

INVESTMENT MANAGEMENT AND ACQUISITION
CHALLENGES AT THE DEPARTMENT OF HOME-
LAND SECURITY

HEARING

BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT
OF THE
COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

SEPTEMBER 15, 2009

Serial No. 111-60

Printed for the use of the Committee on Oversight and Government Reform



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

U.S. GOVERNMENT PRINTING OFFICE

57-625 PDF

WASHINGTON : 2010

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) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania	DARRELL E. ISSA, California
CAROLYN B. MALONEY, New York	DAN BURTON, Indiana
ELIJAH E. CUMMINGS, Maryland	JOHN M. McHUGH, New York
DENNIS J. KUCINICH, Ohio	JOHN L. MICA, Florida
JOHN F. TIERNEY, Massachusetts	MARK E. SOUDER, Indiana
WM. LACY CLAY, Missouri	JOHN J. DUNCAN, Jr., Tennessee
DIANE E. WATSON, California	MICHAEL R. TURNER, Ohio
STEPHEN F. LYNCH, Massachusetts	LYNN A. WESTMORELAND, Georgia
JIM COOPER, Tennessee	PATRICK T. McHENRY, North Carolina
GERALD E. CONNOLLY, Virginia	BRIAN P. BILBRAY, California
MIKE QUIGLEY, Illinois	JIM JORDAN, Ohio
MARCY KAPTUR, Ohio	JEFF FLAKE, Arizona
ELEANOR HOLMES NORTON, District of Columbia	JEFF FORTENBERRY, Nebraska
PATRICK J. KENNEDY, Rhode Island	JASON CHAFFETZ, Utah
DANNY K. DAVIS, Illinois	AARON SCHOCK, Illinois
CHRIS VAN HOLLEN, Maryland	BLAINE LUETKEMEYER, Missouri
HENRY CUELLAR, Texas	
PAUL W. HODES, New Hampshire	
CHRISTOPHER S. MURPHY, Connecticut	
PETER WELCH, Vermont	
BILL FOSTER, Illinois	
JACKIE SPEIER, California	
STEVE DRIEHAUS, Ohio	

RON STROMAN, *Staff Director*

MICHAEL MCCARTHY, *Deputy Staff Director*

CARLA HULTBERG, *Chief Clerk*

LARRY BRADY, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

DIANE E. WATSON, California, *Chairman*

PAUL E. KANJORSKI, Pennsylvania	BRIAN P. BILBRAY, California
JIM COOPER, Tennessee	AARON SCHOCK, Illinois
GERALD E. CONNOLLY, Virginia	JOHN J. DUNCAN, Jr., Tennessee
HENRY CUELLAR, Texas	JEFF FLAKE, Arizona
JACKIE SPEIER, California	BLAINE LUETKEMEYER, Missouri
PAUL W. HODES, New Hampshire	
CHRISTOPHER S. MURPHY, Connecticut	
MIKE QUIGLEY, Illinois	

BERT HAMMOND, *Staff Director*

CONTENTS

	Page
Hearing held on September 15, 2009	1
Statement of:	
Duke, Elaine C., Deputy Under Secretary for Management, Department of Homeland Security; James L. Taylor, Deputy Inspector General, Department of Homeland Security; and Randolph C. Hite, Director, Information Technology Architecture and Systems Issues, Government Accountability Office, accompanied by John Hutton	5
Duke, Elaine C.	5
Hite, Randolph	28
Taylor, James L.	17
Letters, statements, etc., submitted for the record by:	
Duke, Elaine C., Deputy Under Secretary for Management, Department of Homeland Security, prepared statement of	7
Hite, Randolph C., Director, Information Technology Architecture and Systems Issues, Government Accountability Office, prepared statement of	30
Taylor, James L., Deputy Inspector General, Department of Homeland Security, prepared statement of	19

INVESTMENT MANAGEMENT AND ACQUISITION CHALLENGES AT THE DEPARTMENT OF HOMELAND SECURITY

TUESDAY, SEPTEMBER 15, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:40 a.m., in room 2154, Rayburn House Office Building, Hon. Diane E. Watson (chairwoman of the subcommittee) presiding.

Present: Representatives Watson, Connolly, Cuellar, Bilbray, and Leutkemeyer.

Staff present: Bert Hammond, staff director; Adam Bordes and Deborah Mack, professional staff; Valerie Van Buren, clerk; Dan Blankenburg, minority director of outreach and senior advisor; Adam Fromm, minority chief clerk and Member liaison; Steven Castor; minority senior counsel; and Ashley Callen, minority counsel.

Ms. WATSON. The Subcommittee on Government Management, Organization, and Procurement of the Committee on Oversight and Government Reform will now come to order. And I would like to introduce our newest member, and it is Representative Blaine Luetkemeyer from Missouri. Welcome.

Mr. LUETKEMEYER. Thank you, Madam Chairman.

Ms. WATSON. Today's hearing will examine the state of investment management and acquisition oversight practices for major information technology programs at the Department of Homeland Security. And the hearing will also serve as an opportunity for DHS leadership to explain their plans for strengthening agency oversight, mechanisms governing both current investments and future acquisitions.

Without objection, the Chair and ranking member will have 5 minutes to make opening statements, followed by opening statements not to exceed 3 minutes by any other Member who seeks recognition.

Without objection, Members and witnesses may have 5 legislative days to submit a written statement or extraneous materials for the record.

I would like to wish a good morning to all of our witnesses, staff, and all those out in the audience. And as I mentioned, the subcommittee hearing on investment management stewardship and ac-

quisition strategies for major information technology or IT programs at the Department of Homeland Security will be examined. I welcome our distinguished panelists and look forward to hearing their testimony.

Now, today's hearing by our subcommittee is the first look into the oversight mechanisms used by DHS for governing its portfolio of agency acquisition while examining some of the particulars associated with a number of high-risk IT investment in development that are critical for achieving many of their missions. In fact, roughly \$6.6 billion will be spent this year by DHS on technology-specific programs deemed necessary for both administrative and programmatic functions.

According to the GAO, the DHS investment review process is inadequate and has resulted in a number of poorly performing or failed investments. In fact, nearly all the programs achieved in GAO's most recent work were proceeding without adequate oversight from stakeholder leaders or detailed budget justifications for their funding. These factors contribute to excessive cost overruns, extended project delays and projects that are simply ill-conceived from the outset. The inspector general of DHS offered similar observations and findings in his previous work as well.

It goes without saying that funding dedicated to DHS investments will require stout internal controls and planning processes in order to be successful. We know that previous high-profile investments such as the eMerge financial management systems program failed due to significant deficiencies in the agency's investment planning and contract oversight practices.

I think it is imperative today that the DHS provide us some specifics about the lessons learned from previous failed programs and how we can be assured that such costly failures will be avoided in the near future.

As part of the prior administration, I hope Ms. Duke can explain how exactly we got to this point and whether current circumstances merit moving forward with programs that are extensively flawed. To be fair, I know this is a tall order for her and other DHS leaders to undertake alone. And I implore the administration to become more engaged on these issues by finally appointing someone to head the Office of Federal Procurement Policy at OMB.

And today I am hoping that our witnesses will provide us an updated snapshot of where DHS is by providing specifics about some of those programs deemed most at risk or in a poorly performing state. Hopefully this will provide us a way forward for remedying those issues as the subcommittee continues in its oversight of DHS in this Congress.

And with that, I want to thank our panels for joining us today, and we look forward to their testimony.

I would now like to give time to Mr. Bilbray, our ranking member.

Mr. BILBRAY. Thank you, Madam Chair. Madam Chair, first of all, I ask for unanimous consent that a text of my opening statement be included in the record.

Ms. WATSON. Without objection, so ordered.

Mr. BILBRAY. Madam Chair, I thank you very much for holding this hearing. I appreciate the witnesses for being here. I think that in the short span that DHS has been in existence, I remember the scramble to restructure our system after 9/11. We have just passed 8 years, and I think it's a great time to reflect on our successes and our failures. The concerns that we have, obviously, are always tending to focus on the negative, especially in this committee, because that's our responsibility. We tend to be the bean counters for the Congress in a lot of ways, but mostly not deciding who gets the beans but where the beans went. And right now there's a lot of this that does not look very effective.

I got to tell you, the emergency response and the capabilities of the Federal Government to respond to certain threats are obviously one of the highest priorities constitutionally we bear. We do a lot of things and talk about a lot of things that are not constitutionally mandated. But when it comes to securing our borders, securing our neighborhoods, protecting our community at large for the common good, that's definitely one of the major focuses of our Constitution.

And you may not know, I was born and raised on the border with Mexico down in the San Diego region. My district is very close to the largest port of entry in the world, land port of entry. And a lot of people forget that. And we have seen a lot of mistakes on here. I think that one of the frustrations is the half implementation of the VISIT system. I think it's got some great potentials.

I would love to be able to talk about the great potentials of getting the biometrics of everyone who comes into this country legally and being able to use that, but also the frustration of not being able to implement in, what, 12 years—how many years has it been—the Exit program on the VISIT system. So we don't know who is left.

And I think at the same time, when we talk about that we see the failure of the border security system. And frankly I am very interested in seeing how much of that was wishful thinking or a snake oil salesman showing up and saying, I've got technology that will eliminate the need for building a fence. We have agents that are being killed down at the border by people who are able to cross over, drive trucks and then drive over agents. We can detect them but we can't stop them. A lot of that, though, is: Was that some kind of response to political pressure against building structures that, don't worry, we don't have to build a fence and do a structure that somebody may take offense to; we can do it all with technology.

A lot of that kind of question comes out to how much political pressure drove people into an assumption that technology could solve the problem when in fact it was grossly deficient.

The fact that we're going to address this in many different ways I think should be open and frank about it. But I think that we have some successes we can look at, but we also have some great failures. And I just wonder how many of those are people overselling technology or those going to technology to avoid political heat for other tactics that would have been more successful. And I look forward to opening that discussion up.

So thank you very much, Madam Chair, I appreciate holding this hearing, again, and thank you for the testimony of the witnesses.

Ms. WATSON. Thank you.

Mr. Luetkemeyer, would you like to make an opening statement.

Mr. LUETKEMEYER. No.

Ms. WATSON. OK. We're now going to proceed to our first panel. It is the policy of the Committee on Oversight and Government Reform to swear in all witnesses today before they testify. And I would like to ask all of you to please stand and raise your right hands.

[Witnesses sworn.]

Ms. WATSON. Thank you. You may be seated. Let the record reflect that the witnesses answered in the affirmative. I will now introduce our panelists. And first I would like to start with Ms. Elaine C. Duke. She's the Under Secretary for Management at the Department of Homeland Security. She oversees the management of the Department's finance, human capital and contracting programs, including the design and implementation of all major investments and acquisitions. Prior to her appointment as Under Secretary for Management, she served as Deputy Under Secretary for Management and as the Department's Chief Procurement Officer.

Mr. James L. Taylor is the Deputy Inspector General at the Department of Homeland Security where he has participated in multiple audits and examinations of DHS investment management policies and acquisition programs. Prior to joining DHS, Mr. Taylor served in senior financial management roles at both the Department of Commerce and the Federal Emergency Management Agency. Mr. Taylor has been the recipient of numerous awards for outstanding professional accomplishments, including the Presidential Rank Award for Distinguished Executive and the Donald T. Scatterberry Memorial Award for Excellence in Financial Management. Welcome.

Mr. Randolph Hite is the Director of Information Technology, Architecture and Systems issues at the Government Accountability Office. During his career with GAO he has directed reviews of major Federal investments in information technology and major business systems modernization efforts. Mr. Hite is a principal author of several information technology management guides such as GAO's Guide on System Testing, the Federal CIO Council Guide on Enterprise Architectures and GAO's Enterprise and Architecture Management Maturity Framework.

And I understand that you're accompanied by Mr. Hutton of GAO's Acquisition and Sourcing Management division.

I welcome you. And I ask that each one of the witnesses now give a brief summary of their testimony, and to keep this summary under 5 minutes in duration. Your complete written statements will be included in the hearing record.

And we recognize our member, Mr. Cuellar, and thank you for being with us this morning.

OK. I would like to ask Ms. Duke to please proceed.

STATEMENTS OF ELAINE C. DUKE, DEPUTY UNDER SECRETARY FOR MANAGEMENT, DEPARTMENT OF HOMELAND SECURITY; JAMES L. TAYLOR, DEPUTY INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY; AND RANDOLPH C. HITE, DIRECTOR, INFORMATION TECHNOLOGY ARCHITECTURE AND SYSTEMS ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY JOHN HUTTON

STATEMENT OF ELAINE C. DUKE

Ms. DUKE. Good morning Chairwoman Watson, Ranking Member Bilbray and members of the subcommittee. I really appreciate the opportunity to come before you today and talk about this very important topic not only to the Department of Homeland Security but also to our country. And we do indeed, Madam Chairwoman, have lessons learned. And I would like to look forward to talking to you about how DHS is strengthening its oversight of all its acquisition programs, including its information technology programs.

In talking with you this morning I would like to talk about where we were, where we are, and where we're going. In the aftermath of September 11th, Congress created DHS to provide a central point of command for securing our country and citizens. In March 2003, we opened our doors and combined the efforts of 180,000 people from 22 agencies and several newly established offices in the DHS headquarters. In March 2003, the IT infrastructure for DHS included multiple wide-area networks with overlapping and redundant system circuitry, each with its own network operation center and security operation center. The infrastructure had 24 different data centers and multiple independently operated e-mail systems with multiple address lists and help desk services. There are multiple sign-on systems in policy and no secure data transmission capability.

