CIO, provides a collaborative forum for DHS-wide IT decision-making, allows for the socialization of those decisions and acts as the EAB.

The benefits of the CIO Council finalizing and disseminating the EA and CPIC processes are:

- it aligns investment decisions to FYSHP goals and objectives
- it balances DHS resources across Transformational Portfolios and objectives
- it identifies redundancies and integration opportunities across DHS, and
- it maintains enterprise-level OMB, PMA, and Congressional Compliance

As the Department moves forward with the ***eMerge²*** program to achieve standardization of the DHS accounting structure and financial management business rules, processes, and procedures, the same principles of proper program management requirements alignment, IT governance and risk-mitigation will be applied.

eMerge²

Specifically regarding the ***eMerge²*** program, while the project has taken a new direction in recent months, our need and our vision remain the same: To equip DHS managers and senior leadership with the critical resource management information necessary to improve decision-making and to improve service delivery and efficiency.

The initial ***eMerge²*** strategy to develop a new financial system was based in part on an assessment, conducted in 2003, which concluded that the mission support systems being inherited by the new Department of Homeland Security had limitations. Specifically, each of the systems examined failed to meet all mandatory requirements promulgated by the Joint Financial Management Improvement Program (JFMIP), the government's financial standards setting board. Based on this study's findings, and the fact that there were a number of new or transferred organizations that had no resource management systems, the decision was made to develop a new, integrated suite of resource management systems that would serve as a platform for the entire Department.

At the same time, a few other efforts already underway prior to the creation of DHS were allowed to continue. CBP was well on its way to implementing an integrated suite of resource management systems with SAP and SAP was an integral part of the massive CBP Automated Commercial Environment (ACE) initiative. Similarly, both Coast Guard and Secret Service were in the midst of implementing upgrades to their resource management systems. Instead of

requiring CBP, Coast Guard and Secret Service to migrate to the new ***eMerge²*** solution, it was decided to design an interface so that data from these agencies' systems could be fed into the ***eMerge²*** solution to enable department-wide data compilations and evaluations and the development of consolidated financial statements.

In late Fiscal Year 2003/early Fiscal Year 2004, DHS issued contracts with BearingPoint and SAIC to develop the Department's functional and technical requirements and to build the resource management portions of the homeland security enterprise architecture. These requirements were approved by all DHS components. Based on these requirements, DHS developed an RFP for the acquisition and implementation of an integrated resource management solution for the Department.

In September 2004, after a competitive acquisition process, BearingPoint was awarded a Blanket Purchase Agreement (BPA) with a ceiling of $228.7 million to acquire and implement the ***eMerge²*** solution. So as to minimize the risk of such a large project, the Department structured the project so that we would incrementally issue firm-fixed price task orders for small, measurable portions of work. The first task order (Task Order #1) was issued for $20 million for solution development and conference room pilot testing. Soon into work on this task order, concerns began to arise regarding the extent to which there was a clear understanding between DHS and BearingPoint on what was to be delivered. Deadlines were missed and products presented to the project team were not accepted. As a result, in February 2005, the DHS CFO initiated a review of the ***eMerge²*** effort.

Work under Task Order #1 was closed out in April 2005, prior to completion. Based on the work that was satisfactorily completed, the price was adjusted from $20 million to $6 million. As we halted work on Task Order #1, DHS issued a small, finite task order (Task Order #2) to BearingPoint in the amount of $2.9 million. The primary activity under Task Order #2 was to help DHS examine certain component systems in greater detail. We again surveyed the existing financial systems in the Department against the capabilities to meet core functional requirements, which were derived from the requirements developed during the first phase of the ***eMerge²*** project. In particular, the system at the United States Coast Guard, which used a similar suite of products as proposed under the ***eMerge²*** project and which was already a service provider to the Transportation Security Administration, was examined in detail.

The conclusions reached last fall by the OCFO were:

1. The effort that we embarked upon under the BPA with BearingPoint should end because it had not been successful and future action down this path was high-risk;
2. DHS' own organizational maturity issues also made the project high-risk; and
3. Other viable options to leverage existing investments existed and have been successful.

In short, the DHS CFO concluded that several existing components in DHS had upgraded their systems and improved operations to the extent that viable alternatives to restarting with a new system integrator were possible. Our assessment also concluded that the Office of Management and Budget's Financial Management Line of Business and its Centers of Excellence offered

viable alternatives to meet DHS' requirements as well. In December 2005, DHS chose not to exercise the next option year on the BearingPoint BPA, and so the BPA expired. The total expenditure on the ***eMerge²*** contract with BearingPoint under the implementation BPA was $8.9 million.

eMerge² New Direction

DHS still has a need to improve its resource management systems. We have some systems that are aging; some that fail to fully meet user requirements; and some that are not fully integrated between finance, procurement, and asset management. To meet these needs, rather than acquiring, configuring, and implementing a new system within DHS, we recognize the opportunity to leverage investments that have already been made, both inside DHS and outside. We have identified a broader list of potential financial management service providers – including those within DHS and some of the OMB-named Financial Management Centers of Excellence for assessment.

We have now moved on to a process in which we are assessing our requirements against the services and solutions offered by the various potential service providers. Leveraging materials created during the earlier phase of the ***eMerge²*** project, we sent potential service providers an informal Request for Proposal (RFP). The customers also provided answers to a Request for Information (RFI) on organizational size and workload. In addition, customers evaluated what services they required. The Service Centers have responded to the requirements and constraints with a technical proposal and also provided an operational cost proposal for each customer based on the data received in the RFI. Each of the four Service Providers provided a two-day demonstration of their solution for the customers. The customers then rated each Service Center as acceptable or not acceptable. The Service Centers have also been asked to provide a rough estimate for the migration cost and the duration estimated to accomplish the migration. The conclusion of this phase is to put together both near term and long term migration plans, including approximated "go-live" dates. This planning is expected to be largely completed in May 2006, and then sent through the various investment review authorities in June 2006.

The systems development aspect of our new approach will focus largely on the expansion of capabilities and tools to support a global view of DHS finances. DHS has a limited set of centralized reporting tools, used largely to produce the consolidated financial statements and report information to Treasury. But the production of more detailed program reports useful for oversight and monitoring purposes is still too manual and time consuming, and the data is limited. Thus, an important effort for the current Fiscal Year is to begin to increase our collection and use of management information.

With the revised ***eMerge²*** effort, we will also be squarely examining how financial services are provided in DHS. The effort is about more than just getting people onto new systems. It is about the transformation of financial management service delivery in DHS. Over time, to realize increased efficiency, new business models for how we manage financial services will have to be examined and implemented.

eMerge² Funding

In the current Fiscal Year we have $48.4 million available for the ***eMerge²*** project and we have requested an additional $18 million for the program in the President's Fiscal Year 2007 Budget. These funds will be used to implement the revised ***eMerge²*** approach. Specifically, funds will be expended on consolidations & improvement, data cleansing and migration, change management and training, enterprise resource management data visibility, and completing e-Travel implementations.

The _eMerge²_ Project and Financial Management

The ***eMerge²*** project is an important element of improving financial management in DHS; however, it should not be viewed separate from the larger context of financial management, which includes not only systems, but also people and processes. Our efforts to fix audit weaknesses, improve financial management, strengthen internal controls, and modernize financial systems are all interrelated activities.

As you know, DHS received a disclaimer on our Fiscal Year 2005 financial statements. While financial systems are certainly a part of being able to produce reliable financial statements, the weaknesses identified by the auditors have more to do with our people and processes, than with our systems. The DHS Inspector General continued to report ten material weaknesses in DHS' Fiscal Year 2005 financial statement audit report. These findings represent a myriad of complex legacy issues only compounded by the challenge of bringing together separate and disparate automated systems and systems of internal control including the policies, procedures, personnel, and cultures that must evolve into a single way of doing business, a DHS way of doing business.

The financial statements themselves provide an annual portrayal of every financial aspect of DHS mission activities. Yet, the presentation of that information as a uniform whole continues to present challenges at the component and consolidated level. Disclaimers of opinion reflect the inability of the auditors to conduct a sufficient audit necessary to obtain assurance that the financial statements are fairly presented. The reported conditions that are considered material weaknesses contribute to the necessity of the auditors to issue a disclaimer of opinion. These reported conditions that are considered material weaknesses are as follows:

- Financial Management Oversight
- Financial Reporting
- Financial Systems Security
- Fund Balance with Treasury
- Property, Plant, and Equipment
- Operating Materials and Supplies
- Undelivered Orders, Accounts and Grants Payable, and Disbursements
- Actuarial Liabilities
- Budgetary Accounting
- Intragovernmental and Intradepartmental Balances

Corrective Action Plans

A necessary first step in obtaining an opinion on the DHS-wide consolidated financial statements, is to first obtain an opinion on the DHS-wide Consolidated Balance Sheet, which is only one of the six principal financial statements. Material weaknesses that need to be fixed in order to obtain an opinion on DHS' Fiscal Year 2006 Balance Sheet include: Fund Balance with Treasury, Operating Materials and Supplies, Property Plant and Equipment, and Actuarial Liabilities.

Targeting material weaknesses that directly relate to the disclaimer on the DHS Consolidated Balance Sheet will provide the assurance over the processing of activity and transactions that are reflected on this financial statement. DHS OCFO is working closely with the DHS Office of the Inspector General (DHS OIG), DHS OIG's contracted auditors, and key Headquarters and component financial managers to continue to refine and leverage corrective action planning efforts in the most efficient manner to achieve this goal for Fiscal Year 2006.

Tangible progress in remediating the four material weaknesses mentioned above will have the synergistic effect of beginning to reduce the severity of the remaining six material weaknesses related to undelivered orders, accounts and grants payable, inter and intra governmental transactions, budgetary accounting and financial management oversight, and financial reporting.

Central to the planned elimination of all DHS reported material weakness is a credible and enforceable corrective action planning process that has the full backing and funding commitment of upper management, the DHS OIG audit community, and DHS front line financial managers and staff. This year, DHS is entirely revamping its corrective action process. It will be more standardized and disciplined. Among our changes for this year are:

- Identifying the root causes and issues underlying our pervasive weaknesses by comprehensively assessing the current designs of our internal controls, and prioritizing plans to address internal control gaps to support the elimination of pervasive material weaknesses.
- Formalizing the corrective action planning process through a Management Directive, guidance, training, and utilizing authority from the Office of the Secretary to overcome cultural shifts and secure management commitment.
- Implementing an automated corrective action tracking system to ensure progress is tracked and management is held accountable for progress.
- Developing the *Secretary's Strategic Plan for Improving Internal Controls over Financial Reporting*, in close coordination with OMB and OIG.

OIG and auditor input and reporting on internal controls over financial reporting is a critical component of helping us understand our problems, and monitoring the effectiveness of an organization's accountability. The DHS OCFO, OIG and financial statement auditors have had an excellent relationship, and continued open interactions among these parties is critical for success. The DHS OCFO is also partnering with the OIG to help monitor the Department's performance in correcting material weaknesses by establishing periodic reporting by the OIG that assesses and compliments management's corrective action efforts.

Responsibility for resolving material weaknesses, however, falls largely on the same financial and program management professionals throughout DHS that are also needed to successfully implement the ***eMerge²*** project. Accordingly, management faces tradeoffs of time, effort, and money between improving the issues that give rise to our material weaknesses, and preparing to migrate financial systems. For example, Immigration and Customs Enforcement (ICE) provides financial services to many of the organizations that have been identified as being in need of improved financial services and systems. At the same time, financial management improvements at ICE are critical to DHS' efforts to pass an audit this year. Likewise, the USCG is a potential service provider for more DHS customers, but also needs to make improvements that address known material weaknesses. At present, overcoming the material weaknesses cited in our financial statements audit is paramount to consolidating financial systems and is a key consideration as we develop our near- and long-term ***eMerge²*** migration plans.

Internal Controls

DHS' plans for financial management and resource management systems transformation will pivot on a sound foundation of internal control. Through our comprehensive efforts to assess and improve our internal controls, management will work itself into a position where it can provide its assurance that a sound, reliable controls environment exists within DHS.

Our work on internal controls is intricately linked to our work on redressing our material weaknesses and our work on financial systems. It will be through our work on internal controls that we are able to identify and fix many of the underlying problems that lead to material weaknesses. Similarly, our work on the consolidation and migration of financial systems and service providers will help us ensure that we have sufficient controls in place.

The DHS CFO has created a plan to institute a comprehensive network of internal controls throughout DHS. Central to the plan was the creation of an Internal Control Committee (ICC) comprised of key managers from across DHS Headquarters and Components to evaluate best practices from across industry and government and design a system of controls that will support sustainable, clean audit opinions on DHS component and consolidated financial statements.