This non-unified networking made communication and information exchange across Department enterprise arduous and costly and inhibited our mission success and timeline. We are focused on this operational area in unifying, consolidating and modernizing.

However, we understand that this is more than connecting servers and running cables. It is also accomplished through good management and acquisition oversight. To strengthen the institutional approach to acquisition and IT investment management, DHS established the Acquisition Program Management Division. This office is responsible for the overall coordination of acquisition oversight and policy within the Department, with a DHS Chief Information Officer providing the leadership in the oversight of the information technology programs.

We have dramatically increased the formal acquisition review boards we hold in the Department. In fiscal year 2008 we held eight formal board meetings, in fiscal year 2009 to date, we have already held 28, including 8 specifically focused on American Reinvestment and Recovery Act spending. We will also ensure our IT programs are developed in accordance with the Office of Management and Budget's Federal enterprise architecture guidelines through our Enterprise Architecture Board [EAB]. This EAB assesses each IT program and its contribution in alignment with the Homeland Security mission. Additionally, our CIO reviews all ac-

quisitions, purchase requests for any IT investment over \$2½ million.

We have made major strides in cost estimating and analysis, one of the root causes of the weakness in many of our IT programs. We have established a cost estimating division which is part of each acquisition review, and have also provided cost estimating assistance to over a dozen programs. We have assessed the risk of all 79 of our major IT programs and have posted the results on the OMB information technology dashboard.

This year we have conducted seven portfolio reviews encompassing 61 programs. That is one of the recommendations of GAO that we have recently addressed. And in July 2009, we have reissued the information Technology Management Governance Process Catalog providing clear guidance to the Department of how we're overseeing our IT programs.

Additionally, we have provided updates to many of our existing guidance created in the initial startup of the Department.

Also, we have updated existing guidance in terms of our acquisition review and have issued the management directive 102-1 that governs acquisition oversight and policy for the entire Department. And we have revised how we're tracking action items coming out of our reviews in formal acquisition decision memorandum that have specific due-outs and tracking system.

DHS will continue consolidation and oversight of these programs toward the Secretary's goal of one DHS, one enterprise, a shared vision and integrated results-based operations.

Our future efforts in the IT area include completing the Homeland Security data network, primary migration and also fully realizing our OneNet vision, finalizing our data center consolidation, and creating a more efficient and effective IT environment and greater level of information technology security to address our cyber threat.

It is important to note that DHS developed and implemented all initiatives I've outlined above while simultaneously managing an existing information technology program that has grown to nearly \$7 billion within the 6 years of the Department. While we have strengthened many aspects of our IT acquisition program, we will continue to seek improvements in our processes and provide our professionals the tools they need to meet both our mission objectives and achieve IT oversight.

I am happy to note that the Department has brought on the new administration's full-time Chief Information Officer, Richard Spires. Mr. Spires and I have discussed his goals and he is leading the Department in the right direction. His focus is on a sound approach to conducting systematic reviews of major IT investments, and he recognizes the importance of his leadership as the Department's CIO.

Thank you, Madam Chairwoman, and members of the subcommittee for your interest in this very important topic. I look forward to talking to you about where DHS is, the lessons we have learned, and how we plan on moving forward.

Ms. WATSON. Thank you Ms. Duke.

[The prepared statement of Ms. Duke follows:]



**TESTIMONY OF ELAINE C. DUKE,
UNDER SECRETARY FOR MANAGEMENT,
U.S. DEPARTMENT OF HOMELAND SECURITY**

**Testimony before the
House Subcommittee on Management, Organization, and Procurement, Committee
on Oversight and Government Reform
September 15, 2009**

Chairwoman Watson, Ranking Member Bilbray, and members of the subcommittee, thank you for the opportunity to come before you today to discuss how the Department of Homeland Security (DHS) is strengthening its investment oversight on information technology (IT) programs. When we discuss the Department's IT programs, we have to look at it in three time frames: where we were, where we are, and where we are going.

WHERE WE WERE

In the aftermath of September 11th, Congress created the DHS to provide a central point of command for securing our country and citizens. On March 1, 2003, we opened our doors with the combined efforts of 180,000 people from 22 agencies and several newly established offices in the DHS Headquarters.

In March 2003, the IT infrastructure included multiple Wide Area Networks with overlapping and redundant system circuitry; each with its own Network Operations Center (NOC) and Security Operations Centers (SOC). The infrastructure included 24 different data centers, and multiple independently operated e-mail systems, with multiple address lists and help desk services. There were multiple sign-on systems and policies and no secure data transmission capability. This non-unified networking structure made communication and information exchange across the Department enterprise arduous and costly, and inhibited mission success and timeliness.

In May 2004, the DHS Chief Information Officer (CIO) Council, which consists of the CIOs from all DHS Components and major Headquarters organizations, prioritized IT infrastructure domains to achieve strategic goals, improve customer satisfaction, and reduce overall IT infrastructure cost.

DHS has been integrating all DHS Wide Area Network services through the implementation of OneNet. The network transformation will transition Components to a single network and consolidate seven legacy DHS WANs and manage Component migration to OneNet; develop enterprise NOC and SOC Services; and transition DHS Network services to General Services Administration's (GSA) Network Contract in order to achieve greater network functionality and telecommunications compatibilities.

DHS is consolidating 24 existing data centers into two consolidated DHS enterprise data centers through the data center consolidation effort. After full consolidation, we will have the ability to continuously synchronize applications based upon mission requirements, so either facility can seamlessly take over in the event of a disaster.

DHS has been consolidating legacy e-mail systems used throughout the various Components within DHS to implement a standard e-mail platform. This e-mail platform will be established on a standard DHS intranet for efficient and rapid communication and information dissemination across all DHS entities.

The Department continues to overcome challenges related to IT resource allocation and prioritization of supported operational initiatives. To ensure that the right people inside and outside DHS receive and have access to the right information at the right time, and to enhance mission capability of our organizational elements, the DHS Office of the Chief Information Officer (OCIO) established five strategic objectives:

1. Improve project management with alignment of budget and enterprise architecture
2. Improve infrastructure and consolidation
3. Continue cybersecurity improvements
4. Transition projects into actions and operations
5. Improve information sharing and data collaboration/integration

WHERE WE ARE

We recognize that a successful information technology program is more than connecting servers and running cables – it's also good program management and oversight. To strengthen its institutional approach to acquisition and IT investment management, DHS established the Acquisition Program Management Division (APMD) within the Office of the Chief Procurement Officer and assigned it responsibility for developing and maintaining the Department's acquisition policy and providing support and assistance to the Department's acquisition workforce. The APMD recently issued a new departmental

directive and related guidance, which together provide the framework for departmental management, support, review, and approval of programs, including IT acquisitions. The Enterprise Architecture Board (EAB) assesses the alignment of programs to the Homeland Security Enterprise Architecture developed in accordance with OMB Federal Enterprise Architecture guidelines. The EAB, as a working group, recommends and approves program alignments, new technology insertions, new services, and other decision requests. In a continuing effort to improve overall IT investment management, the Office of the Chief Information Officer (OCIO) has successfully implemented several key governance processes over the past year. These include the IT Acquisition Review (ITAR), IT Budget Review, and IT portfolio management. These new processes have improved our ability to validate alignment of IT assets to business priorities and implement corrective actions where appropriate.

We also recognize that a strong IT workforce is essential to providing the support and oversight required for sound information technology programs. In fiscal year 2009, OCIO developed a staffing plan in direct response to Government Accountability Office (GAO) and the Office of the Inspector General (OIG) reports stating needed enhancements for a proficient IT workforce. OCIO started with 4 FTEs in fiscal year 2004 and is now appropriated for 94 FTE. At the close of fiscal year 2009, OCIO will have 122 FTEs on-board. In order to increase the OCIO's involvement in IT spending and improve its ability to meet the department's reporting requirements, we have submitted a plan to increase the federal employee staffing level to 366 over the next two years.

WHERE WE ARE GOING

DHS will continue consolidation and meeting the Secretary's goal of one DHS, one enterprise, a shared vision, with integrated results-based operations. Future efforts will include: completing the Homeland Security Data Network primary migration to protect and provide classified information technology services; establishing disaster recovery capabilities for customer Components at the data centers; completing the transition to the GSA Networkx contract, to realize the full OneNet vision; finalizing data center consolidation, creating a more efficient IT environment and greater level of security; expanding Single Sign-On for authorized users to log on to their applications on any permissible Department work station using the same log-on credentials through the use of Interconnection Security Agreements; deploying the Electronic Key Management System; and fully implementing Advanced Encryption Standards.

I'm proud to note that the Department has brought on a full-time Chief Information Officer – Richard Spires. Richard and I have discussed his goals, and he is leading the Department in the right direction. His focus is on a sound approach to conducting systemic reviews of major IT investments.

OVERVIEW

In the past, OIG and GAO reports have pointed out a continued need for improvement in DHS information technology programs. We appreciate the oversight, which give us more information to continue to improve our information technology programs. However, those reports are a look backward, and I think it is important to review the achievements to date as well as the ambitious path forward that DHS is on with its information technology programs. I am proud of the progress DHS has made to date in building a strong information technology program. DHS has developed and implemented some key building blocks a world-class information technology programs. These include:

Capital Planning and Investment Control (CPIC) – Through the CPIC process, IT investments are scored – scores that influence budget requests and program decisions. The CPIC process has been embedded into the Acquisition Directive 102 Acquisition Review process developed by the Chief Procurement Officer. Additionally, the CPIC process is supported by the DHS Investment Management System and the CPIC Administrator Group (CAG), to aid components in the development of IT investments for FYHSP, OMB300s and Exhibit 53s.

Strategic Planning – The CIO has developed functional areas that have been adopted by the Office of Strategic Policy and serve as the framework for the Integrated Planning Guidance.

Portfolio Management – Visibility into the IT expenditures of the Department has been improved significantly over the past two years. The CIO has grouped functionally related IT investments into IT Portfolios representing the major capability areas required to support mission area strategic goals, priorities, and objectives. The portfolio model provides common, documented processes to establish performance goals and architectural targets, measure the performance, and continuously improve the balance of investments within each portfolio.

IT Budget Review – The CIO has integrated its IT Budget reviews with the CFO annual Resource Allocation Plan and Resource Allocation Decision Process, using the Investment Management System. Over the past three years the CIO has reviewed more than 300 IT investments totaling more than \$6 billion and provided recommendations to senior leadership through the review process with important results – through this successful partnership, the CIO secured senior-level approval to consolidate the Department’s many IT data centers into two enterprise data centers.

System Engineering Life Cycle (SELC) – The DHS CIO partnered with the CPO on the development of a common SELC Framework. This partnership ensured that new capabilities, both IT and non-IT, will be developed in a repeatable and consistent framework that will reduce risks and improve delivery to the customer.

Enterprise Architecture Board (EAB) – The DHS EAB was instituted as a governance process in 2004 to evaluate IT investments and technologies for alignment with the Homeland Security Enterprise Architecture in accordance with OMB Federal Enterprise Architecture guidelines and to reduce duplication, and increase interoperability of IT systems. Since 2004, the number of Level 1 and Level 2 IT investments reviewed by the EAB has increased by more than 50 percent, with 89 programs having been reviewed by the EAB for architecture alignment at various stages of the system lifecycle.

Information Technology Acquisition Review (ITAR) – The ITAR process has increased the number of oversight reviews by 35 percent since 2007. In fiscal year 2007, there were 265 procurements totaling \$3.1 billion; and in fiscal year 2009 there were 385 totaling \$4.1 billion.

nPRS – The CIO has implemented a performance reporting capability to include IT and non- IT Acquisitions. This newly released capability captures the monthly performance reviews of Level 1 and 2 investments and all major Level 3 IT investments. DHS has also created a nPRS Business Reporting Administrators Group that meets once a month with the components to discuss how to provide program/project/contract data into nPRS. Additionally, CIO has supported OMB's new monthly IT Dashboard by providing relevant data to the system.

Federal Information Security Management Act (FISMA) - As of July 2009, 96 percent of DHS IT systems have been found compliant with FISMA requirements.

Chief Information Officer (CIO) Council – The CIO has established a senior level council which collaborates on IT strategy, implementation strategy on IT priorities, and joint budget formulation.

CLOSING

It is important to note that DHS developed and implemented all the initiatives I've outlined above while simultaneously managing an existing information technology program that has grown exponentially in the first six years of the Department. We are proud of our progress to date, and we remain committed to continuous improvement and dedicated management of DHS' IT programs.

While we have strengthened many aspects of our IT acquisition program, we will continue to seek improvements in our processes and provide our professionals the tools they need to both meet our mission and achieve IT excellence.

Thank you, Ms. Chairwoman and members of the subcommittee for your interest in and continued support of DHS IT programs. Thank you for the opportunity to testify before the subcommittee about DHS IT programs. I am happy to answer any questions you or the members of the subcommittee may have.

Ms. WATSON. Mr. Taylor, you may proceed.

STATEMENT OF JAMES L. TAYLOR

Mr. TAYLOR. Thank you, Ms. Chairwoman, Ranking Member Bilbray, and members of the subcommittee. I appreciate the opportunity to appear before you on behalf of the DHS Office of Inspector General. My testimony today will focus on the progress in IT acquisition management DHS has made over the past several years, as well as the challenges the Department and its components face going forward. Specifically, I will discuss our work related to the establishment of institutional and investment management capabilities for delivering major information technology systems at DHS.