To assist the Department's Internal Control Committee in implementing OMB A-123, this past January, we awarded a blanket purchase agreement to PricewaterhouseCoopers LLP (PwC) for up to $7.6 million in Fiscal Year 2006, with a potential 5-year value of up to $42.4 million through January 2011. The Department's Independent Government Cost Estimate was developed and based on historical audit hour estimates from the Department's Financial Statement audit. Our contract with PwC is similar to other CFO Act agency efforts in implementing OMB A-123. Specific PwC tasks will include:

- Providing training to develop skill sets for internal controls,
- Developing internal control process analysis documentation,
- Performing internal control test work,
- Developing remediation strategies for material weaknesses in internal control, and
- Providing project management support for the Department's ICC.

In total, PwC will have approximately 20 to 25 staff and 5 subcontractors assigned to the Department's ICC. Skill sets of these staff include individuals with prior experience in performing internal control assessments, internal control attestations, business process documentation and improvement, and financial management reporting for the Department of Homeland Security and other large, complex Federal agencies.

Conclusion

Although we still have a lot of challenges before us, DHS has made real progress in the systems and financial management areas and has put in place systems and processes to guide and optimize our IT investments in support of the DHS mission. While the ***eMerge²*** project did not progress along the path we had originally envisioned, we managed the project in such a way that enabled us to minimize our risk, identify problems early on, and make course corrections before substantial sums of taxpayer dollars were expended. When progress does not move in the direction or speed at which it should, we have – and will continue to – make changes to ensure we get what is needed to best support DHS operations.

Thank you for your leadership and your continued support of the Department of Homeland Security and its management programs. We would be happy to answer any questions you may have.

Mr. PLATTS. Thank you, Mr. Charbo, and, again, all four of our witnesses for your written testimony and oral statements.

We will go into questions, and we will try to stay roughly to the 5-minute alternation between the Members.

Mr. Williams, Mr. Hite, if we could start with kind of the big picture? And GAO has done a yeoman's job of trying to work with the department's agencies in putting forth the principles that your statement is talking about of what you need to do up front before moving forward with a major overhaul in your financial management plans.

And yet despite your efforts, we have seen some challenges in how that has moved forward across the Federal Government, including here, where we had about $9 million spent on the initial eMerge2 plan and then a decision not to go that route and start over.

In your combined experiences, in looking at the Federal Government compared to the private sector, how common what we are seeing in the Federal Government, whether it be DHS or we have seen it with DOD a number of times with huge sums—as much as $130 million spent before we pull the plug—how similar is that in the private sector, or does the private sector do a better job of kind of pre-planning and weighing all of those considerations before moving forward?

Mr. HITE. One thing I would mention to start off is it is a lot easier for GAO to point out what should be done than to actually do it. So doing it is the harder part. So I just want to recognize that on the part of the department.

But comparing public sector and private sector, a couple of things come to mind. One of which, similar outcomes, unsuccessful outcomes in the private sector are not going to get the publicity that they are going to get in the public sector. There is just not that kind of transparency that goes on.

So my reading has shown that there are ample examples in the private sector where particularly COTS-based solutions have not been implemented successfully. And the reasons they have not been successful are pretty much the same as we found—have found across the board in the Federal Government.

They deal with the fact that when—the premise or the supposition that is made by some when you are implementing a COTS solution is the product exists. All there is—all you have to do is implement it. What is going to take so long, or what is the big deal? Let us move this thing along. Let us have it in place and operating in a matter of months.

But the reality of it is implementing a COTS solution is as difficult as it is designing and developing and implementing a custom solution. You still have to go through the same type of rigor and discipline in doing so, in clearly defining your requirements and making sure that they are complete and unambiguous that they can be, in fact, implemented properly within that COTS solution.

There is a whole other issue associated with COTS solutions, and that is when you are buying that package, you are buying the embedded processes that go with that. And so, what you are talking about is changing the way that your organization does business.

And so, that is a huge change management challenge that has to be dealt with.

And that is not only just changing processes, but you are actually going to have people change their jobs, change their roles and responsibilities. And so, not only do you have to identify those kind of things, but you have to prepare the people for that kind of change, too. And that is something that you have to start doing up front.

So that is a little bit of my perspective on the comparison of the two.

Mr. PLATTS. Mr. Williams.

Mr. WILLIAMS. And that is consistent with what we have observed also. I would agree fully.

Mr. PLATTS. Mr. Schied and Charbo, looking back and I realize not in your exact position that you are in today, but your role in the department and your knowledge of how the initial eMerge2 plan was laid out, is there lessons learned that you could share with us today?

What maybe could have been done different that would get you to where you are today with the shared services model approach that you are taking versus having spent time and money on the initial approach?

And then also could you expand on what type of interaction up front went on between CFO's office and CIO in deciding on kind of the department-wide approach?

Mr. SCHIED. In terms of lessons learned, I guess there were certainly a mix of sort of the positive and the negative.

I think the positive was the fact that we did monitor the program quite closely. There was earned value management, IV&V quality control process in place that, again, gave us the warning flags literally within weeks that there was a divergence in where we were going. And so, enabled us to be able to take action and to work to try and address that before we got too far down the path.

In terms of sort of going back to when eMerge2 was first launched, as you know, I was not in this position, and there was quite a period where I wasn't at Homeland Security as well, some of the lessons learned I think on the management side were, as I mentioned, first, just sort of the organizational capacity to be able to pull off a big project like this so early in the formative stages of the department.

The amount of staffing that we had within the CFO's office. I joined the CFO's office literally just months after it first opened, and there were 20 people or so in the CFO's office at that time, in total. Most of them, actually, on detail.

So I think there was some underestimation of the amount of management attention that is needed to produce a successful outcome in a project like this. And that perhaps wasn't taken—sort of fully taken into account.

Also, as I mentioned, eMerge2 was perhaps initially a little too separated from the overall realm of financial management within DHS in sort of recognizing some of the issues that existed in DHS financial management. You can't broken processes, ineffective processes, poor internal controls, and just throw them onto a new financial system and expect success.

I think when DHS first stood up—and it really wasn't until the 2004 audit that we had the first sort of full scope review of DHS as a consolidated entity—I think by that time, it became obvious where some of the real internal controls and material weakness challenges were.

And so, I think that sort of wasn't necessarily known at the outset of eMerge2, but was certainly part of what came into play as we went through really the past year, year and a half in trying to assess where we go first. There is a certain, again, prerequisite level of, I think, baseline operations that one needs to master before one sort of goes off and does another realm of transformation. It has been quite transformation enough just getting DHS pulled together, and those challenges still remain.

In terms of—just before I throw it over to Scott—collaboration, eMerge2 did go through the initial investment review process. It was a far probably less mature process back a couple of years ago when it first started than it exists today.

It was actually prior to sort of the second round of investment review process the eMerge2 was going to go through basically to get the green light to move forward when it became obvious that the project wasn't succeeding fast enough, and there was no way we could take it through the investment review process further and expect basically permission to continue on. There were simply too many issues.

So I think having that process and that discipline in place, knowing that you have to go before your peers on the Investment Review Board and justify your program and explain what is going on certainly makes managers accountable as to what they are presenting.

Mr. PLATTS. Thank you.

Mr. Charbo.

Mr. CHARBO. I would concur with what Eugene said. Coming into the department at the time, they asked me to take a look at it from a new perspective of the eMerge2 project before the cancellation, and I think we commented on some of the same points already briefed in the testimony.

But it seemed as if, you know, there was a complex migration strategy of moving many variables at once, which may not deliver some of the outcomes.

Our view from the IT side is not to overcomplicate things but assure, I think, the goal of a clean opinion in the accounting processes. When looking at the requirements, I think again it was overly complex, and I would concur with what GAO was stating about requirements management in this case.

Coming from the private sector, I think we tend to make it a bit more simple, a bit more specific in the result. And I think, in this case, there were large wish lists and then not quite sure how to get there in the project.

The procurement strategy as well may not have been optimal in that case. I think that is not unique to DHS. I think procurement is a challenge across the Government at the present time. So coming up with the right procurement strategy in this case is also a requirement.

Mr. PLATTS. Thank you.

And I certainly don't want to diminish the challenge of this effort and the timing of it, having just consolidated 22 agencies, 170,000 employees, and all the different management systems, then trying to move forward. But you know, so we want to acknowledge that as one of the challenges in addition to the specific financial management aspect of the reform.

And I guess the good news is that this process, Mr. Schied, that you reference that were in place to see where you were, that you were at that roughly $8 million to $9 million and said we don't want to go further, as opposed to going through that $229 million in total, as has happened at DOD already. And have the whole sum spent and then realizing it doesn't do what we need it to do. So those checks and balances certainly were important to not getting any further down the road.

I now recognize Chairman Rogers for the purpose of questions.

Mr. ROGERS. I thank the chairman.

Mr. Hite, you opened up making reference to the need for corporate-like institutional controls, and then you went on afterwards to make the point, you recognized these are easier things to find than to resolve.

But in your opinion, why are we having problems finding corporate-like institutional controls and systems being implemented in DHS? Is it something inherent in the public system, in your view? Why isn't that happening?

Mr. HITE. With respect to the corporate controls, even in an organization that has been around for a while, like, you know, pick your department du jour—Department of Defense—trying to get all the different components to come together and want to pursue a line of strategy that is in the best interests of the whole as opposed to the best interests of their respective parts is a cultural change that has to occur.

And this whole notion of taking an institutional approach to how you manage IT forces that cultural change, and there is an inherent resistance to it. Now you take 22 agencies——

Mr. ROGERS. But isn't there an inherent resistance, even in the private sector, to change, period? Why is the private sector able to bring that change about, and we can't see it in these public entities?

Mr. HITE. I would submit that there are cases in the private sector where they aren't successful at bringing about those kind of changes, and in some cases, those institutions go out of business. There is the survivability of those organizations from a financial standpoint that is a great motivator. You know, fear and fear of failure is a tremendous motivator.

In the Federal sector, these organizations have been around a long time, who came together with all the right intentions from a component standpoint, doing what they thought was the best interests of the component. To drop that because a department was formed and say, "I'm willing to suboptimize what I am doing for the betterment of the department as a whole," would be a tough pill to swallow.

And I think that for that kind of cultural change, a couple of things have to be in place. And I think there has to be, No. 1, there would have to be stable and very strong leadership from the top.

And there would have to be—part of that leadership would be a vision of how, collectively, the parts are going to work together for the betterment of the whole.

And then there would have to be—from the human capital side, there has to be performance and accountability built in to how individuals are challenged, expectations are given to them, and how they are rewarded. And I think those would be the keys to the success and making that happen faster.

I would say there is evidence that it is beginning to occur at the department.

Mr. ROGERS. I am anxious to see that. I mean, everything you described I agree with.

But I make reference to the corporate-like reference that you used in your statement because one of the things I see in the private sector in business is people don't try to reinvent the wheel as much as we do and as much as we see on the Federal level. You find somebody that is doing something that works, and you replicate it.

And DHS, Customs and Border Protection got a clean financial audit, and the financial management systems they have seem to be working. Why aren't we seeing the replication of that in the other agencies? What are they doing right that the other agencies aren't?

Do they have a better technology? Do they have better software systems? Why did they get a clean audit? Why are they making it work and the other agencies are not? And I throw that to anybody. Eugene, you might want to take it first.

Mr. SCHIED. I would say in the case of Customs and Border Protection, knowing what I do of their implementation of SAP, they did it, I think, in a very deliberative process, a very phased process.

The financial reporting, the general ledger was, I believe, the last part of SAP that they stood up after they had done procurement and asset management. So I think that—and that is exactly the kind of what you described in terms of the reuse is what we are now looking to do.

I want to—CBP did something. They seem to have gotten it right. The auditors have come in and this past year were able to give them an unqualified opinion on the balance sheet. We have some other successes within DHS.

Over the past couple of years, the Coast Guard became the service provider to the Transportation Security Administration. They have some audit issues. But from a where do we go forward, you know, trying to decide whether you go for sort of the ultimate, which is, as Scott described, a system that sort of meets all your requirements, has everything that you could possibly want in it, versus just getting something that works and meets the basic needs.

Mr. ROGERS. It would seem logical to me that would be a success of approximation of what Scott referenced.

Mr. SCHIED. Yes.

Mr. ROGERS. To find something that works and replicate it and then work toward to the ideal.

Mr. SCHIED. Right.

Mr. ROGERS. Do you all sense that is what is happening? Do you all sense that is the desire of the department?

Mr. SCHIED. Yes, for financial systems, and I think it is probably true with other systems as well. That is certainly where we are at.

Mr. ROGERS. Great.

I want to shift just a minute to Mr. Williams and talk about human capital. We are going to be talking about that issue more in our subcommittee later. But you talked about the human capital asset problems you found.

Well, tell me more about that. Tell me what shortcomings you found in the area of human capital that stood out to you.

Mr. WILLIAMS. The bottom line in the area of human capital, we looked at it from the perspective of what DHS should be considering as they go forward in trying to implement new systems and, as we like to say in the financial management arena, achieve overall accountability of its operations.

What we noted is that during the 1990's, there was a downsizing, and it was not just in the IT community, but across Government. You had some reductions, downsizing in the area of human capital. What the agency needs to do is to look at basically what are our needs in the area of human capital, and what do we currently have? And basically, we call that a gap analysis.

What mix do we need? What type of experts do we need in these various areas in order to get the systems that we need and to get those systems operational? And what mix of people do we need to address what I consider another major component of trying to address this overall problem of accountability, and that is to put the policies and the procedures in place in order to produce information that is timely, reliable, and available for day-to-day decision-making.

Mr. ROGERS. Let me understand now. What you are making reference to was you saw system shortcomings, not shortcomings in human capital assets?

Mr. WILLIAMS. Well, saying that the agency needs to look at what it currently has in place and come up with a strategy as far as what is needed and make a determination what is the gap between what I have and what I need in order to get to that goal that I am trying to achieve down the road.

Mr. ROGERS. I understand. The reason why I raised that issue is, it seems to me, that we have a real problem. And Ranking Member Meek brought it out in his opening statement. We have a real turnover problem in the upper levels of management throughout DHS. And it seems to me that is part of the reason why we are finding these shortcomings in not just in systems management, but in other areas as well.

Mr. WILLIAMS. Yes.

Mr. ROGERS. I didn't know if you had noted that in your review or not?

Mr. WILLIAMS. One of the things that we point out in the review or in the analysis of documents that we put together is that, first of all, you have to have the commitment from top management.

Management has to be committed to the effort of what is going on in the area of trying to achieve accountability, trying to get systems in place, trying to improve the internal control environment, efforts to eliminate the material weaknesses that the outside auditors have reported on, efforts to get the agency in compliance with

key laws and regulations that the auditors have identified, as well as reportable conditions that the auditors have identified.

You need that commitment from the top, not only in words, but you need it in action. It needs to be a long-term commitment because a lot of these problems that we are talking about today and efforts that need to be underway in order to address these issues and to achieve ultimate accountability, it is not going to happen overnight. So you need that long-term commitment.

Mr. ROGERS. You are also going to have to have stability at the top, and we are not seeing that right now.

Mr. WILLIAMS. That is correct.

Mr. ROGERS. I see my time is about up. So I will yield. I am looking forward to the next round of questions, though.

Thank you, Mr. Chairman.

Mr. PLATTS. Thank you, Chairman Rogers.

I would like to recognize we have been joined by the gentlelady from Texas, Ms. Jackson Lee. Thank you for being part of the hearing, and I now recognize Ranking Member Meek and then Ms. Jackson Lee.

Mr. MEEK. Thank you, Mr. Chairman.

I guess this is for our Chief Financial Officer. I know that you are acting at this time, Mr. Schied. I am assuming you are acting, and someone is holding confirmation at this point. Am I correct?

Mr. SCHIED. Yes.

Mr. MEEK. OK. I appreciate your service. You mentioned something about 2 years at the department?

Mr. SCHIED. I was actually at the department for a year when it first stood up, as the budget officer. I left for a year and then chose to come back.

Mr. MEEK. Good for you. But good for, hopefully, a little consistency there. We keep sending that message, but it is something that we have to deal with in our subcommittee with the department to try to make sure that folks are able to have an opportunity to stay at the department.

Mr. Williams, you spoke in a very eloquent way that it has to be a commitment from the top. But as we have the revolving doors, and I just want to share with the committee this article that was in the USA Today of the "Brain Drain Hits Homeland Security." And it talks about not just analysts leaving, but individuals that are sitting at this table making decisions and making statements before Congress.

I want to just—I guess, Mr. Schied, if I could—ask you a question. You mentioned something about the eMerge2. You say you pulled the plug on it. You used that term "pulled the plug" before a lot of money was spent.

How much money was spent? Because I am a little confused. I have in your written testimony here, it says that the total expenditure on eMerge2 contract with BearingPoint under the implementation of BPA—I guess that is the acronym for it—was $8.9 million.

And then in a letter that was sent yesterday afternoon in response to Chairman Rogers and my letter that was dated on February 8th, on the second page, it says that the first phase of the Program 1, $9.4 million was spent, and then after that, the $8.9

million was spent on 2 for a total expenditure of $18.3 million. Is that correct, sir?

Mr. SCHIED. That is correct. There were two phases of the project. The first phase was largely a requirements phase, and that was the $9.4 million that went to a couple of different contractors, and then $8.9 million was under the blanket purchase agreement.

Mr. MEEK. OK. Since your letter is not in the record, it was sent yesterday. I got it yesterday, and I believe the chairman got it yesterday. It was not in the record, I just wanted to make sure that was a part of our record here.

Mr. PLATTS. Without objection, it is included.

Mr. MEEK. Thank you. Thank you, sir.

Also, I guess one of the reasons why I wanted to get into that area because of the attrition rate at the department. We are going to have a new-found commitment to making sure that this works.

I know that, Mr. Charbo, you have this council that you sit down with, with your other Chief Information Officers or information office at the Department of Homeland Security. I am going to give you some level of comfort, if you ask for it or not.

In our subcommittee markup that we just had under the DHS Management Operations Improvement Act, we gave you line authority. Because I believe reading this report that I am looking at here, that is what needs to happen. You have to have the authority to be able to carry out the mission, and I am concerned about that.

And Mr. Charbo, if I can ask you a question, under your existing—because we have legislation moving through the process that will—it is not about you. It is about your position. Giving you that line authority, will it help you implement the recommendations that the GAO has spent a lot of time on in pointing out?

Mr. CHARBO. It will. I mean, it will take some of the arguments away.

Mr. MEEK. I think what is important now is for, hopefully, the department above your, I guess, pay grade to embrace that philosophy that you just answered. I am glad you answered truthfully because if someone was to ask me do I want line authority, I would say yes because I want to lead, and I don't want to do it by committee.

And I think it is important for us to be able to carry it out if we are going to implement any of these. I mean, what is happening right now and I think the reason why we have the attrition we have, Mr. Chairman, is the fact that folks are doing things by committee. And it is just not going to evolve.

Now there was another point in the report that I may want to come back to, since we only have a few Members here, that would allow us to deal with the question, it was in the report—and I guess it is for the GAO, whichever one of you wants to answer it—on page 11 that talks about fixing requirements dealing with the system costs, anywhere from 10 to 100 times more cost. I'm sorry. Ten to 100 times the cost of fixing it when requirements are defined.

Do you know what I am referring to, sir?

Mr. WILLIAMS. Yes.

Mr. MEEK. I want you to kind of elaborate on that because I do have a question after that, if you could?

Mr. WILLIAMS. OK. We will get our chief technologist to talk to that particular point.

Mr. PLATTS. Do you want to state for the record—and actually, Mr. Rhodes, could we have you stand and take the oath?

[Witness sworn.]

Mr. PLATTS. OK. The clerk will reflect an affirmative answer. Thank you.

Please proceed.

Mr. RHODES. Mr. Meek, the variation is you have to think about software development sort of like you are firing a missile, and you are not directly aiming at your target, but you are going to do these course corrections along the way. Well, if you are trying to hit your target and you don't do any adjustments until later on, then you have to burn up a tremendous amount of fuel to hit your target.

Well, here is the same situation. If you don't get clear definition of your requirements up front and certainly if you wait further on to where you are actually in final system integration or certainly if you are in deployment or in operations, then it takes a tremendous amount of money per line of code to fix it.

And the greater concern associated with that is the problems that you introduce trying to fix things that arise. You fix one problem and make five more. So it is not just that one problem now costs you a lot more money. It is that problem, plus the other five you made now cost you a lot of money. You have to fix it up front rather than on the back end.

Mr. MEEK. OK. Well, that comes down to the implementing of the program, especially under our new way of doing business, I would assume, at the department.

Mr. RHODES. Absolutely.

Mr. MEEK. So that is so very, very important. I see that my time has expired.

Hopefully, Mr. Chairman, we may get another round of questioning, and I can get a little further clarification. But thank you for that explanation. I yield back.

Mr. PLATTS. Thank you, Mr. Meek. And we do plan to come back around.

And before we move on to Ms. Jackson Lee, the previous witness, Mr. Keith Rhodes's title, Chief Technologist at the Government Accountability Office. So that we have that in the record.

Thank you. Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman.

That is about the way I feel. Let me go back to just an old contract that may be just that because it is in the history. And I just wanted to find out when the blanket contract was given to BearingPoint and SAIC, two of them, it looks like one was given in 2003, and then a subsequent one was given, and it was subsequently put on hold. After less than a year, however, the CFO put eMerge2 on hold.

Did any of these contracts have performance provisions to them? Who can answer that? Measuring sticks of their performance? What is the terminology of a blanket contract?

Mr. Schied. That is a blanket purchase agreement.

Ms. JACKSON LEE. Right.

Mr. Schied. That meant that there was going to be an overall $220 million project or $229 million project divided up into specific task orders. And in the case of the blanket purchase agreement for eMerge2, we had a first task order. It was a firm fixed-price task order for $20 million. There were specific——

Ms. JACKSON LEE. And so, it was task specific? You do this task for $20 million?

Mr. Schied. It was actually a series of tasks, a series of deliverables. And there was a schedule associated with that, and it was that each of the tasks in the various schedule that BearingPoint was to follow that allowed us to track their progress and to know in a fairly short amount of time that there was a divergence between their performance and what the contract called for.

Ms. JACKSON LEE. And did you all track the performance?

Mr. SCHIED. Yes, ma'am.

Ms. JACKSON LEE. And what did you find? So, in essence, you had performance standards? I mean, what did you have to assess whether the work was being done and done timely?

Mr. SCHIED. There was a project plan that identified everything that was supposed to be done under the contract. And then as products were delivered, they went through an acceptance process by the Government to determine whether or not the products that were being submitted met what was called for under the contract.

Ms. JACKSON LEE. I guess we don't have an IG here. Is there someone that believes that was this an effective approach, Mr. Schied? Was this an effective approach?

Mr. SCHIED. Oh, I would say that it was in that we, again, quickly found out that there were problems, that the products that were being delivered weren't on time. They weren't acceptable. There is actually a chart that looks like this that we used to track the progress, and you will see a fair amount of red there. That indicated that there wasn't success that we had expected.

So that, again, we, within a matter of weeks, realized it was not going right, called essentially at first a timeout. Ultimately decided that we were going to abandon that task order altogether. And rather than pay the $20 million, which is probably what costs were incurred, we wound up paying under this particular task order $6 million, which was the value of the products that we had ultimately accepted.

Ms. JACKSON LEE. Was this a settlement without court? Was this an internal, inner response that you got working with the company, saying that they had not performed?

Mr. SCHIED. Yes. Correct.

Ms. JACKSON LEE. And so, the only amount that you paid was $6 million?

Mr. SCHIED. Well, there were a couple of different contracts. And under this blanket purchase agreement, there were two different task orders.

Ms. JACKSON LEE. So you total up to what?

Mr. SCHIED. Again, under this particular task order or under the blanket purchase agreement, this one was $8.9 million.

Ms. JACKSON LEE. OK. So let me just in the course of that backdrop, are you now prepared to describe how eMerge2 the contract

will be designed and awarded to ensure the best value for the taxpayer?

For example, will the contract be open to full and fair competition? And how do you plan to structure the contract to ensure that the contractor delivers on time at or below cost? And are you somewhere in this process where the Homeland Security and the merger of all these different accounts can finally get a hold of the enormous stream of money that seems to be pouring out with no supervision, no checks and balances?

Mr. SCHIED. At this point, we are going through a replanning phase. I believe at this point, we have abandoned any notion that we are going to go back and rebid that contract, that blanket purchase agreement that we had initially entered into.

We are taking a totally different path. We are looking at reusing investments that have already been made, either through the OMB lines of business or leveraging existing investments that have been successfully implemented within DHS.