As required by the Reports Consolidation Act of 2000, each year the OIG updates our assessment of the major management challenges facing the Department. Given the past concerns we in GAO have raised and the fact that contracting for goods and services consumes nearly 40 percent of the Department's annual budget and is critical to achieving its mission acquisition management, it has consistently remained at the top of that list.

DHS spends over \$6 billion a year for IT systems and infrastructure to support its mission. The Department's components rely extensively on information technology to perform mission operations, including immigration benefits processing, border security, the execution of response and recovery operations and many others.

Given the size and significance of DHS's IT investments, effective management of the Department-wide IT expenditures is absolutely critical. In the past we identified the need for the Department's Chief Information Officer to have greater authority to become a more effective steward of IT funds. The Department has responded by strengthening the CIO's role for centralized management of IT, providing the CIO the authority to guide IT investments and ensure a unified strategy across DHS components.

Additionally, the CIO has gained greater authority over component level IT budgets and oversight of IT acquisitions. This has resulted from the establishment of new policies in IT investment governance functions and a defined IT acquisition review process. However, in 2007 only 57 percent of the estimated \$5.6 billion IT budget was evaluated through this process. The Department officials stated that there have been a lack of sufficient DHS and component CIO staff to effectively execute the ITAR process.

In 2004, around 75 percent of the Federal positions within the CIO's office were filled. By 2007, that number had dropped to only 64 percent. Unable to obtain and keep full-time Federal employees, the CIO has depended heavily on contractor support. During that same timeframe from 2004 to 2007, the number of contractors increased from 121 to 550. A combination of factors have contributed to the low staffing numbers, including the complex and lengthy hiring process, and includes background checks that you have heard as a familiar refrain. Once the CIO positions are filled, many employees have become burned out from working long hours and end up leaving for positions in the private sector.

To address the staffing issues, we recommended that the Department improve the CIO staffing plan to include specific actions and

milestones for recruiting and retaining full-time employees. The Department has since developed a revised staffing plan to increase Federal positions and to augment overall staff by 236, by 2011. This increase is necessary to address the complex IT challenges facing DHS.

An example of major IT challenges, OneNet, an initiative aimed at consolidating existing IT infrastructures into a wide-area network. DHS began working on OneNet in 2005 and envisions it will provide the components with secure data voice and video communications. Specifically, DHS is experiencing delays in meeting its schedule completion date. Some components were reluctant to migrate to OneNet and have insisted instead on maintaining their own Internet gateways. As a result, DHS may not be able to reach its ultimate goal of consolidating and modernizing its existing infrastructure and achieve cost savings originally estimated at nearly \$900 million.

Concluding, CIOs also face significant challenges in their efforts to improve IT management in budgeting, planning and investment. Because programs are often funded through direct appropriations or other sources investment decisions may reside outside the component CIO's purview. In these cases, offices and divisions maintain separate budgets that are independent of the CIO. Insufficient staff, ineffective IT budget controls and fragmented IT management have been longstanding issues for several DHS components.

For example, in November 2006, reporting the results of a follow-up audit of USCIS's transformation program, we noted that although CIS had taken steps to address recommendations in our 2005 report, the component had yet to finalize its transformation of implementation approach. Subsequently, we found in 2009 that the large-scale CIS transformation program is being managed outside the CIO's Office of Information Technology.

The CIO identified the autonomy of CIS's transformation program IT efforts and the program's exemption from normal CIS controls as an emerging internal control deficiency. In addition, we reported that the continuation of decentralized fragmented IT program efforts has led to a growing number of local systems that are beyond the CIO's current budget or staffing level to manage effectively. Although the total number of locally funded IT systems is unknown CIS field offices have reported thousands of applications that were created in-house.

To summarize, Ms. Chairwoman, our work with the Department has shown that there is a recognition of the weaknesses in IT acquisition in governance processes in the Department, and there has been progress in addressing these weaknesses. However, there remains structural and resource constraints that limit the Department's ability to properly plan, acquire, and oversee critical information technology projects.

Thank you for this opportunity, and I welcome any questions from you or members of the subcommittee.

Ms. WATSON. Thank you so much Mr. Taylor.

[The prepared statement of Mr. Taylor follows:]

STATEMENT OF JAMES L. TAYLOR

DEPUTY INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON MANAGEMENT, ORGANIZATION, AND
PROCUREMENT**

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 15, 2009



Ms. Chairwoman and Members of the Subcommittee:

Thank you for the opportunity to appear before you on behalf of the Department of Homeland Security Office of Inspector General. My testimony today will focus on the progress in IT acquisition management DHS has made over the past several years, as well as several challenges the department and its components face going forward. Specifically, I will discuss our work related to the establishment of institutional and investment management capabilities for delivering major information technology (IT) system acquisitions programs at DHS.

The information that I will provide is contained in two reports we've issued on DHS and its components' IT management practices, *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91) and *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-09-90); as well as our annual *Major Management Challenges Facing the Department of Homeland Security* (OIG-09-08).

DHS Acquisition Management

Contracting for goods and services consumes nearly 40% of the department's annual budget and is critical to achieving its mission. Acquisition management is a complex process that involves much more than simply awarding a contract. It begins with identification of a mission need, the development of specific requirements, and a strategy to fulfill that need and meet those requirements while balancing cost, schedule, and performance. A successful acquisition process requires an effective acquisition management infrastructure and skilled professionals.

In our November, 2008 Major Management Challenges report, we rated the department's progress in four areas of acquisition management: organizational alignment and leadership; policies and processes; acquisition workforce; and knowledge management and information systems. In all these areas, we rated the department's progress as "Modest." While we identified some improvements, our reviews indicated that many of the critical success factors had not yet been met.

DHS' IT Investment Management Oversight

DHS spends over \$6 billion a year for IT systems and infrastructure to support its mission. The department's component agencies rely extensively on information technology to perform mission operations, including immigration benefits processing, support for its security mission, the execution of response and recovery operations, human resources and financial management, and many others. Given the size and significance of DHS' IT investments, effective management of department-wide IT expenditures is critical.

The Clinger-Cohen Act requires that departments and agencies create a capital planning and investment control (CPIC) process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources to benefit the strategic needs of the department. As part of the CPIC process, agencies are required to submit business plans for IT investments to OMB demonstrating adequate planning. Through such efforts, in FY 2007, the 94 DHS programs on the management watch list were reduced to 18. In FY 2008, 53 programs were listed. Officials in the OCIO have sought to remove these programs from the list by working with the program managers through the CPIC Administrator's bimonthly meetings.

In the past, we identified the need for the department's Chief Information Officer (CIO) to have greater authority to become a more effective steward of IT funds.¹ Most components have not yet achieved an integrated planning and investment management capability. More than 70% of the major DHS components had limited capital planning processes outside the existing OMB 300 process. However, some component CIOs said that they are creating a CPIC process to integrate with existing governance structures such as the Investment Review Board. For example, the ICE Investment Review Board resembles a CPIC group, incorporating major areas such as security, budget, and enterprise architecture. The ICE CIO said that this process has helped components leverage resources more effectively.

The department has strengthened the CIO's role for centralized management of IT, providing the CIO the authority to guide IT investments to ensure a unified IT direction across DHS components.

Additionally, the DHS CIO has gained greater authority over component-level IT budgets and oversight of IT acquisitions. This has resulted from the establishment of new policies and IT investment governance functions. For example, DHS management directive 0007.1, *Information Technology Integration and Management*, establishes the IT acquisition authorities and responsibilities of the DHS CIO, and is the principal document for leading, governing, integrating, and managing the department's IT. The directive also defines the department's IT acquisition review (ITAR) process.

Improvements to IT Acquisitions and Governance

Implementation of the ITAR process has increased the DHS CIO's ability to ensure program and project alignment with department-wide IT policy, standards, objectives, and goals. For example, it has enabled the DHS CIO to direct IT efforts toward the department's primary infrastructure goals, such as consolidating component network and data centers.

Additionally, the ITAR process has improved compliance with the DHS enterprise architecture, enabling the DHS CIO to direct IT efforts to align with the department's

¹ *Improvements Needed to DHS' Information Technology Management Structure* (OIG-04-30, July 2004).

target architecture goals. For example, the Transportation Security Administration (TSA) planned to create an E-authentication solution for its Alien Flight School Program. However, during the ITAR process, the Office of the CIO (OCIO) recognized that TSA's system needs could be met by using the solution that U.S. Immigration and Customs Enforcement (ICE) created for its Student Exchange Visitor Information System, thus preventing unnecessary duplication.

Component-level CIOs also have benefited from the ITAR process, which requires that component IT procurement requests be approved by the CIO before they are completed by the acquisitions office. Under this process, the TSA CIO identified opportunities to use more enterprise licenses for products, such as security software, and consolidated IT support contracts, resulting in cost savings.

The DHS CIO relies on a variety of IT investment governance structures and functions to ensure compliance with IT management policies and to promote centralized IT management, including the CIO Council, an Investment Review Board, an Enterprise Architecture Board, the Capital Planning and Investment Control process, and Portfolio Management process.

The DHS CIO Council sets the vision and strategy for the IT function and information resources. This council provides recommendations for the department IT strategic plan and establishes policies, processes, best practices, performance measures, and decision criteria for managing IT service delivery. According to several component CIOs, the council has improved component collaboration, productivity, and communication. The Investment Review Board is a governance body responsible for providing senior managers with visibility, oversight, and accountability for IT investments. The DHS CIO plays a major role in reviewing IT investments that reach the Investment Review Board. The Enterprise Architecture Board is an investment review mechanism that has improved department-wide IT management functions. The board's review ensures that IT investments align with the department's enterprise architecture and that sound IT investment approval recommendations are provided to the DHS CIO.

As discussed earlier, the CPIC process requires components to submit business cases for IT investments to demonstrate adequate planning. The business cases are reviewed for approval and progress based on the Office of Management and Budget's annual budget process. CPIC administrators from each component act as liaisons between the department and the component programs to aid the CPIC process. These administrators regularly review issues and identify process improvements. The DHS Portfolio Management process establishes portfolios based on DHS' mission areas, strategic goals, and objectives to align IT investments with DHS' strategic objectives. Operating these governance bodies and executing these processes require commitment and a significant amount of resources, including staff time.

Ongoing Challenges

Implementing the ITAR process has been challenging and we continue to identify problems with outdated or stove-piped systems, at times supporting inefficient business processes. Planning to modernize IT has been unfocused, often with inadequate requirements identification, analysis, and testing to support acquisition and deployment of the systems and other technologies needed to improve operations.

In 2007, only 57% of the department's estimated \$5.6 billion IT budget was evaluated through the ITAR process. Department officials stated that there has been a lack of sufficient DHS CIO and component CIO staff to effectively execute the ITAR processes at the department and component levels. In 2004, around 75% of the federal positions within the OCIO were filled. By 2007, only 64% of the positions were filled.

Unable to obtain and keep fulltime, federal employees, the OCIO has depended heavily on contractor support. The number of contractors increased from 121 in 2004 to 550 in 2007. A combination of factors have contributed to the low staffing numbers, including the complex and lengthy hiring process that involves background checks for security clearances. Once OCIO positions are filled, employees become "burned out" from working long hours and end up leaving for positions in the private sector.

To address its staffing issues, we recommended that the DHS CIO improve the DHS OCIO Staffing Plan to include specific actions and milestones for recruiting and retaining fulltime employees. We closed this recommendation in June 2009 based on the department's development of a revised staffing plan that detailed plans to increase federal positions and to augment overall staff by 236 throughout the OCIO by 2011.

Agencywide IT Infrastructure Initiatives

Even with these improvements, the department will continue to face significant challenges as it attempts to create a unified IT infrastructure for effective integration and agencywide management of IT assets and programs. Toward that end, DHS has several initiatives underway to improve IT operations and reduce costs. One such program is the development of an enterprise-wide IT disaster recovery program to ensure that the department's operations can continue uninterrupted should its IT systems fail. We reported in April 2009 that DHS had made progress in implementing a disaster recovery program by allocating funds to establish two new data centers.² However, we noted that more work was needed to ensure the new data centers were fully capable of meeting the department's significant IT disaster recovery needs.

Another major IT challenge for the DHS CIO is OneNet, an initiative aimed at consolidating existing IT infrastructures into a wide area network. DHS began work on OneNet in 2005, and envisions it will provide the components with secure data, voice, video, tactical radio, and satellite communications between internal and external DHS resources. We recently reported that DHS has taken various steps to consolidate existing infrastructures into OneNet, but faces challenges in completing its OneNet

² *DHS' Progress In Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).

implementation.³ Specifically, we reported that DHS is experiencing delays in meeting its scheduled completion date, and that some components are reluctant to migrate to OneNet, have insisted on maintaining their own Internet gateways, and are hesitant to use DHS Trusted Internet Connection (TIC) services. As a result, DHS may not be able to reach its ultimate goal of consolidating and modernizing its existing infrastructures and achieve cost savings.