I don't see that there is going to be another contract like there was with BearingPoint. We have decided to go a different route. We believe it will be less risk and less costly.

Ms. JACKSON LEE. But I am sorry. Can I just hear the different route that you are going?

Mr. SCHIED. Oh, certainly. We are going through each—there is a DHS—when eMerge2 was initiated, at that time, looking across the systems that were in place within DHS, there were notable weaknesses in all of the systems. None of them completely met, for example, the JFMIP requirements.

Since DHS came together in 2003 and since eMerge2 was initiated in 2003, there have been a number of changes. OMB has endorsed a lines of business approach. Customs and Border Protection has implemented successfully a core financial system. The Coast Guard has upgraded their core system and taken on the role of a service provider. The Secret Service has implemented a new system.

So the environment has changed quite a bit since we initiated eMerge2. So it was a combination of factors of not being successful with where we were going with eMerge2 and seeing that the environment changed and there were opportunities that we could leverage that is taking us a different direction.

Ms. JACKSON LEE. Mr. Chairman, I thank you for the indulgence. I was going to ask for an additional 1 minute. I was going to ask unanimous consent for an additional 1 minute.

I would just say to you that I know that the hearing has been going on for a while. I was in a Science Committee hearing. So I am directing this to the attention of the chairman.

The gentlemen here are certainly fine public servants, but I am just shocked at the repetitiveness of what keeps coming up about expenditures. I know this is on one particular area, and I hear the acting director, and I appreciate his commentary. But $20 million was already spent, and they had to just let that go.

In New Orleans, that is a separate story, but I think this is an important, enormously important challenge that we have, and I don't know how we are going to complete it. But certainly, there

needs to be a great deal more work because money just seems to be spilling out with no accountability.

And I don't know if bells are ringing, but let me just pose a question that maybe we can get—there are reports here, I understand that. But maybe we can get, at least pointedly on this issue, is just what money we lost? What money has been wasted in sort of a lump sum?

And I yield back.

Mr. PLATTS. Thank you, Ms. Jackson Lee. Appreciate the challenge here with schedules of us having to be at three or four different spots at once throughout the day.

We did have earlier testimony about the sums, the $8.9 million, and in the written testimony that goes into some detail of how it was spent. And certainly if there is a specific followup question you would like to submit, we will be keeping the record open for 2 weeks as well, if there is something more specific you would like them to provide.

I want to pick up kind of where we were there with Ms. Jackson Lee on the cost and certainly in the intent of this hearing is to learn of what has transpired and, as asked earlier, what lessons have been learned and, hopefully, what knowledge has been gained, even though you haven't gone forward with the department-wide eMerge2 program. What did you learn from the dollars spent that you can now put to good use with the new approach?

And so, that we are being responsible with taxpayer funds. And especially for this department, it is so critical because any dollar that we do lose is a dollar that is not available to actually be out there defending the country and our citizens. So your work is critically important to the lives of our citizens and to their security.

With the new approach, originally you envisioned the department-wide approach, $229 million. And now with the new approach, is there a dollar figure? I know in the testimony we talk about that you have $48.4 million available in the current fiscal year. You have asked for an additional $18 million in the 2007 President's budget. So right there, we have about $76.5 million.

Do you have a figure, taking this new shared services approach? What do you envision total cost being as compared to that $229 million?

Mr. SCHIED. I think it would be a bit preliminary for me to really give you very finite estimate. Let me say in terms of the work that was done to date on eMerge2, there are a number of products that were produced under the original—under the money we basically already spent that will still be, I think, quite helpful for us going forward.

For example, all of the requirements that were identified. Rather than looking to find a COTS system and to build that out to meet all of the requirements, it serves as a useful reference model when assessing other systems that are in place to determine what gaps there were.

That is, what did we want? What can we get out of one of these existing systems? Where are the gaps, and what do we do about closing the gaps? Either decide that it is not that important or decide that we are going to conform, or obviously, we will need to conform to what is in place, but is there something about what was

in the original requirements versus what we would be moving to that, going forward, say, if we were to reuse the CBP system or the Coast Guard system that we would want to keep an eye on to possibly upgrade at some point in the future?

A lot of the costs are still going to be the same. That is, there was under the original eMerge2 project, there was going to be a data warehouse to give us greater visibility, to give management greater insight into information. And that will still be a part of the project and probably even more importantly so.

The cost of cleaning up data and migrating components from the system we are on now to whatever the new target system will be, those costs will still be similar. I think in terms of total project range, quoted probably in the order of $150 million to maybe $200 million.

And so, I think it is probably less expensive than where we were going before. It will also be stretched out, I think, over a greater period of time versus where we were going before.

Mr. PLATTS. On that specific point, one, my hope is I understand you can't give an exact figure or exact numbers, but in that saying it is a little preliminary, it kind of comes back to where we started is the hope that there is a pretty definitive plan of where you are going that should give you some guidance of what your costs are going to be as opposed to saying, well, we know we are going to spend $66.5 million, but not really know what that end cost is going to be.

Well, that gets into the issue that we need to know that now, not a year from now, well, it is actually going to be $300 million, not $150 million. So that does concern me that there has not been a better fleshing out of what that is going to be in the end.

Mr. SCHIED. Well, we are still deciding just sort of who will be sort of clustering around. I mean, I want to reuse systems, but I don't know at this point whether I am sending everybody to one system or I am sending people to perhaps two different systems, if they will be inside the department or outside.

That is part of the planning phase that we are going through now and that I foresee somewhat will depend on the timing of the confirmation of the next CFO, for him to be able to put his stamp on it. But sometime in the May/June timeframe is when I want to take it back through the investment review process.

Scott right now controls all of my money, and he is pretty hard about making sure that before I spend it, I know what I am going to do with it.

Mr. PLATTS. Well, Scott, that is a good approach. Stay focused on that approach.

On the timeframe, May to June, as to when you kind of think you will have that plan and come back to that review, you talked about it may be over a longer period of time because originally, in the original plan, it was by this year, 2006——

Mr. SCHIED. Right. We would be up on that.

Mr. PLATTS [continuing]. We would have that department-wide plan. So now we are kind of starting over. Do you have a timeframe that you believe you are going to be able to pursue?

Mr. SCHIED. Well, I mean, it is complicated by, again, our recognition of simply the challenges we face in terms of improving fi-

nancial management in DHS. Most of the—many of sort of the first wave of components that were to migrate to a new system are currently being serviced by Immigration and Customs Enforcement. They contribute in a fairly significant way to the material weaknesses that we have in the department.

Mr. PLATTS. Right.

Mr. SCHIED. I walk the line between how fast I can say get their customers off their system and being serviced by somebody else and how much I need Immigration and Customs Enforcement to be able to fix the problems they have, which go not only to servicing, say, me because I am a customer of them, but also what supports their mission.

I am at the point now where I have to focus probably for the next 18 months on Immigration and Customs Enforcement and the Coast Guard, improving their material weaknesses and improving controls before we are really ready about moving people onto different systems.

Not to say that a lot of the work can't happen—there is work that can happen concurrently. We are not going to be sitting around for 18 months, figuring out what we are going to do with eMerge2. But it is not going to be like a September 2006 kind of decision at this point.

Mr. PLATTS. And you touch on exactly where I was going to go next. I am going to wait until we come back around to the next round. But on those centers and the problems that some, ICE and the Coast Guard already have and the ability to actually migrate within the department given some of the challenges that you have. But I will come back to that on the next round.

I recognize Chairman Rogers.

Mr. ROGERS. I want to stick with Mr. Schied and go back to your reference to leveraging existing programs or investments. Tell me more about what you mean by that.

Mr. SCHIED. Well, what happened over the past couple of years while eMerge2 was not making success, there were a number of successes going on within DHS. The Coast Guard became a service provider to TSA. That is, TSA was on Transportation's system. They weren't happy with that. They were going to be a part of the eMerge2 solution, but they wanted to move fairly quickly, quicker than we were going to schedule them for eMerge2.

And so, they approached the department, along with the Coast Guard, asking to be able to move from Transportation onto the Coast Guard system. Both of them had been in Transportation together.

But CFO Maner basically green-lighted that, allowed it to happen. And in 2005, TSA got not only the systems, but the financial services through the Coast Guard. And it was seeing that worked, and it seemed to work reasonably well, and seeing where CBP had upgraded their system or Secret Service had put in a system, we realized, look, other people are having some successes at this. We are not being that successful.

OMB at the same time has, over the past year, promoted their lines of business. It really, I think, fostered a lot of the same kind of thinking, led us to the conclusion there are probably things here we can leverage.

I mean, I now have half of the department, depending on how you want to measure it, on the Coast Guard, between Coast Guard and TSA being about half of the employees in the Department of Homeland Security.

Mr. ROGERS. So, in a nutshell, you are talking about replicating what they are doing in other agencies?

Mr. SCHIED. That same idea, yes.

Mr. ROGERS. OK. Mr. Charbo, what do we get for $18 million?

Mr. CHARBO. I think—as Eugene pointed out, I think the one deliverable they have is the requirements baseline. That is reusable. That is not a short-term tasking. That is not an easy tasking. As has been pointed out, we have had 22 different systems and components that we were trying to bring in, all with the different wish lists of wanting to get to a different objective.

So I believe what they got is that understanding of where those requirements are and some of the documentation it would take to move forward.

Mr. ROGERS. I want to go back and talk a little bit more about human capital. You made reference in your comments earlier that you were one of the people who were with the CFO's office when the department was originally stood up. Is that not correct?

Mr. SCHIED. I was.

Mr. ROGERS. You were?

Mr. SCHIED. Yes.

Mr. ROGERS. I am sorry. I got the wrong note on the wrong pad. What percentage of those people are still around?

Mr. SCHIED. Percentage wise, very few. I mean, I could probably—again, there were maybe, a rough number, 20, when I joined, and it was shortly after DHS was stood up, actually in May 2003. I am guessing there is probably maybe one or two that are actually still within the CFO's office.

Mr. ROGERS. In your opinion, is that a significant factor in the problems that we are talking about here today in these management systems, or is that really an aside?

Mr. SCHIED. I think specific to the CFO's office, it is somewhat an aside. I think the overall issue, sort of the bigger issue is just the number of people versus the turnover.

There certainly has been turnover, and particularly with the office that is managing this particular project, there has been quite a bit of turnover, particularly since we decided to change direction. It is not really what the team envisioned.

Mr. ROGERS. The turnover throughout these departments, whether it is in the CFO's office or information systems, you don't think that personnel turnover is really the big reason why we are having problems?

Mr. SCHIED. Oh, I think it does—I think it adds something to it. I would say particularly where we are at today versus where we started out, I mean, today, the CFO's office is somewhere between 80 and 90 staffed at versus the 20. I mean, when things started out, it was just very, very scantily staffed. Certainly some turnover does play its role, too, though.

Mr. ROGERS. I do think it was Mr. Charbo that made the point that you saw real problems in the procurement process. Was that you or Mr. Schied?

Mr. CHARBO. I did make the statement that——

Mr. ROGERS. Tell me about the shortcomings that you see in the procurement process.

Mr. CHARBO. Well, this is in general. It is awfully difficult to put together procurements in Government that are sort of focused on performance based that meet the general outcomes. I mean, often we have multiple procurements that overlap that you need to align those, integrate integrators toward a common goal.

The timelines certainly are a challenge in a lot of the procurements. I mean, that is my perspective also coming in from outside of Government. I think that is a difference. You were asking differences earlier. I think that is a clear difference, and being able to make decisions and procure those and start the projects on a faster note.

Finding the right vehicles, going through the processes, answering the questions that come in. That takes a long time, and that puts a burden on important key projects.

Mr. ROGERS. All right. And the last thing I want to ask about is this "F" that for the 3rd year the department has gotten from the Government Reform Committee's annual assessment, and I throw this out to anybody. Why is this continuing to happen?

Mr. CHARBO. Let me—I will comment on that. I think the first thing is, is coming into DHS, again, I changed the project around. You know, where we were is not where we wanted to be in that certification progress. I believe we had 20 percent or less of our systems certified and accredited.

We made it a key objective. It is one of my major initiatives. We had the Secretary make it one of his major initiatives. He wanted to make it that. We had him kick the project off at an IT security conference last October.

And since that point, we are at 62 percent of our systems. Our goal at this point is we wanted to be at least 50 percent complete. So we are on target of meeting our 100 percent by the end of the year. That is our goal. That is our objective.

We have made our executives accountable for that goal. They don't have any other performance mark. We made it real easy for them. Your goal is 100 percent certification and accreditation.