Component IT Management

Although improvements have been made, component CIOs also face significant challenges in their efforts to improve IT management, budgeting, planning, and investment. Because programs are often funded through direct appropriations or other sources, investment decisions may reside outside of the component CIO's purview. In these cases, offices and divisions maintain separate budgets that are independent of the CIO. Insufficient staff, ineffective IT budget controls, and fragmented IT management have been long-standing issues for several DHS components. For example:

U.S. Citizenship and Immigration Services (USCIS)

The USCIS CIO has been challenged to enforce compliance with component-level IT system development control mechanisms for the past several years. In January 2005, USCIS developed a transformation strategy that discussed the business requirements and vision for modernizing IT to meet mission needs. In September 2005, we reported that USCIS' IT environment is inadequate to effectively support immigration benefits processing.⁴ Specifically, USCIS uses multiple, disparate information systems that are difficult to use and do not adequately share information, resulting in data integrity problems. The lack of a fully integrated IT environment has forced employees to spend time tracking the location of paper files as they are transferred among and within USCIS offices numerous times over their life cycle.

In November 2006, we reported on the results of a follow-up audit of USCIS' transformation program.⁵ We noted that although USCIS had taken steps to address the recommendations in our 2005 report, the component had yet to finalize its transformation implementation approach. Subsequently, we reported in July 2009 that the large-scale USCIS transformation program is being managed outside of the CIO's Office of Information Technology.⁶ The CIO identified the autonomy of the USCIS transformation program IT efforts and the program's exemption from normal USCIS controls as an emerging internal control deficiency. In addition, we reported that the continuation of decentralized, fragmented IT program efforts has led to a growing

³ *Improved Management and Stronger Leadership are Essential to Complete the OneNet Implementation* (OIG-09-98, September 2009).

⁴ *USCIS Faces Challenges in Modernizing Information Technology* (OIG-05-41, September 2005).

⁵ *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-07-11, November 2006).

⁶ *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-09-90, July 2009).

number of local systems that are beyond the USCIS CIO's current budget or staffing level to manage effectively. Although the total number of locally-funded IT systems is unknown, USCIS field offices have reported thousands of applications were developed "in-house."

We concluded that transformation will be critical to support the agency's current workload, address the ongoing backlog, and prepare for future increases in demand for immigration benefits processing. Among other things, we recommended that the Acting Deputy Director provide the CIO agency-wide budget and investment review authority for all USCIS IT initiatives and system development efforts.

Transportation Security Administration (TSA)

The TSA CIO faces major challenges in managing and applying IT effectively in support of TSA's security mission. We reported in October 2007 that TSA strengthened its IT governance and acquisition processes.⁷ However, technology investments were being managed in a decentralized fashion. Further we reported that TSA established an acquisition process and supporting governance structure, but has not instituted mechanisms for consistent oversight of agency-wide IT resources and initiatives. Questions remain regarding the agency's ability to enforce the guidance consistently across TSA programs. Program managers are not consistently aware of the existing review boards and have a limited understanding of the decision making process.

Further, we reported that TSA's decentralized IT budget hinders visibility of IT spending across the organization. As the agency evolved in a decentralized manner, the CIO has had no official or substantive role in budgeting or planning for IT programs initiated in other offices apart from the IT Division. As a result, the CIO frequently is not consulted on significant technology decisions and investments. Some high-profile programs, such as Secure Flight, receive direct funding through appropriations or user-generated fees. Because of its mandated funding, the program has not relied on external support from the IT Division. Such mandated funding also hinders enterprise-wide, long-term IT planning, and reduces opportunities to integrate and leverage existing IT initiatives.

We recommended that the Assistant Administrator for TSA strengthen agency IT management by empowering the CIO with agency-wide IT budget and investment review authority to ensure that IT initiatives and decisions support accomplishment of TSA mission objectives. We also recommended that TSA apply adequate staff resources to strengthen the IT Division in addressing IT needs and support agency-wide operations. The Assistant Administrator concurred with our recommendations and has taken steps to improve the CIO's agency-wide IT budget and investment review authority by expressing support for DHS management directive 0007.1, *Information Technology Integration and Management*. However, IT staffing levels continue to be a concern and have not yet been addressed due to budget constraints.

⁷ *Information Technology Management Needs to Be Strengthened at the Transportation Security Administration* (OIG-08-07, October 2007).

Federal Emergency Management Agency (FEMA)

DHS components, such as the Federal Emergency Management Agency (FEMA), have taken steps to improve acquisition management. We reported in February 2009 that FEMA had made progress in improving internal controls over its acquisition process, but identified additional safeguards that FEMA needed to take.⁸ For example, we recommended that FEMA establish an internal control board and assess the adequacy of its internal controls annually. In addition, we recommended that FEMA comply with the Federal Acquisition Regulation on contract close out, so that unused funds can be spent to address future needs. FEMA agreed with our recommendations and has begun to address some of the weaknesses identified in the report.

We reported as well in February 2009 that FEMA's Office of Acquisition Management had made progress in implementing best practices into the acquisition process.⁹ In our report we noted additional practices that FEMA needs to include, such as:

- Developing a strategic plan that links to the agency plan or outcome-based performance measures that tie to the agency's strategic goals;
- Working with program officials to create a more strategic approach to acquisition planning and management;
- Developing an oversight process to determine the efficiency and effectiveness of the acquisition program; and,
- Creating systems to document and share lessons learned throughout the acquisition function

FEMA concurred with our recommendations and has begun to implement these best practices as well.

The FEMA CIO also faces significant challenges in efforts to improve IT management, budgeting, planning, and investment. We reported in September 2005 that the CIO could not ensure that IT investments were well-integrated or aligned with mission needs.¹⁰ We noted that an inadequate long-term IT strategy, coupled with insufficient IT budget control has resulted in IT systems unable to share information. Subsequently, in May 2008, we reported that FEMA's logistics management systems do not provide complete asset visibility, comprehensive asset management, or integrated information during disaster response.¹¹ Without effective IT support for its logistics activities, FEMA staff will find it difficult to perform disaster response in an effective, timely manner.

⁸ *Internal Controls in the FEMA Disaster Acquisition Process* (OIG-09-32, February 2009).

⁹ *FEMA's Implementation of Best Practices in the Acquisition Process* (OIG-09-31, February 2009).

¹⁰ *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery* (OIG-05-36, September 2005).

¹¹ *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency* (OIG-08-60, May 2008)

Until the IT budget data is fully controlled at the component level and consolidated at the department level, the DHS CIO will not attain complete visibility of IT spending across components, hindering the ability to influence technology decisions and investments.

In summary, the DHS CIO has a responsibility to effectively manage IT acquisitions to promote a unified direction and ensure alignment to departmental goals. However, insufficient department OCIO and component-level OCIO staff and fragmented IT budget and management practices have hindered the department's ability to fully integrate new IT management and acquisitions practices. Once fully implemented and supplied with sufficient resources, the IT management and acquisition mechanisms that DHS has put into place may ensure IT investments fulfill mission and IT goals, thus promoting overall efficiency and effectiveness across the department.

Ms. Chairwoman, this concludes my prepared statement. Thank you for this opportunity and I welcome any questions from you or Members of the Subcommittee.

Ms. WATSON. And Mr. Hite you may now proceed.

STATEMENT OF RANDOLPH HITE

Mr. HITE. Thank you. On behalf of Mr. Hutton and myself, let me begin by saying that it was about 3½ years ago that I sat before this subcommittee and I testified on where DHS stood in managing large-scale IT system acquisitions. Noting that while it had made progress since it was formed in establishing this range of institutional management controls needed to successfully deliver these systems, it was not where it needed to be.

Today, 3 years later, further progress has been made, most notably in the last year. However, more needs to be done on a number of fronts to define and implement the range of controls needed so that the Department can successfully deliver these systems on a repeatable basis.

Now, what are these institutional management controls that I am talking about? One is having and using enterprise architecture which can be viewed as an institutional blueprint to guide and constrain the structure and the content of what these systems are.

Another is having acquisition investment management structures, policies, and procedures that decisionmaking bodies can then use to make informed decisions not only about programs, but portfolios of programs, decisions around their selection and the control. So they are managed in a way to maximize benefits, minimize costs and mitigate risks.

A third is having a defined system life cycle methodology that is used to govern how systems are defined, designed, developed, tested, integrated, deployed, operated and maintained all through their life cycle.

And a fourth is having the people that you need in order to execute all these things.

How does the Department stack up today against these management controls? The answer is mixed. For example, it has recently strengthened its acquisition investment management approach and has in the last year possibly conducted as many formal oversight reviews of major system acquisition programs as it did in the prior 5 years combined. However, its new approach is still missing key aspects, such as criteria for prioritizing and selecting among competing investment options and procedures governing oversight reviews.

Also, while the Department has recently created a system life cycle methodology, the scope of this methodology does not yet address important topics such as key practices associated with acquiring COTS or commercial-off-the-shelf solutions.

Further, while it has undertaken a number of initiatives to expand its acquisition work force, particularly contract specialists, it has made very little progress in adopting and implementing a strategic and proactive approach to managing its IT work force. Over the last 3½ years, DHS has similarly made mixed, or had similarly mixed success when it comes to implementing these controls on large-scale IT programs.

Specifically, our work has shown that programs have been allowed to begin and proceed, sometimes for several years, without sufficient management, discipline and rigor. And as a result they've

fallen short of cost scheduling performance expectations, assuming in some cases that expectations were even set for these programs. That's the bad news.

The good news is that when we have reported on these weaknesses, the Department has acted to correct them and bring the program back on track. This means that programs like Secure Flight, for example, which is the prescreening of passengers on commercial flights, matching their names against a watch list, is now being managed effectively. But to get to that point, these programs had to overcome several years of poor program management and oversight.

To give you a flavor for the kind of program-specific management control weaknesses that we have seen repeat themselves on these key programs and that have been addressed to varying degrees across the programs, let me cite a few programs. They include poor requirements, development and management, inadequate testing, unreliable cost and schedule estimates, insufficient program office staffing, inadequate risk management, limited information security management and poor performance measurement.

So, having said all this, what needs to be done? What needs to change? The bottom line is that DHS must effectively manage and oversee its newly starting IT programs, like TASC. TASC is the follow-on program to the eMerge2 that the chairwoman mentioned in her opening remarks. That was a failed acquisition. It needs to start managing these acquisitions properly, right out of the gate. And for those programs that are ongoing but have not yet turned the corner, like the SBInet virtual fence, it needs to bring them in line quickly.

In my view, the recommendations that we have made to the Department provide a comprehensive framework for doing this. And to DHS's credit it has agreed with these recommendations, and we are committed to working with the Department constructively to ensure that they are implemented.

This concludes my statement. I would be happy to answer any questions that you have at this time.

[The prepared statement of Mr. Hite follows:]

United States Government Accountability Office

GAO

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

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

HOMELAND SECURITY

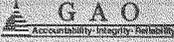
Despite Progress, DHS Continues to Be Challenged in Managing Its Multi-Billion Dollar Annual Investment in Large-Scale Information Technology Systems

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



September 15, 2009

HOMELAND SECURITY

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


Highlights

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

Why GAO Did This Study

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

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

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

What GAO Found

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

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

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

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

Madame Chairwoman and Members of the Subcommittee

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

For DHS to effectively manage the billions of dollars that it invests each year in IT, we reported in 2004² that it needed to put in place key institutional IT management controls, such as employing a departmentwide operational and technological blueprint to guide and constrain its acquisitions (enterprise architecture), and following institutional policies, practices, and structures for acquiring and investing in these programs. Other institutional controls and capabilities include employing rigorous and disciplined system life cycle management processes and having capable acquisition and IT workforces.