So that is where we are moving toward. I think we are on the right plan, and we are looking to change that "F" next year.

Mr. ROGERS. Thanks a lot.

Mr. PLATTS. Thank you, Chairman Rogers.

Ranking Member Meek.

Mr. MEEK. Thank you, Mr. Chairman.

Mr. Charbo, I want to ask you a quick question. I know that your predecessor, Steve Cooper, planned to develop the department-wide IT strategy plan. That plan was supposed to be released in the end of 2004. The plan still has not been released. Two years have passed, and the department has spent millions, if not billions, on technology without having a strategic plan.

Do you believe that the department needs to have a strategic plan? And if I missed something and they do have a strategic plan, please share it with me.

Mr. CHARBO. We will share it with you. There is a department strategic plan, and our IT strategic plan does align with that de-

partment-wide plan. We are also in the process of creating a new strategic plan for IT. But we have a document that is our IT strategic plan, and we could share that with you.

Mr. MEEK. When was that document developed?

Mr. CHARBO. I believe it pre-dates myself as well. I am not sure of the exact publish date.

Mr. MEEK. OK. We would like to get a copy of it——

Mr. CHARBO. Sure.

Mr. MEEK [continuing]. So we will know exactly what is happening.

Also, I guess this is for you, Mr. Hite. I understand that there was some mention of the Coast Guard and the whole integration, but I understand that the Coast Guard is servicing TSA for its financial management activities. Please explain how that works specifically as is each component running the same system, or has the same system been customized for each?

And please explain the difference between consolidating them on the same system and allowing them to have similar core systems with customization? What impacts does it have on integration efforts?

I am asking that because this is all going as we start to step off again to hopefully not step back in the same hole we just got out of. You can kind of elaborate on that a little bit.

Mr. HITE. I will actually ask my colleague, who is the financial management expert, to respond.

Mr. MEEK. Whichever person that can answer that question better. We are all for the best information.

Mr. WILLIAMS. OK. Basically, when you are talking about a service provider, it is similar to the National Finance Center that provides a payroll service for various agencies in the Federal Government.

You have your operation in which you are processing transactions, be it accounting transactions or what have you, and that information is processed. You have policies and procedures within your organization as to how you are going to operate or your concept of operations. And information through various means is provided to the service provider. It could be manually, electronically, or what have you.

That service provider would then actually process that financial data, that information, and produce reports and provide that information for the entity or the organization that it is providing the service for.

Mr. MEEK. So I don't think they have the same system. That is my question. I mean, they don't have an individual system, a customization. Is that needed?

Mr. SCHIED. The Coast Guard and TSA do use two different instances of the Oracle system that the Coast Guard has in operation. That was part of the agreement when TSA came over. There were a number of improvements that they wanted to see made.

Again, the Coast Guard does have a number of cited weaknesses. The TSA in assessing the Coast Guard system wanted some improvements. And if the Coast Guard—I think the Coast Guard, even if they didn't become a further service provider, very much wants to be able to standardize on the TSA instance of the system

because I think they see it as an improvement over what they had, and that will just take some time and money for them to do that.

I think if anyone is a service provider, they generally want to have a single instance of the system, the single version that all of their customers are serviced on rather than trying to operate multiple and somewhat different versions of the system.

Mr. MEEK. Yes. And you can see where the concern comes in. Even when you look at personnel issues or you look at mission, there are a lot of, you know, "This is my little spot here in Department of Homeland Security, and don't you dare cross that line."

I mean it's almost like Mr. Charbo here, who has a great job. They have this council, and I don't think that there is a person at the head of the table who says, "Well, we talked about this at the last council meeting. Why don't you have it?" And no one feels a level of urgency to carry out any of these reports that we have.

Mr. Chairman, I keep driving to that because we have a situation where taxpayers' money was wasted and national security was jeopardized. And you know, this is not about the crop report, you know, as it relates to corn or whatever the case may be.

I don't want the National Corn Growers Association to get upset with me, but the real issue is this, is that this is national security. And you know, I feel and Chairman Rogers, we tried to address many of the management issues in our mark. But I think that it is important that we look at when you say "best practices" or things that we have learned, I think that we have something to learn as policymakers.

We believe that we have a department that we can say, "Well, this is the way it should be done because we are the representative of the American people," and you say, "OK, fine." But you go back to the department, and then you have these little kingdoms that are out there, and they all have gates and drawbridges and all of those different things.

And unless we give you the authority, which we have, in your case, to be able to carry out the mission and look at a GAO report and say, "OK, fine. This is what we are going to use as our beacon of light toward improvement, then let us do it."

I don't know. Maybe I should buy lunch for you every Friday. I want you to stay in place so that we can get this in line. You know, I am joking. I am trying to be a little funny.

But at the same time, we have to have a mission statement that will carry on even when the next person comes into the office, saying, "Well, this is what we already have going." Because someone could look at it and say—it is like a letter almost. If I write a letter in my office, I hand it to my senior advisor. She looks at it. She changes it. It goes to the chief of staff. He looks at it. He changes it.

And so, everyone starts changing this letter, and sooner or later, it is going to lose the original intent that I had tried to, I guess, share with the person I was writing the letter with.

But Mr. Chairman, I believe we are going to have to address it because I think we have people here, people of good will who I know everyone at that table is for national security and for accountability and for saving the taxpayers money. But I think that

we are going to have to further dig into how can we hopefully continue to fine-tune and sharpen?

I think the department is a pencil and is dull, and we just need to sharpen it because when it is dull, it is kind of hard to write with. I think that is what you all are going through on a daily basis. We just need to get down to the bare facts of what is needed. That is difficult, and we understand that, but we don't want to have to legislate in haste.

I think the department was, even though there was some thought went into it, it was a kind of "We need to do this now. So let us do it." And now it has happened. Folks are getting more cemented in and in quick-drying cement, saying that this is the way the cookie is going to crumble. It doesn't work, especially when we are trying to make this happen.

Mr. Chairman, that would be the conclusion. I won't have any closing statements. I wouldn't want to ask for another round. But I just want to thank you and Chairman Rogers for putting this hearing together. I think it was very insightful not only for me, but also for the staff that is listening.

Some of the questions were answered. We were able to get some good things into the record.

Mr. PLATTS. Thank you, Ranking Member Meek.

And your point about getting to the bare facts is very important. And one of the things through the legislation that the House and Senate adopted with the department is the audit internal control is to try to get to that bedrock of the information capturing and then build from there forward. That, actually, I plan to get into a little bit in questions in the next round for myself.

And your counsel that we really take what we learned and put it to action here is something that if I have the number right, I think GAO has done about 40 different reports in this general area, and the importance of the department, both our CFO and CIO to really lean on GAO for the knowledge they have as you move forward and to stay on the right track.

The wealth of knowledge is there to be embraced and acted upon and to see GAO as a friendly partner, you know, to work hand in hand with you as you go forward.

Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Following the line of questioning that has persisted all afternoon, I want to try to get to another component. Mr. Charbo, if you would? We know when we are talking about best practices and information technology, it calls for another component, which is the human capital.

And I think some of my colleagues have mentioned some of our concern and maybe even disappointment at the seeming revolving door. Unfortunately, it is a very large department, and we are recognizing that more and more.

When it first started, the Homeland Security Department was 180,000 that we thought we were putting together. In the course of that, of course, in the merger, we are sure you lose people. But it seems that we have had a tough time.

I want to know does the department now have sufficient information technology, human capital, the right skills to effectively carry

out its mission now and in the future? If you answer yes, how do you know that DHS and the components have this capability? What is the analysis that has been performed to determine the capability? And if you don't feel we are there, can you explain the reasons why not and whether there is a plan to do so?

And I also want Mr. Hite to comment on the human capital question. Mr. Schied, I would be interested in your overall view as to this fact that DHS did not receive a clean financial opinion in 2005. And we may have gone again over this, but how are we prospectively going to achieve that clean opinion as we look toward the future? And how do we give comfort to Americans that we are actually utilizing their tax dollars efficiently?

Mr. Charbo.

Mr. CHARBO. I think one of the—addressing the IT human capital. We have a heavy contractor utilization in the department. So a lot of the gaps that we have done some analysis for, and we have prepared a plan. Even our conference report and the appropriation required us to produce a document this year that identified it, and that goes hand in hand with what the OMB requirement is, is to do the IT human capital gap analysis as well.

So we have done that. We are identifying solutions or ways that we can mitigate those plans. Primarily, that is for a lot of the higher grade project/program management level positions. Some of the unique security or network administration positions that we have. Those are some of the areas that have been identified as gaps. But the tendency is to fill those with contract support in order to continue the systems operating and the mission moving forward.

So we have done the initial analysis, and we are beginning to fill the gaps and publish that report.

Ms. JACKSON LEE. But are you telling me that you are using mostly contractors as part of the human capital?

Mr. CHARBO. At the department. At the department, a lot of the IT positions, which typically aren't identified as inherently Government, are filled with contract support.

Now you need Government employees to supervise those contract employees. So, as we do the gap analysis for that, we have identified that solid program managers, solid IT project managers are areas that we need to fill in more robust.

We look for lots of authorities in that area. Certain components have some direct-hire authorities. Others do not. So we are trying to sort of level that playing field. That is one of the gaps identified. That is one of the things that we would ask for some support in getting.

Ms. JACKSON LEE. You don't think that undermines institutional knowledge?

Mr. CHARBO. Using contractors?

Ms. JACKSON LEE. Yes.

Mr. CHARBO. No. I think that is the gap analysis that we have identified at the upper levels, the managing positions for IT, that is where we look for that institutional knowledge. There are a lot of IT positions that are administration or pulling cable, development. I mean, most of that is done on a contract basis.

Ms. JACKSON LEE. Thank you.

Mr. Hite.

Mr. HITE. Certainly. I will speak to strategic management of IT human capital at both the program level, the component level, and the department level because you want to do it at all levels. And basically, what we are talking about is understanding what is the suite of functions that we need to perform to execute this program or to execute a component's IT mission?

What are the core competencies associated with those? Who do we have onboard now? How do they match up against those core competencies? Do we have an inventory of those skill sets? What are we going to need strategically going forward on a continuous basis? Where is that gap? And then what are our strategies for filling that gap?

And contracting for services is part of strategy, but also certainly through hiring and retention and training are other strategies as well. Our work has shown at the program level, some of these large programs that we have looked at—for example, the ACE program—that kind of strategic approach to human capital management isn't going on. They recognize it. They intend—they have represented to us that they are going to work on that.

At the component level, CBP, for example, which is the component that ACE resides within, that hasn't happened. They recognize it, and they have represented that they are going to work on that.

At the department level, I look forward to seeing the IT human capital strategic plan that the—Mr. Charbo referenced. We are, by law, required to look at that once it is produced. I have not seen one to date. I am not aware of one.

Ms. JACKSON LEE. Thank you.

Mr. SCHIED. In terms of improving on financial management and being able to provide some assurance, some positive assurance about the controls that we have in place, I guess I would point to a couple of initiatives that we have underway this year different from what we did last year.

As you know in 2004, we had 10 material weaknesses and a disclaimer of opinion. And in 2005, we had 10 material weaknesses and a disclaimer of opinion. Obviously, something didn't work last year in terms of making the improvements that were expected. I think some improvements were made, but I was frustrated at the rate at which improvements have been made.

So what is different this year? I think several things. First, the way we get out of the hole is through corrective action plans. And in all of the audit—the 10 material weaknesses break down to many reportable conditions, actually probably hundreds of specific findings that the auditors see when they come in and assess our financial statements.

We have been kind of down at too low a level in trying to fix some of those problems. That is, you have to recognize that they all tie back up, and they all report back to—somehow relate back to the 10 material weaknesses. I think we are taking a more holistic approach at how to fix those.

We are getting—and a couple of weeks ago, I wrote the inspector general to engage on the internal controls audit and identified the frustration I have and asked for their more active involvement this

year at monitoring our corrective action plan process. We have changed the process itself.

There is a management directive forthcoming that will identify a corrective action accountability official so that we have some clear lines of who is responsible for fixing which material weaknesses. While it may involve many different players, there is ultimately someone that has to be held accountable to fix each of the weaknesses.

We are improving our ability to track the weaknesses so that, again, similar to what we had with the eMerge2 project, to know when are we off track, is there something we need to do about it? We will have a much more open system and a system that I believe the IG and the auditors will also look at to be able to track whether or not we are making the progress.

What I found last year is you can go through, and you can execute the plans, and you can really get nowhere. And we want to certainly avoid that from coming about again this year.