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

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

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

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

Background

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

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

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

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

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

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

DHS Components and IT Spending

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

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

Figure 1: DHS Organizational Structure

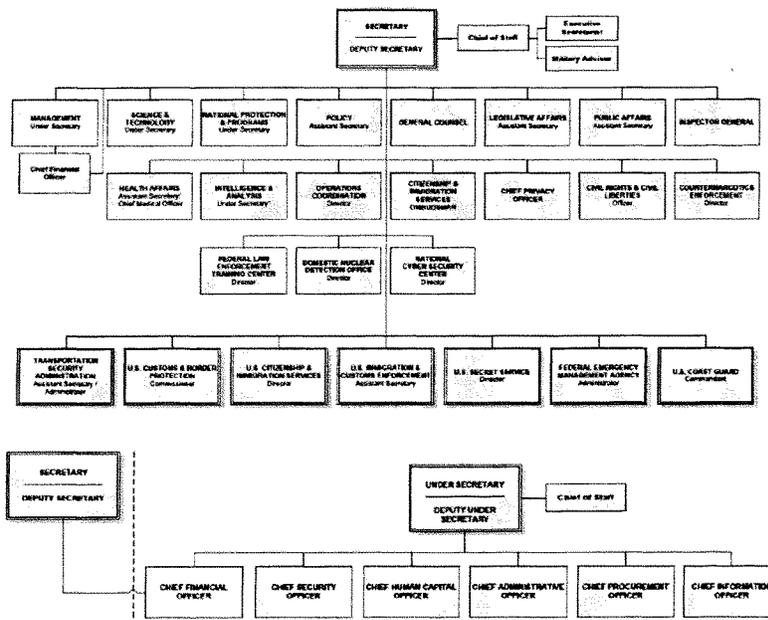


Table 1: DHS' Principal Component Organizations and their Missions

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

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

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

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

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

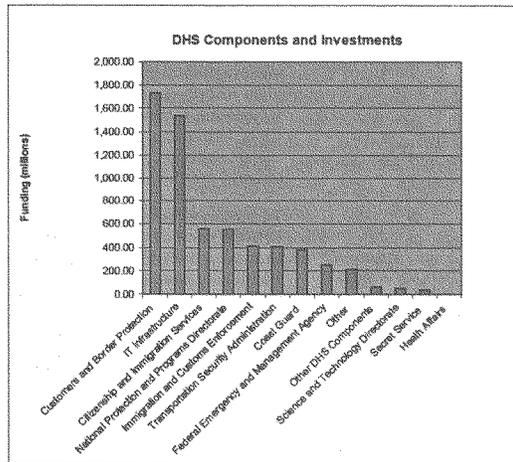
Also within the Management Directorate is the Office of the Chief Procurement Officer (CPO). The CPO is the department's senior procurement executive who has leadership and authority over DHS acquisition and contracting, including major investments. This office's responsibilities include issuing policies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

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

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

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

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



Source: DHS

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

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

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

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

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

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

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

- **Rescue 21:** This is a Coast Guard program to modernize a 30-year-old search and rescue communications system used for missions 20 miles or less from shore, referred to as the National Distress and Response System. Among other things, it is to increase communications coverage area, allow electronic tracking of department vessels and other mobile assets, and enable secure communication with other federal and state entities. As of June 2009, Rescue 21's initial operating capability has been deployed and accepted at 23 of 42 regions. Additional system capability (e.g., the ability to track vessels) remains to be developed, as does a system to meet the unique needs of the Alaska region. Through fiscal year 2009, DHS has been appropriated about \$723 million for Rescue 21, and for fiscal year 2010, the department has requested about \$117 million.
- **Secure Flight:** This is a Transportation Security Administration (TSA) program to allow the federal government to assume from airlines the responsibility of prescreening passengers for domestic flights by matching of passenger biographic information against watch lists. Among other things, Secure Flight is to prevent people suspected of posing a threat to aviation from boarding commercial aircraft in the United States, protect passengers' privacy and civil liberties, and reduce the number of people unnecessarily selected for secondary screening. TSA is currently in the process of phasing in its use of Secure Flight for domestic flights. Through fiscal year 2009, DHS has been appropriated about \$326 million for Secure Flight, and for fiscal year 2010, the department has requested about \$84.4 million.
- **SBLnet:** SBLnet is the technology component of a CBP program known as SBI, which is to help secure the nation's borders and reduce illegal immigration through physical infrastructure (e.g., fencing), surveillance systems, and command, control, communications, and intelligence technologies. As of 2009, a

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

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

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

Enterprise Architecture Continues to Evolve, But Key Content Still Missing

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

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

Since 2003, DHS has issued annual updates to its EA that have improved on prior versions by adding previously missing content.⁹ Specifically, we reported in November 2003⁹ that DHS's initial version of its EA was not sufficiently mature to guide and constrain investments. For example, while the department had established the management foundation for developing, maintaining, and implementing its EA and had issued an initial version of its target architecture, it had yet to develop products that fully described its current and target architectural environments, as well as a plan for transitioning from the current to the target environment.

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

In May 2007, we reported¹¹ on the third version of DHS's EA, concluding that while this version partially addressed each of our prior recommendations, it did not fully address them, and thus important content was still missing. Further, we reported that DHS organizational components were not adequately involved in its development. Accordingly, we made additional recommendations.

⁹ The Homeland Security EA version 1.0 was issued in September 2003 and version 2.0 was issued in October 2004. The next version, HLS EA 2006, was issued in June 2006, followed by HLS EA 2007 in March 2007, HLS EA 2008 in February 2008, and the HLS EA 2009 in June 2009.

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

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

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

To the department's credit, recent versions of its EA largely address our prior recommendations aimed at adding needed architectural depth and breadth. For example, in response to our prior recommendation that the architecture include a technical reference model (TRM) that describes, among other things, the technical standards to be implemented for each enterprise service, the 2008 version of the EA included a TRM that identified such standards. It also adopted an approach for extending the architecture through segments, which is a "divide and conquer" approach to architecture development advocated by OMB. To implement this approach, OMB guidance¹² states that agencies should define and prioritize enterprise segments,¹³ focusing first on those segments that will help it perform its mission most effectively, and that they should first focus on developing architectures for high priority segments. However, while the 2008 EA identified 22 segments, it did not prioritize the segments.

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

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

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

functional areas. As we have previously reported¹⁴, segment architectures serve as a bridge between the corporate frame of reference captured in the EA and each individual system investment. Without well-defined segment architectures, DHS does not have a sufficient basis for investing in IT programs in a manner to ensure that they investments are properly sequenced, well integrated, and not duplicative.

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

Through effective corporate acquisition and investment management, organizations can make informed decisions when selecting among competing investment options and when controlling them throughout their acquisition life cycles. Based on our research, we issued an IT investment management framework¹⁵ that encompasses, among other things, best practices of successful public and private sector organizations relative to selecting and controlling individual investments as well as portfolios (segments) of investments. During the select phase, organizations are to (1) identify and analyze program/project risks and value before committing significant funds and (2) select those that will best support its mission needs. In the control phase, they are to ensure that programs/projects are meeting cost, schedule, and performance expectations at key milestone events, and that actions are taken to address deviations.

Since 2003, DHS has attempted to define and implement a corporate approach to overseeing its acquisition of major system investments, and we have continued to report limitations in its efforts to do so. Specifically, in August 2004, we reported¹⁶ that DHS had established

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

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

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

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

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

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

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

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

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

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

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

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

assigned it responsibility for developing and maintaining the department's acquisition policy and providing support and assistance to the department's acquisition workforce. To that end, DHS issued a new departmental directive²⁰ and related guidance in November 2008,²¹ which together provide the framework for departmental management, support, review, and approval of programs, including IT acquisitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Since 2004, we have reported that DHS lacked a standard and repeatable life cycle management process, and instead was relying on the processes that each of its components had in place. In 2008, DHS issued an interim life cycle management guide to introduce a standard system development methodology that can be tailored to specific projects.²⁶ To the department's credit, this guide addresses important aspects of effective system acquisition and development. For example, the guide requires that business objectives and systems requirements, as well as baseline performance goals, be defined and used as the measures of success for each program, and it requires that all programs be aligned with the HLS EA. Further, it requires acquisition management oversight and defines the roles and responsibilities of key stakeholders, including component CIOs and DHS IT portfolio managers, and to accomplish this it requires checkpoint reviews (i.e., stage reviews) throughout the program's life cycle. In addition, it specifies key activities associated with each life cycle stage (planning, requirements definition, design, development, integration and test, implementation, operation and maintenance, and disposition).

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

²⁶ DHS, *Systems Engineering Life Cycle Instruction Guide v 1.0*, Nov. 7, 2008.

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

Acquisition and IT Workforce Management Remains a Challenge

A strategic approach to human capital management is critical to ensuring that an organization has the right people with the right skills at the right time to perform a given function. Based on our research of leading organizations, we issued a model²⁶ for strategic human capital management in which strategic human capital planning was one cornerstone.²⁷ Through such planning, organizations can remain aware of its current workforce capabilities and its future workforce needs, and can be prepared for meeting these needs. According to our guidance, key practices for effective strategic human capital planning are generic, applying to any organization or component, such as an agency's acquisition or IT organization.²⁸ They include:

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

²⁶ GAO-02-373SP.

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

²⁸ GAO-04-39.

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

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

Acquisition Workforce

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

- lacked an overall direction for acquisition workforce planning, and notwithstanding some recent actions, had not fully involved key stakeholders, such as the CHCO and component procurement and program offices, both of which have been shown to increase the likelihood of success for workforce planning;
- excluded some acquisition-related career fields from its definition of acquisition workforce, thus limiting the scope of its planning efforts, and while it intended to expand its definition, it had yet to identify which positions should be included;
- lacked sufficient data to fully assess its acquisition workforce needs, including the gaps in the number of employees needed or the skills of these employees; and

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

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

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

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

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

³⁰ GAO-09-30

IT Workforce

In June 2004,²¹ we reported that DHS had begun strategic planning for IT human capital at the headquarters level, but it had not yet systematically gathered baseline data about its existing IT workforce across the department. Moreover, the DHS CIO had expressed concern at that time about staffing and acknowledged that progress in this area had been slow. In our report, we recommended that the department analyze whether it had appropriately allocated and deployed IT staff with the relevant skills to obtain its institutional and program-related goals. In response, the CIO established an IT human capital Center of Excellence to deliver, plans, processes, and procedures to execute an IT human capital strategy and to conduct an analysis of the skill sets of DHS IT professionals.

In September 2007,²² we reported that DHS had developed a IT human capital plan and related documents that were largely consistent with federal guidance and associated best practices. For example, they provided for developing a complete inventory of existing IT staff skills, identifying IT skills needed to achieve agency goals, determining skill gaps, and developing plans to address such gaps. They also provided for involving key stakeholders—such as the CIO, Chief Human Capital Officer (CHCO), and component agency CIOs and human capital directors—in carrying out the skill gap analyses and follow on workforce planning.

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

²¹ GAO, *Human Capital: DHS Faces Challenges In Implementing Its New Personnel System*, GAO-04-790 (Washington, D.C.: June 18, 2004).

²² GAO, *Information Technology: DHS's Human Capital Plan Is Largely Consistent with Relevant Guidance, but Improvements and Implementation Steps Are Still Needed*, GAO-07-425 (Washington, D.C.: Sept. 10, 2007).

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

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

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

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

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

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

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

ACE

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

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

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

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

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

known key acquisition and IT management control weaknesses associated with, for example, program office human capital and software management processes.³⁶ Subsequently, we reported that CBP was working to implement our previous recommendations aimed at addressing acquisition and IT management control weaknesses, but that problems continued.³⁷ For example, ACE cost estimates were not reliable because they were not derived in accordance with estimating best practices. The next year we again reported that ACE was not following rigorous and disciplined acquisition and IT management controls, such as those related to managing the program office human capital, risks, and contract management.³⁸ For example, while initial ACE test results were positive, CBP had not taken steps to independently oversee the contractor's testing.

In May 2004,³⁹ we reported that the first two ACE system increments were operating, but that CBP's approach to incrementally acquiring and deploying ACE involved excessive overlap among increments. Moreover, the scheduling of increments had allowed for considerable overlap and concurrency among them, and this had produced a pattern of having to borrow resources from later increments to complete earlier increments. We concluded that this pattern had and would continue to result in ACE cost overruns and schedule delays. The next year, we reported that while CBP had revised its cost baselines in light of ACE overruns, this was not sufficient because the number of ACE increments had increased and system quality standards had been relaxed to allow increments to

³⁶ GAO, *Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project*, GAO-02-545 (Washington, D.C.: May 13, 2002).

³⁷ GAO, *Customs Service Modernization: Third Expenditure Plan Meets Legislative Conditions, but Cost Estimating Improvements Needed*, GAO-02-908 (Washington, D.C.: Aug. 9, 2002).

³⁸ GAO, *Customs Service Modernization: Automated Commercial Environment Progressing, but Further Acquisition Management Improvements Needed*, GAO-03-406 (Washington, D.C.: Feb. 28, 2003).

³⁹ GAO, *Information Technology: Early Releases of Customs Trade System Operating, but Pattern of Cost and Schedule Problems Needs to Be Addressed*, GAO-04-719 (Washington, D.C.: May 14, 2004).

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

In May 2006,⁴⁰ we reported that CBP had begun to make progress in addressing our recommendations through the establishment and use of a program-wide performance and accountability framework, as we had also recommended. However, control weaknesses remained. For example, considerable concurrency still remained among increments, thus increasing the risk of continued cost and schedule overruns. Also, while earned value management⁴¹ was an OMB requirement, CBP discontinued its use on two ACE increments, thus limiting its ability to measure performance and progress.

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

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

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

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

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

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

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

US-VISIT

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

We first reported on US-VISIT in June 2003,⁴³ finding that program plans did not sufficiently define what specific system capabilities and benefits would be delivered, by when, and at what cost, and how US-VISIT intended to manage the acquisition to provide reasonable assurance that it would meet their commitments. Without defining such commitments, it was not possible to measure program performance and promote accountability for results. Shortly thereafter, in September 2003⁴⁴, we concluded that the

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

⁴⁴ GAO, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to be Addressed*, GAO-03-1063 (Washington, D.C.: Sept. 19, 2003).

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

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

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

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

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

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

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

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

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

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

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

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

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

In December 2008,³¹ we reported on a lack of effective DHS executive oversight of the program, including involvement from the DHS CPO and the CHCO. In addition, we again reported that DHS lacked a detailed schedule for implementing an exit capability, and that, among other things, cost estimates for the then proposed exit solution were not reliable, risk management was not being effectively performed, and the program's task orders were frequently rebaselined, thus minimizing the significance of earned value management-based schedule variances.

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

³¹ GAO, *Homeland Security: U.S. Visitor and Immigrant Status Indicator Technology Program Planning and Execution Improvements Needed*, GAO-09-96 (Washington, D.C.: Dec. 12, 2008).

Rescue 21

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

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

In May 2006⁵³, we reported that Rescue 21 continued to experience acquisition management weaknesses relative to requirements management, project monitoring and oversight, risk management, cost and schedule estimating, and executive oversight, and that these weaknesses had contributed to program cost overruns and

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

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

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

Secure Flight

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

We first reported on Secure Flight in March 2005,⁶⁴ finding that TSA had not yet completed key development activities needed to successfully deliver an operational system, such as finalizing requirements documents or completing required test activities. In addition, TSA had not developed performance goals and measures to gauge the effectiveness of the Secure Flight program, nor had it developed life-cycle cost estimates, which limited oversight and accountability.

In February 2006,⁶⁵ we reported that while TSA had made some progress in developing and testing Secure Flight, it had not followed a disciplined life cycle approach and, as a result, some project activities were conducted out of sequence, requirements were not well defined, and documentation contained contradictory information or omissions. Further, while TSA had taken steps to implement an information security management program for protecting information and assets, its efforts were incomplete, and that the program lacked schedule and cost estimates. Accordingly, we made recommendations to address these limitations. Later that year we reported that TSA had begun taking actions to address our recommendation,⁶⁶ including suspending development and undertaking a rebaselining, of the program.

In February 2007,⁶⁷ we reported that despite 4 years of effort, TSA had been unable to develop and implement Secure Flight, in large part, because it had not employed a range of acquisition and IT management control disciplines to effectively manage cost, schedule, performance, and privacy risks. At that time, TSA officials

⁶⁴ GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should be Managed as System is Further Developed*, GAO-05-356 (Washington, D.C.: Mar. 28, 2005).

⁶⁵ GAO, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: Feb. 9, 2006).

⁶⁶ GAO, *Transportation Security Administration's Office of Intelligence: Response to Posthearing Questions on Secure Flight*, GAO-06-1051R (Washington, D.C.: Aug. 4, 2006).

⁶⁷ GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, But More Work Remains*, GAO-07-448T, (Washington, D.C.: Feb. 13, 2007).

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

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

On January 7, 2009,⁵⁹ we reported that TSA had not demonstrated Secure Flight's operational readiness and had generally not achieved several conditions set forth in the Department of Homeland Security (DHS) Appropriations Act, 2005.⁶⁰ These conditions related to, among other things, performance of stress testing and estimation of cost and schedule. For example, we found that despite provisions for stress testing in Secure Flight test plans, stress testing had not been performed. Further, while TSA had made improvements to its life-cycle cost estimate and schedule, neither were developed in accordance with key best practices.⁶¹ As a result, the life-cycle cost estimate did not provide a meaningful baseline from which to track

⁵⁸ GAO, *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*, GAO-08-458T (Washington, D.C.: Feb. 28, 2008).

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

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

⁶¹ GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-35P (Washington, D.C.: March 2009).

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

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

SBLnet

SBLnet is a multi-billion dollar program that involves the acquisition, development, integration, and deployment of surveillance systems and command, control, communications, and intelligence (C3I) technologies to create a "virtual fence" along our nation's borders. Since 2007, we have reported on a number of SBLnet acquisition and IT management weaknesses that increased the risk that the SBLnet system will not perform as intended and meet user needs and expectations. For example, our first report identified weaknesses in how CBP was defining system requirements and managing program risks, including risks associated with acquiring SBLnet through a series of concurrent task orders.⁶³ In October 2007⁶⁴ and again in February 2008,⁶⁵ we reported that the SBLnet pilot, known as Project 28, was almost 8 months behind schedule in part because requirements were not adequately defined, contractor oversight was limited, and testing was not sufficiently performed. Later in 2008, we again reported on limitations in how SBLnet risks were being

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

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

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

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

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

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

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

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

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

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

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

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

Contacts and Acknowledgements

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

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



United States Government Accountability Office
Washington, DC 20548

October 22, 2009

The Honorable Diane E. Watson
Chairwoman
Subcommittee on Government Management, Organization, and Procurement
Committee on Oversight and Government Reform
House of Representatives

Subject: Post Hearing Questions on the Department of Homeland Security's
Information Technology Management

Dear Madam Chairwoman:

This letter responds to your request that we answer questions related to our testimony on September 15, 2009.¹ During that hearing, we discussed, among other things, the Department of Homeland Security's (DHS) efforts to improve its acquisition workforce capability and its management of large-scale information technology (IT) programs, such as the Secure Border Initiative Network (SBInet). Your questions, along with our responses, follow.

1. What recommendations do you have for DHS's Chief Procurement Officer to fill vacant procurement positions within the agency?

To begin filling vacant acquisition workforce positions within the DHS components in the short term, we recommended in November 2008² that DHS focus on expanding current recruiting initiatives. Since our report, the Office of the Chief Procurement Officer (CPO) has begun to do this by, for example, expanding its Acquisition Professional Career Program to include such career fields as program management and engineering, and planning for the addition of acquisition career fields to its centralized hiring program. However, our recommendations would also provide for determining whether the human capital flexibilities³ used to hire contract specialists can be expanded to address other acquisition workforce shortages. Further, tools to effectively monitor and evaluate the implementation of CPO recruiting initiatives are needed. For example, we have recommended⁴ that DHS develop implementation plans for these initiatives that include such elements as actions to be taken and related milestones, and needed resources.

¹ GAO, *Homeland Security: Despite Progress, DHS Continues to Be Challenged in Managing its Multi-Billion Dollar Annual Investment in Large-Scale Information Technology Systems*, GAO-09-1002T (Washington, D.C.: Sept. 15, 2009).

² GAO, *Department of Homeland Security: A Strategic Approach is Needed to Better Ensure the Acquisition Workforce Can Meet Mission Needs*, GAO-09-30 (Washington, D.C.: Nov. 19, 2008).

³ These flexibilities include direct hire authority which allows DHS to expedite hiring by eliminating such requirements as competitive rating and ranking.

⁴ GAO-09-30.

In the long term, DHS would also benefit from additional workforce planning, particularly for non-contract specialist positions, which were not covered in the succession plan DHS provided to the Office of Federal Procurement Policy in February 2009. Such planning would enable DHS to better understand its specific workforce needs and develop more tailored recruitment strategies, if necessary.

Beyond filling the acquisition workforce positions within DHS, CPO also needs to address its own staffing vacancies, as its staff play key roles in supporting the oversight of the department's acquisition function. To this end, we have recommended⁵ that CPO identify and align sufficient management resources to fulfill its oversight responsibilities in a timely manner. In response, CPO initiated efforts in 2008 to increase oversight staffing from 12 experienced acquisition and program management specialists to 58 by the end of fiscal year 2010. While the CPO office is making progress in reaching this staffing goal, sustained management attention is needed because DHS has been unable to provide sufficient resources to support its acquisition oversight function in the past, and its staff shortages continue to impact acquisition oversight.

2. What problems with SBInet have we learned from the pilot project near Tucson that could inform decisions about expansion of SBInet?

The pilot project, which is commonly referred to as Project 28, is part of Custom and Border Protection's (CBP) Secure Border Initiative (SBI). The goal of the SBI program is to leverage technology, tactical infrastructure, and people to strengthen control of the nation's borders. The Secure Border Initiative Network, or SBInet, is a component of SBI that is to acquire, develop, integrate, and deploy a mix of (1) surveillance technologies, such as cameras, radars, and sensors and (2) command, control, communications, and intelligence (C3I) technologies. Project 28 was an SBInet pilot project along 28 miles of the southwest border. CBP accepted Project 28 from the contractor 8 months later than planned because of system performance problems. As we have previously reported,⁶ this delay was due to a number of project management weaknesses, each of which provides lessons to be learned. These lessons include the following:

- *Ensuring that system requirements are adequately defined, to include involving users in defining them.* As we reported in February 2008,⁷ Project 28 system requirements were not adequately defined, and users were not sufficiently involved in their development. For example, SBI program officials and Border Patrol told us that Project 28 requirements were developed by the program's contractor with minimal input from system operators, including Border Patrol agents. Instead, the contractor based the requirements on information in the task order. As a result, the Project 28 system did not fully

⁵ GAO, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, GAO-09-29 (Washington, D.C.: Nov. 18, 2008).

⁶ GAO, *Secure Border Initiative: Observations on Selected Aspects of SBInet Program Implementation*, GAO-08-131T (Washington, D.C.: Oct. 24, 2007); *Secure Border Initiative, Observations on the Importance of Applying Lessons Learned to Future Projects*, GAO-08-508T (Washington, D.C.: Feb. 27, 2008); and *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, GAO-08-1086 (Washington, D.C.: Sept. 22, 2008).

⁷ GAO-08-508T.

address or satisfy user needs. For example, the software product that the contractor used to create the Common Operating Picture (COP)⁸ did not meet the agent's needs. Specifically, the COP was based on a software product that was designed as a law enforcement dispatch system rather than as a system to process and distribute the type of information being collected by surveillance systems (e.g., cameras, radars, and sensors). Similarly, agents stated that the laptops mounted in vehicles were difficult to use because they required the use of a pencil-shaped stylus to manipulate the screen while driving, which was impractical. According to Border Patrol agents, the Project 28 system would have been more useful if they, and others, had been given an opportunity to provide feedback during the system's development.

- *Ensuring that system testing is adequately performed.* As we also reported,⁹ Project 28 testing, which was intended to ensure that the system's components (e.g., radars and cameras) functioned properly in their intended environment, was not completed prior to the system's installation of the product. According to the SBI program office, this was due to time constraints. As a result, technical problems, such as radars being activated by rain and delays in availability of information from the radar at the command centers, were not discovered until after the components had been delivered and deployed.
- *Ensuring that the contractor is adequately overseen.* We have also reported that CBP did not maintain adequate oversight of Project 28 contractor activities.¹⁰ According to CBP, it selected a firm-fixed-price contract type for Project 28 in order to limit cost overruns,¹¹ which program officials stated necessitated a limited government's role in directing the contractor in its decision-making process. As a result, even though both program and contractor officials told us that they knew that the timeline for completing Project 28 would not be met, program officials said that they chose not to modify the contract because that would make CBP responsible for costs beyond the \$20 million fixed-price contract. Not until August 2007, which was well after the system acceptance milestone, did CBP exercise greater influence in milestone setting and corrective action planning and oversight.

-- -- -- -- --

In responding to these questions, we analyzed previously issued reports and testimonies. We performed this analysis in October 2009. The reports and testimonies on which this correspondence is based were performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

⁸ The Common Operating Picture is a uniform presentation of activities within specific areas of the border.

⁹ GAO-08-508T.

¹⁰ GAO-08-131T.

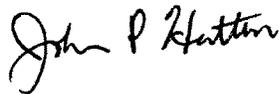
¹¹ In April 2007, CBP and its contractor reached an agreement to modify the terms of the Project 28 contract, increasing it to about \$20.66 million. CBP modified the contract to add several project design requirements that the existing task order did not address.

Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-3439 or hiter@gao.gov. Key contributions to this report were made by Tonia Johnson (Assistant Director), Amelia Shachoy (Assistant Director), Scott Borre, Elena Epps, Rebecca Eyler, Lee McCracken, Anne McDonough-Hughes, David Plocher, and William Russell.

Sincerely yours,



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



John P. Hutton
Director, Acquisition and Sourcing Management

Ms. WATSON. Well, I would like to thank all of you for your testimony. And we are now going to move to the question period. And we will all proceed under the 5-minute rule.

And I am going to first start with Ms. Duke and some of the points you brought out in your opening testimony, but I want you to consolidate them and be more specific. DHS has been operating for more than 6 years, during which you have played a key leadership role in shaping how it requires and acquires and manages large-scale IT programs. It would certainly seem that 6 years is a sufficient amount of time for the Department to become a mature and capable acquirer and manager of IT.

How would you characterize where the Department stands in its capacity to acquire and manage major IT instruments? And please describe how DHS matured in developing better capabilities for managing its investment portfolios.

Ms. DUKE. I think it is important to note that we have three roles. We're both providing the services in many cases to DHS headquarters, we're building the policies and procedures and then we're doing the oversight.

Both the GAO and the IG have talked about resource constraints. We are hoping this month to reach 100 people in the CIO's office. So I think when we think about all three roles, which is doing the IT operations, building, writing the policies, putting the procedures in place and then actually performing the oversight, I think that puts in perspective how much we really accomplished in 6 years.

So what have we done that specifically, I think, is going to make a difference now in going forward in the iterations of policies we have done? One is we have strengthened the role of the CIO. Mr. Spires is the Chief Information Officer for the Department and has all the authorities of Clinger-Cohen plus. He has authority not only over IT investments but over IT portions of non-IT investments. And we have integrated the IT oversight into our major acquisition program so that there's a consolidated look at acquisition for our senior leadership.

Our new deputy secretary Jane Holl Lute, chairs our acquisition review board and she is personally looking at the IT and non-IT investments. And that's one of the reasons we have had such an increase in our number of board reviews.

The other thing that we're doing that may sound simple but is really making a difference is each one of these review meetings we used to document having the reports and give recommendations. What we have switched to is we have precise action items that are tracked. And so for each one of these meetings we say what the program needs to do for its next stage of maturation, and we're tracking on those. And that is reported to me biweekly.

And the final thing I will say is we have a new on-line system for our leadership called NPRS that gives the state of affairs for each program in terms of cost, schedule and performance. And that is going to give visibility continually, not only as we have these board meetings, but in between those, in terms of the performance of each of the acquisition programs.

Ms. WATSON. That probably answers the next question I was going to ask. That you assure our subcommittee that all IT pro-

grams are being reviewed at least once a year for all major development milestones. And I think that's what you're describing.

Ms. DUKE. Yes ma'am.