I think we are in a pretty good position to resolve a number of the material weaknesses this year. If we don't fully remediate them, I would expect that work can be done. It is really about probably an 18-month process to successfully eliminate I think all the weaknesses. We have a good chance of eliminating all the weaknesses. It is a lot of work, and we are committed.

And the last thing I would point out, I guess, too, is most of the weaknesses are identified in two organizations—ICE and the Coast Guard. And in the past year, they have had a renewed commitment. I mean, there's a CFO at ICE that wasn't there before, a new assistant secretary. They have, you know, what used to be a plan that was about yea thick. It is now about yea thick. I mean they have put a lot more thought and effort into it.

I think they have increased their staffing. Likewise, within the CFO's office, we have increased staffing particularly for the internal controls group that is going to be responsible for overseeing our corrective action plans. I think all of those things are going to make a difference.

The Coast Guard is certainly stepping up to the challenge. They have a number of weaknesses that they need to fix. I got an e-mail a couple of weeks ago from Admiral Allen, forwarding me information just sort of out of the blue, showing how they are fixing some of their weaknesses. I mean, it is that tone at the top that really makes a difference as well.

And last week, or actually it was a couple of weeks ago now, Admiral Allen, the Assistant Secretary for ICE, myself, the inspector general met with the Deputy Secretary to talk about progress. Those are all changes that have happened over the past several months and I think increase the likelihood that we will actually make progress and demonstrable progress.

Ms. JACKSON LEE. Wow. Thank you.

The only question is, is that chart in the record that you keep holding up? Is that something that we can——

Mr. PLATTS. I don't think it was in your written testimony.

Mr. SCHIED. I can provide it.

Ms. JACKSON LEE. I would appreciate it.

Mr. PLATTS. Without objection, we will have it entered into the record.

Ms. JACKSON LEE. I thank you, Mr. Chairman.

Thank you very much, both, for the hearing.

Mr. PLATTS. Thank you, Ms. Jackson Lee.

Want to come back to the issue of the shared services and the center of excellence approach and first get an understanding that what you are envisioning with the new eMerge2 approach is basically in line with what OMB talks about with their centers of excellence, you know, line of business for financial management.

And is that a correct understanding that it is one and the same?

Mr. SCHIED. It is in alignment with, but I guess I would—I don't know that I could tell you it is necessarily one and the same. That is, basically, OMB says that their policy is that you will migrate to one of their particular centers of excellence, or you will yourself become a centers of excellence provider beyond your own agency.

And OMB allows for certain exceptions to that, and I think we are one of the exceptions, and we are working closely with OMB on this. That is, we want to sort of apply a similar concept within DHS. I am not, at this point, interested in going out and selling my services to other Federal agencies.

Mr. PLATTS. Now make sure, because we worked through this with OMB, and my staff will correct me if I get this wrong from our hearing with OMB, that it is exceptions, but not with the actual systems, the financial systems. There is a mandatory. You are either a center of excellence or you migrate to one. I think in that aspect, I thought it was mandatory that you have to do one or the other?

Mr. SCHIED. I guess I understand it a little bit differently. I mean, certainly, we are not—I am not precluding at this point that some or I guess potentially even all of our systems will be met through OMB centers of excellence. I guess we are taking a somewhat broader approach within DHS in that not only do I want to migrate and consolidate systems, I am also interested in doing the same with the services because I think——

Mr. PLATTS. And ideally, I think that is——

Mr. SCHIED [continuing]. Hopefully that is where you will get the bang for the buck in terms of efficiencies, a smaller control environment, fewer systems, fewer processes in place.

Mr. PLATTS. Are you working with OMB in assessing Customs and Border Patrol and Coast Guard, Federal Law Enforcement Training Center? Are you working with OMB in how you are assessing your own agencies as centers of excellence?

Mr. SCHIED. We report to—at this point, we have weekly meetings with them, and they are monitoring our development of the plan. And they will have to approve whatever plan we have going forward.

Mr. PLATTS. Are there specific agencies? I mean, the ones I am aware of seem to be Secret Service, Coast Guard, Federal Law Enforcement Training Center, and Customs and Border Protection. Are those the ones you are focusing on for your centers of excellence?

Mr. SCHIED. Yes. I guess I had also just sort of—since it has been used several times. I don't really so much see it as centers of excel-

lence, and this may be kind of splitting hairs a little bit. Centers of excellence could connote—if I had, say, multiple ones, say, CBP and Coast Guard—that they would be in some way sort of forever independent of each other.

I think however we consolidate our efforts, we want to be able to also have a relationship between our centers of excellence, so it doesn't make them sound like they are islands unto themselves. I want to have a plan going forward. I think sort of a long-term vision is that we would also look for opportunities to have business arrangements even between the centers of excellence, say, one perhaps focused on one particular aspect of financial management, one on perhaps a different element.

And in terms of centers of excellence concept, those are—the ones you mentioned are the organizations we are interested—I mean, that we have been looking at so far. They are the ones that have the newer, relatively newer investments in systems.

Or there were a couple of considerations that we looked at. How new is their system? How integrated is the system, that is, procurement, financial management, asset management?

I think, long term, you want to drive, do as much integration of those systems as possible to eliminate, say, duplicate entry of financial information in the procurement system and then in the finance system, which is the case today in various places within DHS.

Also their overall financial performance. FLETC, for example, CBP—FLETC hasn't had a stand-alone audit. We are having them go through that, I believe, this year for 2006. CBP has had a balance sheet audit this last year. They passed it. Next year, actually this current year, there will be a full scope audit.

So we want to take into account financial performance. I mean, I think a financial service provider ought to be able to obtain certain standards of, say, excellence in order to be a financial service provider.

Mr. PLATTS. I want to followup on that a little bit. Before I do, though, I wanted to check if either—did you want to make a statement before I continue on? Ms. Jackson Lee, before I continue on with some other questions, did you have other questions or comments?

Ms. JACKSON LEE. No. Simply to thank you, Mr. Chairman, and yield back to you for your questions and look forward to the answers of the questions that we have raised in this hearing.

Thank you very much.

Mr. PLATTS. Thank you.

My, I guess, question or more a caution, I guess, is just to be working very closely with OMB on what they clearly want is mandatory versus what is discretionary and be able to be just done inhouse regarding their Financial Management Line of Business approach.

And in our hearing with the OMB last week, we got a little more delineation. But I think they still have a lot of questions they are trying to answer. So before you get too far down the path with your own entities, that you are certain are going to be line with what they actually are going to demand from you in the end.

Mr. SCHIED. Certainly before we begin to execute on our plan, they will approve the plan.

Mr. PLATTS. Let me switch to just one question on the internal controls audit and kind of where you stand with your contractor and kind of an update on the issue.

Mr. SCHIED. OK. On internal controls, I mean, we have really, I think, over the past year have expanded our thinking quite a bit to not see internal controls and the financial audit and the material weaknesses and the corrective action plans and the audited financial statements as being separate things. They are one and the same thing.

That is the weaknesses that the auditors find in the annual financial statement, they are material weaknesses. And they are material weaknesses that are known to us and that we are attacking. And so, as we go and go about assessing our internal controls, they are not separate processes. It is one and the same.

And the way we are going about it this year is by identifying a couple of the pervasive weaknesses that I think will have ultimate ripple effects down to helping fix some of the other weaknesses cited by the auditors. That is financial reporting, financial management oversight, and fund balance with Treasury. Those are key weaknesses in the audit. They are a part of what our internal controls team is working on fixing, going through assessing what processes we have in place.

By taking the internal controls sort of angle to our material weaknesses, it really gets us to looking at the systemic and root causes of the weaknesses we have in place. That is, we are not just trying to say put a band-aid on a particular weakness. We are looking at how the whole process works. You have to understand what process you have working in place to really get down to the root cause of the problems that you have and how you go about—how you are going to go about fixing it.

I think in terms of the particular audit provision and how we are relating with the IG and the auditor, the IG, the auditor, GAO, I think also with you and your staff, have been kicking about what the actual audit would consist of for 2006. My understanding with the discussions with the IG at this point is that there is going to be some additional work that, in this case, KPMG will do in addition to just the financial statement audit.

They will be looking at our internal controls and how we are managing them through the corrective action plan process that is I think the intention will be for KPMG to work with the IG to assess whether or not the changes that we are putting in place with the corrective action plan are effective. And then they are going to essentially periodically audit us on our performance against the corrective action plan as well as the financial statement.

I think that, plus the ultimate statement of assurance that the Secretary provides at the end of the year, will perhaps form a basis for the IG then to provide some kind of opinion or express an opinion on the internal controls within DHS similar to what GAO does on behalf of basically the entire Federal Government.

Mr. PLATTS. With the focus on your internal controls in that audit and an opinion being expressed, in-house—asked earlier, if I remember, by my colleagues—on the human capital side, do you

believe you are in good shape with your own staff to be able to work with your contractor on the audit?

Mr. SCHIED. It is certainly a growing staff. We have added—for 2006, Congress appropriated several new positions specifically to work—and that was actually the core that allowed us to reorganize within the financial management office to form a core team that will focus on internal controls and the corrective actions.

I think that we have brought the staffing in just the finance office up to about 21 this year. I believe in the 2007 request, there is probably eight more positions that would go toward the finance office as a whole and further bolster our efforts. So I don't think the staffing level is where it needs to be. The budget requests more.

I would also say that we have put within the budget for 2007 requests throughout DHS that the CFO's office was able to put. So, for example, you will see going through the budgets $1 million requested in CBP, in FEMA, in ICE, in TSA; $2 million in the Coast Guard.

It is a total of $16 million, actually almost $17 million that the department is looking for in 2007 specifically related to those internal controls and remediating the material weaknesses.

So we have a good start this year. Congress provided additional positions and about $4 million. That, plus the additional $12 that we are looking for in 2007, will be able to expand the effort.

Mr. PLATTS. And the importance of that effort, of getting to the root causes, as you said, is long term going to make a huge difference, I think, as you go forward. So we want that effort to succeed.

I have three what I think will be very quick answers for the panel that will wrap things up here. First is just with Mr. Williams and Mr. Hite, in hearing testimony here today and your efforts day in and day out working with the department and taking this new approach, one of the questions earlier to Mr. Schied was the question of timeframe.

Are you able to give your best guestimate on if we move forward as planned and are successful, when do you think we see the financial house in order at DHS?

Mr. WILLIAMS. It is difficult to say at this particular point in time. When you look at an organization like the Department of Homeland Security that had 10 material weaknesses, 2 reportable conditions, 7 noncompliance with laws and regulations, you are looking at a huge organization that is very diverse.

One of the things that I was glad to hear today is that there is a focus on the internal control issues because we, at GAO, have basically taken the position that achieving overall accountability is not just getting a clean opinion on your financial statements. We have known of situations where agencies have gotten a clean opinion on their financial statements on September 30th, and the books were out of balance on October 1st.

The overall objective of the Chief Financial Officers Act was to have systems, policies, and procedures in place that would produce accurate, timely, and reliable information that could be used on a day-to-day basis.

And I think when you get to the root causes, and that is addressing these internal control weaknesses—these reportable conditions, these other issues that would require new policies and procedures—in addition to just putting a new financial management in place, then you are getting to what the original intent of the Chief Financial Officers Act is.

And a focus on the internal control environment, which is, as I said, what I heard today, I think is a step in the right direction for achieving overall financial accountability.

Mr. PLATTS. And that reason for this committee and our efforts in pushing the importance of DHS being under the CFO Act and then fulfilling the goals of that act.

Mr. WILLIAMS. That is correct. Because while the current administration was committed to the intent of the act, the overall philosophy behind the passage of the act back in 1990 was you want a structure in place that not only is for today, but for 15, 20 years from today. That you are still getting that good accountability that we strive for.

Mr. PLATTS. OK. Thank you, Mr. Williams.

I think we are going to wrap up there, and if we do have any followups, we will do in writing. And any items that you are going to submit, we will be keeping the record open for the 2 weeks.

Appreciate all five of your testimonies and also your efforts day in and day out at GAO and at the department, and the work you are doing at the department certainly is about the safety and security ultimately of our citizens throughout the country.

So, Chairman Rogers, did you have a closing comment? We certainly have been very pleased to partner with your subcommittee and look forward to continued cooperation and work with the department and GAO.

This hearing stands adjourned.

[Whereupon, at 4:57 p.m., the subcommittee was adjourned.]

[The prepared statements of Hon. Edolphus Towns and Hon. Bennie G. Thompson, and additional information submitted for the hearing record follow:]

STATEMENT OF CONGRESSMAN ED TOWNS
DHS FINANCIAL MANAGEMENT SYSTEMS
MARCH 29, 2006

Thank you, Mr. Chairman, for calling today's hearing on the status and future of the Department of Homeland Security's financial management information systems. It's good to be joining with our colleagues from the Homeland Security Committee as we seek to remedy the major financial management and IT problems ailing DHS.

Since its creation in 2003, the integration of DHS and its 22 legacy agencies has posed significant barriers in our efforts to provide America with protection from domestic terrorism and effective natural disaster recovery efforts. Departmental functions for exchanging information and program data among sister agencies are failing, and high turnover throughout DHS leadership is only complicating matters.

In his FY 2006 annual performance plan, the DHS Inspector General cited approximately one dozen major challenges facing DHS in the coming years, with several specifically related to the financial management functions of agency business units. Thus, I remain concerned about the Department's efforts to design and implement its proposed financial management system, known as eMerge^2 , without knowing more specifics about the program or roles DHS key management will have in its development.

Along these lines, I'm hopeful our agency witnesses before us can describe how the offices of the CFO and CIO plan on sharing development and oversight responsibilities for the proposed system. This includes describing for us who will have budget and acquisition authority for the program, as well as responsibility for the development of measures needed to determine if the new system is meeting agency expectations.

Furthermore, I want to know what DHS is doing to ensure that program vendors are sharing in the responsibility for developing a system that is on-time, under budget, and performing at a level it ought to. With so much time and money at stake, I believe these are questions that need to be answered before proceeding further along with this program.

Mr. Chairman, this concludes my statement.

Statement of Ranking Member Bennie G. Thompson
Joint Subcommittee Hearing on "Department of Homeland Security Information Technology Challenges and the Future of eMerge2"

March 29, 2006

- Chairman Platts and Chairman Rogers, I want to thank you for calling today's hearing to examine the challenges faced by the Department in implementing the financial management system known as Emerge2.

- I also want to acknowledge the unique nature of this joint hearing.

- It is rare for the Committee on Homeland Security and the Committee on Government Reform to collaborate in our oversight efforts.

- I believe that this kind of collaboration can yield positive results for the Congress and the nation.

- Oversight of the Emerge2 program is an excellent candidate for this kind of joint effort.

- The ultimate success of the Department's merger of 22 component agencies is dependent upon its ability to construct and implement a system to manage its finances.

- Everything from travel and grants to payroll and major procurements must be tracked as is done in every other cabinet Department.

- If the Department does not have a firm grip on where its money is going, the American people and the Congress will never have a firm grip on where the Department is going and what it is doing.

- The lack of a firm grip on its finances has led the Department to be the recipient of qualified opinions by auditors and placement on GAO's "high risk" list.

- It has even caused one of its component agencies—ICE—to have budgetary shortfalls that jeopardized its operations.

- Emerge2 was envisioned as a system that would provide the Department with the kind of financial accountability it would need to operate efficiently. But it failed.

- Emerge2 failed because the Department entrusted this program to a contractor without providing adequate guidelines or appropriate supervision.

- And today—almost year after it was started—the American taxpayer is left with a $10 million tab but no financial management system. There is only one word to describe this—unacceptable.

- Today, we will hear testimony from GAO about the steps the Department needs to take.

- I strongly urge the Department to listen, take notes and comply with GAO's recommendations.

- While I am happy that we are having this joint hearing, I do not want to be here next year, listening to new testimony about why the Department cannot deliver.

- I want to thank the witnesses and want to say to my Government Reform colleagues—I look forward to working with you on this and other shared interests.

03/29/06 Submitted for the record
By Congressman Meek
2247 RHOB - 3:00pm
Joint Hearing - Dept Hqtrs
Homeland Security

MAR. 27. 2006 7:22PM DHS NO. 1631 P. 10

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

Homeland Security

The Honorable Mike Rogers
Chairman
Subcommittee on Management, Integration, and Oversight
Committee on Homeland Security
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter of February 8, 2006, and the opportunity to clarify the new direction DHS is taking on the ***eMerge²*** project. Answers to your questions are provided in the attached paper. I also look forward to discussing this matter in greater detail at the hearing scheduled for March 29, 2006.

A few general points to the opening paragraphs of your letter may help clarify the overall status of the ***eMerge²*** project. As explained in the answers to your questions, the effort to improve financial systems in DHS, which has been known broadly as the ***eMerge²*** project, has not been terminated. Rather, we are going about meeting our needs in another way. We are seeking to leverage investments in systems that have already been made, rather than implementing something new. DHS is in the process of assessing which organizations, both inside and outside DHS, have resource management systems and offer services that can meet our needs.

We are closely tying our ***eMerge²*** effort into our broader effort to improve overall resource management in DHS. This includes taking the actions necessary to remediate material weaknesses in our financial statements reporting so that we can obtain an unqualified audit opinion. It also includes taking the actions necessary to put DHS senior leadership in a position to provide assurances that our internal controls over financial reporting are in place and working effectively. These are interdependent efforts which our revised ***eMerge²*** plans must take into account.

I apologize for the delay in responding to your letter and would be happy to provide any additional information you may require.

Sincerely,

Eugene Schied
Acting Chief Financial Officer

Answers to Questions Regarding the *eMerge²* Project

eMerge²

1. ***What were the circumstances surrounding the award, issuance of task orders, and termination of the eMerge² contract? What was the total expenditure by DHS for this program?***

DHS Response:

DHS issued two sets of contracts related to the planning, implementation, and integration of a new resource management system.

The first set of contracts was awarded in late Fiscal Year 2003/early Fiscal Year 2004, to BearingPoint and SAIC. This effort was to develop the Department's functional and technical requirements for an integrated resource management solution and to build the resource management portions of the homeland security enterprise architecture. These requirements were approved by all DHS components. The cost of these contracts was $9.4 million.

Based on the requirements developed in the first set of contracts, DHS developed an RFP for the acquisition and implementation of an integrated resource management solution for the Department.

The DHS CFO formed a source selection team composed of a technical evaluation team and a cost evaluation team. After issuing the solicitation and receiving proposals, the source selection team evaluated the proposals and made a recommendation to the Source Selection Official. BearingPoint was selected as the best value choice for the Department. A BPA was awarded to BearingPoint in September 2004, with a ceiling of $228.7M.

So as to minimize the risk of such a large project, the Department structured the project so that we would incrementally issue firm-fixed-price task orders for small, measurable portions of work. The first task order (Task Order #1) was issued for $20 million for solution development and conference room pilot testing. Soon into work on this task order, concerns began to arise regarding the extent to which there was a clear understanding between DHS and BearingPoint on what was to be delivered. Deadlines were missed and products presented to the project team were not accepted. As a result, in February 2005, the DHS CFO initiated a review of the *eMerge²* effort.

Work under Task Order #1 was closed out in April 2005, prior to completion. Based on the work that was satisfactorily completed, the price was adjusted from $20 million to $6 million. As we halted work on Task Order #1, DHS issued a small, finite task order (Task Order #2) to BearingPoint in the amount of $2.9 million. The primary activity under Task Order #2 was to help DHS examine certain component systems in greater

detail. We again surveyed the existing financial systems in the Department against the capabilities to meet core functional requirements, which were derived from the requirements developed during the first phase of the ***eMerge²*** project. In particular, the system at the United States Coast Guard, which used a similar suite of products as proposed under the ***eMerge²*** project and which was already a service provider to the Transportation Security Administration, was examined in detail.

The conclusions reached last fall by the OCFO were:

- The effort that we embarked upon under the BPA with BearingPoint should come to an end because it had not been successful and future action down this path was high-risk;
- DHS' own organizational maturity issues also made the project high-risk; and
- Other viable options to leverage existing investments existed and have been successful.

In short, the DHS CFO concluded that several existing components in DHS had upgraded their systems and improved operations to the extent that viable alternatives to restarting with a new system integrator were possible. Our assessment also concluded that the Office of Management and Budget's Financial Management Line of Business and its Centers of Excellence offered viable alternatives to meet DHS' requirements as well. In December 2005, DHS chose not to exercise the next option year on the BearingPoint BPA, and so the BPA expired. The total expenditure on the second BPA to BearingPoint BPA was $8.9 million.

The total expenditure for both BPA #1 and BPA #2 was $18.3 million.

2. ***What capabilities cannot be achieved using existing systems that the Department had hoped to gain through the development of a new system?***

DHS Response: In general, both approaches should be capable of achieving the ***eMerge²*** objectives, though they differ in terms of risk, timing of capability realization, and cost. However, DHS is yet to select exactly which systems and service providers it will leverage going forward. The initial ***eMerge²*** effort sought to provide capabilities much sooner than will be realized under the revised approach. We have, and will continue to use the requirements developed under the earlier effort to benchmark our movement to alterative solutions.

3. ***What systems were assessed and determined not capable of meeting the goals of a Department-wide solution?***

DHS Response: To date, the following organizations/systems have been assessed to one degree or anther by DHS:

- Internal
    a. US Coast Guard

b. Customs and Border Protection
c. US Secret Service
d. Federal Law Enforcement Training Center
e. Immigrations and Customs Enforcement
f. Federal Emergency Management Agency

- External -- OMB Financial Management Centers of Excellence
  a. Bureau of Public Debt
  b. Department of the Interior
  c. Department of Transportation
  d. General Services Administration

We have not yet definitively included or excluded any organization/system as a service provider, as we are still finalizing the revised end-state vision and 5-year strategy for the new *eMerge²* direction.

4. ***The eMerge² initiative illustrates the Department's challenges in assessing its needs and executing large scale multi-layer contracts. How will DHS apply the lessons learned from eMerge² to strengthen its planning and procurement strategies and processes?***

DHS Response: Although DHS experienced difficulties with the project, aspects of project management worked well. We managed the contract in such a way that enabled us to minimize our risk, identify problems early on, and make course corrections before substantial sums of taxpayer dollars were expended. Our task orders were firm fixed price. We monitored performance closely. And when the risks were deemed too great, we closed out the contract.

The most important strategy to be shared from facing these challenges is the value of having effective project controls. Through the controls established by DHS, it became readily apparent that the contractor's performance did not meet government expectations. Performance problems were documented in Weekly Status Reports, Earned Value Metrics, and the deliverable review process. Because of this thorough documentation, the government was able to close out the contract and pay only for the goods and services that met the criteria for acceptance.

DHS also placed tremendous emphasis on structuring and scheduling work products in small measurable, incremental deliveries, enabling the government to manage the contractor's level of effort accordingly. Instead of attempting to carry out a broad range of tasks in a phased manner, analogous to the 'waterfall approach', large implementations like this should evolve in small increments to enable better performance monitoring.

While the effort to design and implement a new system was unsuccessful, the first lesson we learned, and it is the foundation of our new approach, is that we believe viable alternatives to meet our core requirements exist, so that we do not need to go out and rebid the earlier contract. From seeing where DHS had successful resource management transformations in the past couple of years, such as at Customs and Border Protection and

the United States Coast Guard, we see where implementing smaller and more achievable incremental functional improvements were keys to success. CBP stood their system up in phases over several years. Likewise, USCG made small but important upgrades to their system, in order to support the Transportation Security Administration.

In addition, a lesson learned over the past year is that we must closely link our systems improvement efforts to our more global financial management improvements efforts. DHS has numerous challenges in financial management. We have many material weaknesses to address, most of which are not about systems. DHS needs to reach a baseline level of financial management performance, before we can meaningfully transform DHS. Moving ineffective processes, controls, and organizations onto an improved system is not a recipe for success. Our ***eMerge²*** plans going forward must take into account the reality and the plans of all aspects of DHS financial management.

Centers of Excellence

1. ***How many centers of excellence and centers of need will there be?***

DHS Response: We will not know exactly how many service providers or customers there will be until we finish our revised end-state vision and 5-year strategy for the new ***eMerge²*** direction. We presently have 5 different core financial systems products operating in DHS, and 8 financial service providers. We are in the process of putting together the business case for reducing that number, and the path for how we plan to get there.

   a. ***Which agencies' financial systems are being designated as centers of excellence?***

   DHS Response: This is yet to be determined.

   b. ***Who will make the determination as to which financial systems will be centers of excellence and what will be the criteria?***

   DHS Response: As part of the revised planning effort, we will determine the governance structure for this effort. This will set up the day-to-day oversight of the project. The overall approach is considered a major IT investment, and as such will need to be reviewed by DHS' Joint Requirements Council and approved by the Investment Review Board, whose membership includes the Deputy Secretary, Under Secretary for Management, Chief Financial Officer, Chief Procurement Officer, Chief Information Officer, Assistant Secretary for Policy, and other DHS component heads as appropriate.