Ms. WATSON. What does the new DHS leadership have to say about the deficient processes in place for overseeing agency investments, and have they established a long-term blueprint for strengthening the investment management process? And if so, how does it differ from the prior administration?

Ms. DUKE. I think the new Secretary, Secretary Napolitano, she came in with not only a knowledge of the mission from her leading in the State of Arizona, a border State, a lot of DHS-type activity. But I think from being a Governor and being in the role of managing a bureaucracy, she also came in with a very, very strong understanding of how management has to effectively work not only the CIO, but the personnel piece, the financial piece. So she immediately considered me and the management staff as a key partner, considering how we're doing, not only meeting the mission but effectively and efficiently meeting the mission, including IT. So I think that her work as Governor came in with a presumption that we would do everything not just to meet mission, but with good business sense. And that really has put management, I think, on the front burner for each of our mission decisions and has really bolstered our visibility in the Department.

Ms. WATSON. I understand that DHS is in its planning stages of developing its new headquarters.

Ms. DUKE. Yes.

Ms. WATSON. Here in D.C., which will consolidate a significant number of legacy operations and sites into one campus. What assurances can you offer us that a multibillion-dollar investment like this, with so many major program and infrastructure components as part of its nerve center, has been designed with effective capabilities and requirements for meeting the mission and the needs of DHS for decades into the future? And do you have specific programmatic life cycle cost estimates and benchmarks for delivering that you can share with our committee today?

Ms. DUKE. There's actually three pieces of our headquarters consolidation. There's the St. Elizabeth Campus, which has gotten the most visibility, and that is going to be where the Secretary and the senior leadership are. Additionally, we will keep about four of our existing facilities, including the Secret Service Building and a few others. And, additionally, we will be consolidating the remaining 40 or so leases from the National Capital Region into about 1.2 million square feet, so we will actually end up with about five to eight facilities.

The way we're managing that project is through management of the Chief Administrative Officer. We were given 20 positions to manage that project in DHS. We got them in fiscal year 2009, which is really a recognition of our appropriators that you do need the staff to manage that appropriately. Additionally, with leasing, because this is a GSA site, we are using GSA as our execution agent. So we are using our 20 assets to determine the requirements to make sure we have a stable program that meets DHS's headquarter's needs. All the work is being executed through GSA. They are awarding the contracts and they are managing the contracts.

And they have the expertise and the bandwidth to actually do those programs.

So I think the fact that we have a program office fully dedicated to this, in addition to DHS's expertise in facilities, will help ensure this project goes forward.

Ms. WATSON. I want to thank you, Ms. Duke.

And I now recognize our ranking minority member, Mr. Bilbray, for 5 minutes.

Mr. BILBRAY. Thank you, Madam Chair. And let me just say to our witnesses, as I ask questions to one Member, if there is anything you want to add to it, this is a dialog, we're trying to get into it.

Ms. Duke, I'll start with you. Where was—let me just say, where was the Department coming from—and I know it predated the Department to some degree and got into it—but this whole issue of the virtual fence that technology could replace structures and then have Boeing walk in and say basically, We can handle all of this, you don't need to do this, you don't need to do that. How did that evolve?

I mean how does a—I mean, I think all of us here kind of trust our lives to Boeing every couple of weeks, but I am not so sure I would choose Boeing to be a security force for the national frontiers. How did that evolve into such a bet on technology that ended up going—you know, basically going bust?

Ms. DUKE. Well, I think that our approach to the southwest border started with looking at what mix of solutions do we need to appropriately secure the border. We call it an alternatives analysis. What mixture of people, Border Patrol, tactical infrastructure—which includes fence and roads—and technology do we need based on the geography and topography of especially the southwest border? And we started doing a very systematic look.

I think that the deviations in the program from taking a really bottoms-up look ended up by the urgency—or driven by the urgency of protecting the southwest border. So I believe if there is one fault that I can point to to be kind of a root cause, it would be instead of completing the analysis of alternatives and looking at what are the operational requirements of the Border Patrol to secure the border, and building up to what we buy, because of the urgency there was a predisposition to jump to solutions, to jump to technology, whether it be tactical infrastructure or technology, but not really take the time—

Mr. BILBRAY. Looking for a silver bullet.

Ms. DUKE. Looking for a silver bullet, or jumping to fix this rather than looking at the needs.

Mr. BILBRAY. Did anybody take the time to go down and look at the terrain, to look at the operation? I mean, the fact is I am not against the IT application there. But anybody who has ever been there realizes that jersey walls across the canyons were going to do a lot more a lot quicker than putting up towers with sensors and whatever.

I hate to say this. I am a history major. It reminds me so much of what happened after World War II when the Air Force came in and said, we don't need the Army, we don't need the Navy; you

know, with Atomic Age, all you need is airplanes that can drop bombs and all we other services should be abandoned, so bet on us.

And Korea—and we were actually moving toward that. Korea taught us real quick what a failed concept that was based on that. That seemed like this element. But to be fair with you and with the agency, I would ask the question how much politics goes into it, too, with people not liking the concept or the message sent by putting barriers up at the border, and how much of that influenced it? And then how did Boeing end up with this thing?

Ms. DUKE. I believe that Boeing was—Boeing was selected because what the acquisition strategy, what we were looking for, it was a major systems integrator. And Boeing brought both the ability to help DHS in determining what mixture of technologies and infrastructure go at the border and the capability to perform.

I think in terms of the tactical infrastructure, that was our first focus, the fence. In terms of technology we are moving forward very carefully and we are doing capabilities demonstration to see what benefit technology can bring.

But I think in going to Mr. Taylor's comment that we should move carefully, and Mr. Hite's new programs, we are not wholesale just deploying technology across the border. We are doing two small test projects in Tucson and Aho and seeing does this technology help the Border Patrol.

Mr. BILBRAY. And let me just say I have seen technology work right. We were actually back in the seventies, using ground sensors that had been developed during Vietnam. And the Border Patrol were using them back then. There were all kinds of technologies. They're still using those. You don't drive a road in the border region without our guys knowing that a car has passed.

What about the VISIT system? One of the great successes is the fact that we now have the data base and biometrics on everybody that comes into this country legally. And a lot of people forget that 40 percent of the people who are illegally in this country are overstays and would fall in that category. That's been a great success.

But what's happened over a decade of waiting for the Exit program? And I know my time has expired. But that's very important. How can we move that agenda? And it appears that no matter who is the administration, this issue is being avoided, and that's the Exit part of the VISIT program, so we know who is left, which makes it a lot easier to know who is left in.

Ms. DUKE. I think the policy decision on Exit has not been made. In terms of management of my controls, what we're making sure is we're not spending money on a contractor until that policy decision is made. And so I do believe, Mr. Bilbray, that is one where we have not made progress on it.

The good news from the management perspective is we're not just out there kind of doing things while a policy decision is made. So I think that's the approach that this administration is taking, is to decide what Exit is.

Mr. BILBRAY. I appreciate that. And let me just close by saying this. I thought the policy decision was made by Congress when we passed a law that says this program will be plugged in. Now, I appreciate you get the political pressure. You got people that say it

is more important for people to freely pass back and forth across that Tijuana crossing every day; that commerce being able to come into our ports is more important than securing and making sure that only good things get across; that the implementation of the law is secondary to political pressure by business and political groups. So I think that a lot of these problems are based on politics, not on policy, as you said, or technology. But we need to separate those two and make sure that we take care of the politics and you take care of the technology.

Thank you, Madam Chair. I yield back.

Ms. WATSON. We now yield to the distinguished gentleman from Texas, Mr. Cuellar.

Mr. CUELLAR. Thank you, Madam Chair. Thank you for holding this meeting. And I want to thank the witnesses for being here. I guess March 2003 is when we had the reorganization, 22 different agencies. And I know from that time there's been a lot of good progress that Homeland has done, and I appreciate all the work that the men and women have provided.

At the same time, there have been some issues, some of the issues that the gentleman just brought up, talking about the border fence or the technology. Since I live in Laredo, I am very familiar with it, extremely familiar with it. And I've always wondered why we always try to reinvent the wheel. I am very familiar with the SBI part of the other committee, Homeland. My understanding is that the Department of Defense has already done a couple of pilot programs and done a briefing on them, where the sensors and the cameras are at a fraction of the cost of what you all have invested already. So if it has worked for the military, why do we have to go out there and reinvent the wheel where it has been already tested? It is proven technology at a much cheaper price. And here we are spending billions of dollars, No. 1, on technology.

And I know one of the excuses was, oh, we're still working on it, but don't worry we're going to bring team A now to work on the issues. This is one of the things.

So I wondered, you know, so what was this, team B, team C, and now we're bringing team A in. And, oh, we didn't know it was going to be that hot on the border. I mean, there were a lot of things that came up on that.

But I would ask you to look at the proven technology. And if you all haven't sat down with the Department of Defense, with the specific agency, and said to the Department, I'll be happy to sit down with you, I think it will save you probably billions of dollars.

The other thing is if you look at it, it took us less time to win World War II than what we have been trying to organize, reorganize. And I saw your testimony and you're saying GAO is looking backward. We need to look forward. But we still have to look backward to see what the problems are.

We still know Homeland Security, what, had morale issues. There was, what, one of the last ones, or had one of the biggest morale issues of any agencies that were surveyed. On top of that, we have looked at some of the issues that we have here. I can give you specific issues as to how you all contract and how you do this, and I can give you examples what's happened in my hometown without going into much specifics. But one of the things that I really would

like to see is your performance measures. I have a list of questions, Madam Chair, that I would provide to the clerk.

Ms. WATSON. You still have time.

Mr. CUELLAR. And I would like to request that we can submit this for the record.

Ms. WATSON. Without objection.

Mr. CUELLAR. Thank you, Madam Chair. And ask you to go ahead and bring them in. But I want to know how do you measure the work that you're doing, what sort of indicators do you have, performance measures that you have, how do you indicate success? I mean, if you can't tell us what we're doing, then we don't know if we're rewarding success or failure. So I would ask you to—and, I don't know, Madam Chair, 2 weeks, is that sufficient time?

Ms. WATSON. I would think so.

Mr. CUELLAR. I would ask you if you can submit this to the committee within 2 weeks to the list of questions that I have.

So I guess my statement now, or my question is: When you hear from the GAO or the inspector general, what do you do with the recommendations, what actually—what's the thought process? Because they've given some recommendations and you're considered an at-risk agency, which means vulnerable to fraud, waste, mismanagement, etc. What actually goes through a thought process? When GAO gives you a report, what do you all do? Look at it, put it upside down and say, OK, let's move on? What's the thought process?

Ms. DUKE. We take the reviews of the IG and the GAO very seriously, in addition to the oversight provided to us by Congress. Most of the issues, it's very rarely that we nonconcur with any of the findings. We might nonconcur on a specific fact. And I think that when you look at the reports, generally they're saying we're moving in the right direction, we just have gaps still in the effectiveness of what we're doing.

So what I look at, No. 1, are there any indications that we're going in the wrong direction; are our practices not best practices; do our policies have areas that GAO or the IG are saying are wrong or not good for the Department? So the first thing I look at is a systems look of are we going in the right direction? And then the second thing I look at is what specifically is called out on a program. Is that a system vulnerability? So if they review one program, like SBInet, does that same vulnerability—for instance, cost estimating is one. We feel that even though the GAO or IG might call that out as a vulnerability on one program, we think that's a systemic vulnerability or we see it coming up, so we address those first.

Mr. CUELLAR. When you get a report, do you sit down with a follow-up with GAO and say, We got your recommendations, do you have any suggestions on how we can implement this because of cost or whatever the factors might come in?

Ms. DUKE. Yes. We sit down with them on specific reports. We also sit down with them just regularly, both with the IT group and there's an acquisition group, and just look at overall. We have also used some of their best practices. We're using GAO's cost estimating best practices as part of our policy, so we leverage wherever we can.

Mr. CUELLAR. Madam Chair, can I just ask GAO, do they follow-up? I mean what happens afterwards? I know my time is up. But I am kind of curious on—there's a report that's given; then what happens after that?

Mr. HITE. We have interaction on a continuous basis with the Department to ensure that the recommendations are implemented. Within 60 days after the report, they have to report formally to the Congress on what they intend to do to address those recommendations. Every year we followup on the status of our recommendations and work with the Department to find out where those things stand. If it deals with major programs like SBIInet or US-VISIT, we have work that is going on continuously, so it is part of that engagement with the agency. We're constantly looking to see what's happening. And believe me, we're encouraging and urging faster action on some of these things.

Sometimes there's some misunderstanding in the communication. Sometimes when we write a recommendation, we think it's abundantly clear to anybody, exactly what we meant. But sometimes it calls for some clarification down the road, and we have worked to do that.

Mr. CUELLAR. Thank you, Madam Chair.

Ms. WATSON. Thank you. I would like now to yield to Mr. Luetkemeyer, the gentleman from Missouri.

Mr. LUETKEMEYER. Thank you, Madam Chair. Mr. Hite, do you have any private sector experience?

Mr. HITE. No sir.

Mr. LUETKEMEYER. You have worked for the GAO all your—

Mr. HITE. I worked for GAO for 32 years, except for my details to the Hill.

Mr. LUETKEMEYER. OK. Very good.

Ms. DUKE, in the report that I've got here of the summary of some of the reports that were done, back in November 2008 it says that the agency concurred with all seven recommendations but appears that they have only implemented two of the recommendations. Can you explain that?