   Generally, criteria for determine which service centers we use could include: the degree of application integration; past performance (system and service); the extent to which the system provides required business capabilities; and how the center fits into the overall end-state vision for DHS.

c. Are DHS agencies with internal control weaknesses eligible to be designated as centers of excellence? If so, why?

DHS Response: We have not yet defined which service centers we will use, but as part of our criteria we will certainly consider the weaknesses in internal control. We believe that prior to taking on any new customers, it would be ideal for DHS service providers to have effective internal controls over financial reporting.

We are executing a broad effort to fix the weaknesses already known to us, and to ensure that all aspects of our internal controls over financial reporting are sound. All DHS organizations posses at least some known or potential weakness in internal control, and some of these organizations are currently serving as a financial service center for other DHS organizations.

Where a potential service provider has some weakness, we would need to review their corrective action plans, and determine what the risk would be to them servicing other customers. This is why we are more closely integrating our *eMerge*^{2} efforts into our broader financial management improvement efforts, because of the interdependencies. Our revised end-state vision and 5-year strategy for the new *eMerge*^{2} direction will not only lay out the criteria for being a service center, but will also address steps that must be taken, such as remediating weaknesses in internal control.

d. Will the CFO have line authority over either type of center?

DHS Response: Presently, through the Department's Management Directive on the functional integration of financial management, the CFO has a shared authority over all financial management activity within DHS, including the financial service centers within DHS. DHS has no central service provider under the direct control of the CFO. Over time, we may examine the possibility of consolidating financial services under the CFO.

e. Is there a plan to transform a center of need into a center of excellence? If so, please elaborate.

DHS Response: Our plans are to elevate the efficiency and effectiveness of financial management across all of DHS over the next several years, so that we can obtain unqualified audit opinions and attest to the effectiveness and efficiency of our internal controls over financial reporting.

As we do that, our plan will also lay out, considering factors such as cost, risk, and capability, how we are going to reduce the number of service providers and financial management systems. Those that have the most to offer going forward, and considering cost, will be the ones around which we consolidate.

2. ***Please discuss in detail how the decision will be made to transfer a center in need to the financial system of a center of excellence.***

   a. ***What is the role of the Department's Chief Information Officer (CIO) in evaluating and approving the technologies that will be adapted or expanded through this process?***

   DHS Response: The DHS CIO is responsible for creating and maintaining the DHS enterprise architecture and oversight of all IT projects, including the *eMerge²* Project. Accordingly, the DHS CIO has provided their considerations for architecture, infrastructure, hosting and technological capabilities and will weigh in during the final decision process. The CIO will be part of the revised *eMerge²* governance structure, and he is part of the JRC and IRB that will oversee the project.

   b. ***How will the CFO and the CIO ensure that these technologies will be consistent with the Department's overall information technology and information security goals?***

   DHS Response: When the CFO introduces a new IT solution, the CIO must Certify and Accredit (C&A) that the system is compliant with IT security standards, prior to granting an Authority to Operate. The CIO may grant an Interim Authority to Operate under certain conditions.

   c. ***What role will the agencies with centers in need play in determining which of the centers of excellence is most appropriate for their respective agencies?***

   DHS Response: Potential customer organizations have been – and will continue to be – given the opportunity to evaluate various potential service providers. The Department will take into account Customers assessments and preferences when deciding how to match customers to service providers. But other factors must be considered as well. In the end, the final decision will be made by the project's governance board.

3. ***What is the Department's timeframe for matching centers in need with centers of excellence? What is the timeframe for implementation of these changes once such determinations are made?***

DHS Response: We plan to have our revised end-state vision and 5-year strategy for the new *eMerge²* direction ready for presentation to the DHS Investment Review Board by the May/June 2006 timeframe.

Integration of Financial Information

1. ***Please describe how building a data warehouse, or data center, will provide the CFO with the ability to gather budget information in a timely fashion and to exercise his oversight function.***

DHS Response: We are working on a data visibility initiative which will:

- Consolidate budget information and other resource management data from the Service Centers to support enterprise-wide reporting, analysis, and decision making.
- Support the individual needs of functional domains that comprise the ***eMerge²*** project scope, e.g., acquisition, asset management, financial management, and grants management.
- Implement a data warehouse, executive dashboard and business intelligence tools to create and maintain situational awareness across programs and organizations.
- Provide DHS leadership a comprehensive view of high-level, key indicators to gauge the financial health of the Department and its components on a near-real time basis.
- Improve financial reporting and increase operational efficiency and effectiveness.

2. ***Will the decentralized centers of excellence approach automatically integrate internal control capabilities in the Department's financial management systems, as set forth in OMB Circular A-123 "Management's Responsibility for Internal Controls?" How will you ensure that necessary internal controls are in place to ensure the accuracy and completeness of data, and the consistency of transaction processing?***

DHS Response: Nothing will automatically integrate internal controls capabilities. A major effort is currently underway to bring DHS into compliance with the provisions of OMB Circular A-123. This effort is being led by the Financial Management Division within the Office of The Chief Financial Officer. The primary focus of this effort is on improving financial reporting, a major component of internal controls, across all the Department's financial systems. An audit has been conducted or is in progress for each of the Department's financial systems; and, for identified weaknesses, Corrective Action Plans have been prepared. Our exhaustive implementation effort, which will be reviewed by the Inspector General and our auditors, will help ensure that we get the necessary controls in place.

The decentralized approach to systems, versus a single solution, will increase the effort required to perform audits (because multiple environments have to be considered), but this actually has little or no effect on the overall quality of the results. Part of our consideration for the systems we will use in the future will be how it fits into our controls environment. Furthermore, because corrective actions can be applied to existing systems,

the Department is able to realize improved controls sooner than would have otherwise been provided by waiting for the development of a new system.

Several ***eMerge²*** strategies will ensure that data is accurate and complete and that transactions are processed consistently:

- Migration of customers will cause the affected organizations to examine and cleanse existing data—this activity is expected to improve the quality of data significantly.
- Improvements made to existing systems will correct current deficiencies causing data inaccuracies.
- Implementation of the data visibility initiative will require an enterprise-wide assessment of data meaning and use—this activity is expected to improve the consistency of data and transaction processing.

3. ***How will the Department's centers of excellence approach fulfill the "single integrated financial management system" standard set forth in OMB Circular A-127?***

DHS Response: The new ***eMerge²*** decentralized approach will fulfill the A-127 standard by providing a unified set of financial systems that implement standard integrated business processes in order to provide decision makers with an enterprise-wide view of accurate and timely business information.

PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

February 8, 2006

Via Facsimile and U.S. Mail

The Honorable Janet Hale
Under Secretary for Management
U.S. Department of Homeland Security
Washington, DC 20528

Dear Under Secretary Hale:

In September 2004, the Department of Homeland Security (DHS) announced a department-wide effort to consolidate the financial systems of its 22 components. Recent news reports indicate that the Department's Chief Financial Officer (CFO) has cancelled this program, called Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency, otherwise known as eMerge2.

We are advised that the Department has since announced its intention to utilize existing financial systems rather than develop a new integrated system. Instead of the eMerge2 model, the Department reportedly will designate agencies with well-functioning financial systems as "centers of excellence" and transfer agencies with troubled financial systems, referred to as "centers of need," to one of the centers of excellence.

We would appreciate learning more about the Department's decision to reevaluate eMerge2 to ensure that taxpayer dollars are put to best use. As the Department proceeds with a new, more decentralized model, we request pursuant to Rules X and XI of the House of Representatives that you respond to the following questions:

eMerge2

1. What were the circumstances surrounding the award, issuance of task orders, and termination of the eMerge2 contract? What was the total expenditure by DHS for this program?

2. What capabilities cannot be achieved using existing systems that the Department had hoped to gain through the development of a new system?

3. What systems were assessed and determined not capable of meeting the goals of a Department-wide solution?

4. The eMerge2 initiative illustrates the Department's challenges in assessing its needs and executing large scale multi-layer contracts. How will DHS apply the lessons learned from eMerge2 to strengthen its planning and procurement strategies and processes?

Centers of Excellence

1. How many centers of excellence and centers of need will there be?

    a. Which agencies' financial systems are being designated as centers of excellence?
    a. Who will make the determination as to which financial systems will be centers of excellence and what will be the criteria?
    b. Are DHS agencies with internal control weaknesses eligible to be designated as centers of excellence? If so, why?
    c. Will the CFO have line authority over either type of center?
    d. Is there a plan to transform a center of need into a center of excellence? If so, please elaborate.

2. Please discuss in detail how the decision will be made to transfer a center in need to the financial system of a center of excellence?

    a. What is the role of the Department's Chief Information Officer (CIO) in evaluating and approving the technologies that will be adapted or expanded through this process?
    b. How will the CFO and the CIO ensure that these technologies will be consistent with the Department's overall information technology and information security goals?
    c. What role will the agencies with centers in need play in determining which of the centers of excellence is most appropriate for their respective agencies?

3. What is the Department's timeframe for matching centers in need with centers of excellence? What is the timeframe for implementation of these changes once such determinations are made?

Integration of Financial Information

1. Please describe how building a data warehouse, or data center, will provide the CFO with the ability to gather budget information in a timely fashion and to exercise his oversight function.

2. Will the decentralized centers of excellence approach automatically integrate internal control capabilities into the Department's financial management systems, as set forth in OMB Circular A-123 "Management's Responsibility for Internal Controls?" How will you ensure that necessary internal controls are in place to ensure the accuracy and completeness of data, and the consistency of transaction processing?

3. How will the Department's centers of excellence approach fulfill the "single, integrated financial management system" standard set forth in OMB Circular A-127?

Please provide the requested information to the Committee by March 1, 2006. Should you have any questions regarding this request for information, please contact Heather Hogg with the Majority staff at (202) 226-8417, or Rosaline Cohen with the Minority staff at (202) 226-2616. Thank you for your prompt and personal attention to this matter.

Sincerely,

The Honorable Mike Rogers
Chairman
Subcommittee on Management,
Integration, and Oversight

The Honorable Kendrick B. Meek
Ranking Member
Subcommittee on Management,
Integration, and Oversight

Statement of MI&O Ranking Member Kendrick B. Meek
Joint Subcommittee Hearing on "Department of Homeland Security Information Technology Challenges and the Future of eMerge2"

March 29, 2006

- Thank you.
- This hearing marks the first time that the Homeland Security and Government Reform Committees have held a joint oversight hearing.
- The fact that these two committees have come together today says a lot about the level of concern we have about the Department of Homeland Security.
- No one ever expected the establishment of the Department to be "an easy lift."
- We all knew that it would take a lot of work to transform the Department and get each agency to read from the same play book.
- Yet, the Department has not approached its integration challenges with any "sense of urgency".
- The GAO has stated that successful transformations of large organizations take between 5 to 7 years.
- At the rate the Department is going, I cannot see full integration being achieved by the end of the decade.
- GAO put DHS on its "HIGH RISK" list because it believes that the Department's failure to effectively address its management challenges could have serious consequences for our national security.
- I completely agree.
- That is why I am concerned about the constant turnover at the Department.
- In its short history, DHS has shown itself to be incapable of attracting and retaining professionals with the knowledge and experience to oversee complex multi-year projects.
- Every time the Department loses one of its leaders— be it the Chief Financial Officer or the Commissioner of Customs and Border Protection—progress slows down or comes to a grinding halt.
- Then the new leader comes in, reviews existing work, and makes changes.

- At any given moment at the Department, this cycle is being played out and precious time is lost.
- Even if we had the right people in place, I am not sure that Department-wide integration can be achieved under DHS' current management structure.
- Today, the Chief Information Officer does not hold the purse-strings over the Department's IT projects.
- He also does not have any actual authority over his counterparts in the agencies.
- The CIO must be able to compel compliance on Department-wide priorities, such Emerge 2 or Information Security.
- Today's look at Emerge 2 provides us with a good jumping off point to discuss the problems with the Department's approach to IT planning.
- The problems start at the beginning of the process.
- First of all, there is a lack of planning.
- And as the saying goes—"if you fail to plan, you plan to fail."
- Specifically, the Department has gotten out of the habit of providing system requirements.
- Without requirements, you cannot track performance.
- Another major weakness is that there is no Department-wide Technology strategic plan.
- The Department's last CIO promised to release the strategy by the end of 2004.
- Two years later . . . there is no technology plan, but millions—if not billions—have been spent.
- Clearly, I have some concerns about the way the Department is going about purchasing technology systems.
- I look forward to hearing from our panel today.
- Thank you.