Ms. DUKE. I am not sure exactly what report you're referring to, which GAO report.

Mr. LUETKEMEYER. It's a 2007 DHS report where it obligated \$12 billion for acquisitions. GAO recommended certain steps by DHS that would take more thorough—could take to more thoroughly implement the following investment review process. And in here it says the agency concurred with all recommendations, but appears that they have only implemented two of the recommendations.

So I was just curious why we didn't implement the rest or what's the problem? Are we getting on it?

Ms. DUKE. Did you want to say something?

Mr. HUTTON. If I may. I am John Hutton with GAO. I was one of the authors of that report. And as Randy said, Mr. Hite said, we do followup on our recommendations. But what we won't do initially is close the recommendation if we haven't seen something executed a little bit further down the line toward fruition.

I share what Ms. Duke has said, that they have taken several steps that get right at the specifics of our recommendation. But we really believe, and I think Mr. Cuellar mentioned earlier, the im-

portance of looking back. We feel that the work that we have done where we have looked at the execution of their investment reviews through 2004 through March 2010—or 2008—it just was not being executed. And we came up—we identified several reasons why. So we think it is important that you look back, find out why it hasn't worked in the past. But to me, execution—follow through to the end is what's important here before we're going to consider it a recommendation fully met.

Ms. DUKE. And that report, now that I understood it a little more fully, we were moving in that direction. But again the GAO thought we weren't making enough progress. So some of the specific recommendations was we're not holding enough board meetings, we're not documenting it properly.

Mr. LUETKEMEYER. You're not having enough meetings?

Ms. DUKE. Enough board meetings, yes. They looked at how many acquisition review board meetings we were having, the documentation of them, the followup and those type of things. I think we have corrected that. At this point the recommendations are still open because they want us to demonstrate sustained performance in actually keeping the system going. But, yes, a lot of it was counting the number of review board meetings we had and the documentation of them.

Mr. LUETKEMEYER. Not to be argumentative, but having a meeting doesn't mean anything unless you do something in the meeting. You can have a meeting every day, but if you don't do something in a meeting it's wasting everybody's time. Also, with regard to this report it says that they found 14 major investments that experienced cost growth, schedule slips or performance shortfalls. Have those problems that caused those things to happen, have they been fixed?

Ms. DUKE. We have programs that are—

Mr. LUETKEMEYER. Or did we have more meetings to discuss it?

Ms. DUKE. The way we're fixing the problems of those type are to have putting in place what's called an acquisition program baseline that sets cost.

Mr. LUETKEMEYER. Why was it not put in place to begin with?

Ms. DUKE. The programs were active when they came to the Department and they were not in place. So we're going back and we're fixing the programs that came into the Department. Those programs, we only have a few new-start programs since the Department stood up. SBInet, CIS transmission, most of those programs existed in legacy agencies, and we're trying to build a structure around them without stopping them, and balancing, building the controls while they're still performing. So, yes, it is a going-back exercise.

Mr. LUETKEMEYER. Sir.

Mr. HUTTON. Sir, I would like to continue the discussion a little bit on the question about what steps have been taken. And Ms. Duke mentioned one of our points was about the meetings. But I want to add some context to that. What we are talking about is that we looked at—I believe it was 48 major investments over almost a 4-year period. And there was already a process in place at the time. If it was applied with discipline and, for example, the programs had mission need statements that were approved, if they

had operational requirement documents that were approved, if they had acquisition program baselines that were approved, and DHS was actually involved in holding a meeting, although I think it's more than just a meeting, it's getting Department-level approval of that investment as it moves forward, that's the key.

But some of our other recommendations were that two of the components didn't have their own process that they're supposed to have that's consistent with the departmental process. That's just another example.

So we have several recommendations that I think get at the core of some of the problems that we saw. And I think that while they have taken some steps—and I would agree with Ms. Duke—I didn't want to leave the impression that it was just having a meeting.

Mr. LUETKEMEYER. OK. Thank you. I see my time has expired. Thank you Madam Chair, or ranking member.

Mr. BILBRAY [presiding]. I want to follow back up, Ms. Duke. I don't mean to be picking on you. But the issue of policy with the VISIT system, was it the policy of the Bush administration that the Exit part of the VISIT system was not going to be implemented at that time?

Ms. DUKE. Mr. Bilbray, I honestly don't have firsthand knowledge of that because I wasn't involved in the policy decisions. My role was more do we have an actual requirement to execute? So I honestly can't answer that question.

Mr. BILBRAY. I am trying to remember, but I remember pretty closely when the VISIT system was being pushed by Lamar Smith and Chairman Sensenbrenner. And as far as I know, that was not a voluntary authorization, it was a mandatory implementation. And I still have a problem with why it hasn't been implemented, unless they're still using the excuse that the technology doesn't exist to monitor those who are leaving the country. Or if the executive branch claims the authority to veto the legislative intent with the fact that we feel that it's inappropriate at this time to implement the legislative mandate. And you have no recollection where the justification was that was outside of your realm?

Ms. DUKE. No, I have never heard any discussions that the issue was technology. It's more what the Exit solution would look like, the specifics. And if you would like, I can get back to you for the record on where we currently stand with the Exit solution implementation. But it is not a technology issue, it was just more—and it wasn't even an issue of whether we are going to do Exit or not. It was going to be what precisely is Exit going to look like.

Mr. BILBRAY. I am kind of interested to see what decade we come to that conclusion, what it's going to look like. Because it is one of those situations that after 9/11 there was a lot of talk about how terrible it was that the bureaucracy wasn't doing the commonsense things and implementing and overlooking and avoiding things. And that is State and Federal bureaucracy. But now after all this time, to go back and say we're still trying to figure out what we want this to look like. At a time—and let me just say this—at a time that our neighbors to the south are stopping traffic and going through traffic as it comes south, we are worried about if somebody may have to slow down for a monitor to pick it up. And how many of us drive through toll booths that electronically pick up our data?

And it seems like if it's to raise money, if it seems like it's to generate revenue, the technology is there and implementation is OK. But if it is to regulate the Federal constitutional mandate of immigration and border security that the Federal Government has, we just don't know how to implement it.

And maybe what we ought to be talking about is just going to the State agencies that are handling toll roads and saying, You know, maybe we want to contract with you guys to do it, because they seem to do it pretty well. I mean I avoid the toll road, the Dulles toll road, like the plague. But I drive next to it every day that I drive south—and south meaning southwest. And they sure seem to be able to get that technology working there.

So I want to leave an open invitation that, please, if there's political barriers to the implementation of the law, we need to know about it. And frankly, I think that's one of those things that we need to address.

The other issue that the gentleman from Texas brought up, I want an open invitation of how we can do it better, where you see the system needing to be improved. Because we're going to be following up on why are we reinventing the wheel. When we have sensors and technology that's been used by our military and our clandestine services for decades, why aren't those technologies being looked at further rather than what appears to be last?

And a lot of this is politics. Look, I have been in the game since I was 25 years old. I know how much influence of the politics is. And politics can be good or bad. Let's thank God that somebody was willing to stand up and tell the bureaucracy that we can't do all observations from outer space; we are going to try this little remote-control airplane called the Predator, which has been one of the greatest success of military application within decades.

But the politics of the lobbyists here pushing us to go use technology unproven, the silver bullet that looks so great when someone is selling here in Washington, I think those are things we are going to address. And I leave you an open invitation, as much as you can within the law and protocol, to work with us so that we're not just digging through your records, you're able to participate with us so we address the issue and serve the community we're sworn to serve, and that is the American people.

Thank you very much. I appreciate it.

Go ahead. Mr. Hite.

Mr. HITE. Yes, sir. Just a couple thoughts concerning US-VISIT Exit. I can't comment to the extent it was a policy or political decision. I'm not aware of that. The real challenge with dealing with US-VISIT Exit is that the physical infrastructure was never there to screen people as they were leaving this country. It has always been there to screen people as they come in, and there are extraordinary physical space limitations for land-based borders as well as in airports and seaports, too.

So the real issue, the real challenge that is trying to be dealt with now with respect to US-VISIT is not technology, it is operationally how are we going to implement this? How are we going to implement the technology? Who is going to do what? Is TSA going to do it at the checkpoint? Is CBP going to do it at the gate for land borders? How are we going to expand the physical lanes

in a very constricted environment in some of these urban ports of entry? So, that is the nature of the challenge that is being dealt with now.

Mr. BILBRAY. Let me just say this: The largest land port of entry in the world is being rebuilt today. My question to you is as we're rebuilding that whole structure, putting diagonal lanes, increase, double them up on there, are we engineering and designing into that new system the Exit system? Is that being engineered in there? Do you know?

Mr. HITE. I can't tell you that, but that is an excellent question, and that is what should be dealt with when you look at a portfolio of investments and say, we invest in physical infrastructure here; how does that relate to what we want to accomplish through technology, through the US-VISIT program? So let us make sure they work in lockstep.

Mr. BILBRAY. Let me tell you as someone who has worked on border issues since the 1970's, the political pressure is to get people into this country and back and forth as quickly as possible, and security is way down the list. And the trouble is we don't have that kind of lobby and political pressure on the bureaucracy to implement the law as we do as to make sure that commerce is never obstructed to any degree.

And frankly, as you said, the infrastructure, if we were charging at the border, you darn well say that infrastructure would be there like that. But when it comes to securing and implementing the requirements of the representatives of the people of the United States, it has been put off for a decade.

So I guess that is one of those things we need to make a priority, and my staff will be checking with the millions that are going into redesigning and rebuilding the border crossing at Tijuana, let us see if the Exit part of it is being executed. Let us see if the administration is following the law or responding to the political pressure.

Thank you very much.

Ms. WATSON. Mr. Bilbray, we intend to hold a series of these hearings and make recommendations. Since we have a new administration, it is just mind-blowing. When we put the Department of Homeland Security together, we brought over 750,000 people from various agencies and departments who had their own budgets, and we have to see that this Department functions for its intended purposes. And we might quote a number of years, but still we have the kinks to work out. And so have faith that when we gather all the information, we will make the kind of recommendation so Homeland Security will indeed secure our homeland.

I would like to go on now to Mr. Taylor. And your testimony cites the explosive growth of contractor support in the CIO's office at DHS since 2007. And what are the causes of the staffing shortages, and is it a cultural or due to ineffective management? I know we threw all of it together; that is why I made that comment. And we just want to know, has DHS made the significant alterations to its staffing plans since your recommendations were made to do so?

And you can chime in, Ms. Duke.

Mr. TAYLOR. Sure. In response to the recommendations, the Department has put together a plan to significantly increase the

CIO's office, and I think Ms. Duke mentioned that they're going to hit 100. The total that they plan to do by 2011 was something like 236, I believe. So they have responded to that.

To answer your question about why it got to where it is, I think there were—we identified just a number of potential reasons. There has been a push historically to reduce the number of permanent, full-time Federal employees anyway and rely more on contractors in the past. Also the IT area is one of these areas where we all sitting at this table and in the Federal Government have had a heck of a time hiring qualified people. So it is tough to start with because we have trouble competing with the private sector, and there are barriers still in the hiring process to make it frustrating for someone to try to come from the private sector and get into the government if they're not experienced with the process. There is background checks. Sometimes it takes months to get someone in. They get frustrated. They have another offer, they move on.

Ms. WATSON. With the job loss and the situation is now, do we see more people out there that would be eligible?

Ms. Duke.

Ms. DUKE. We see some increase in—especially at the lower—excuse me, the higher grades, so people coming out of industry with pay parity, kind of the 14, 15 and above levels. Our biggest challenge in recruiting is at the journeyman level, the high working level, the GS-12s and 13s, and we're not seeing too much of an increase in those, but we're starting to see.

Additionally we're working on some with Mr. Berry, who is now running the Office of Personnel Management, on getting some flexibilities with hiring.

And the third thing we're doing, because you specifically mentioned contractors, is not only in the CIO's office, but across DHS, we're looking at the balance of our work force. Within CIO we have adjusted our work force to—we were going to just about 200 through contractor conversions of essential functions; our goal now to be at about 325 Federal employees by 2011. We think we can do that with the existing budget by making core functions of Federal employees. It is going to be a human resources challenge to recruit that many people for DHS, though.

Ms. WATSON. Let me move on. We're losing a lot of our time. Let me address this to Mr. Hite and Mr. Hutton. I want to begin with a very general question. And how would you characterize the success of DHS in delivering large-scale systems that are on time, under budget, and that meet preestablished requirements? And let me go, I guess, to Mr. Hite.

Mr. HITE. A very general question like that, overall I would say the success has been poor in doing that. What we have seen is a pattern of programs—as I mentioned in my oral remarks, a pattern of programs getting started and allowing to proceed for many years, where they're rudderless basically. And then when these problems come to the attention of certain principals, then they get acted on, and, through many years of efforts, the programs begin to be brought back on track. That, to me, is not an indication of a successful program.

To measure success, and success can be anywhere on the continuum from achieving everything we possibly hoped of to achieving

nothing, you need to establish what it is you're trying to deliver, and you need to make that commitment, and you need to measure yourself against it. Time and time again on some of these programs I've seen where they get started, and they're allowed to proceed in the absence of any commitments, without defining what is going to be done by when to deliver what kind of capabilities to produce what kind of value. If if you don't have those commitments, it is hard to judge success. You can proceed for a while and deliver some capability and declare success.

One of the things we have pushed for in our reports, and one of the things I would emphasize, is that when programs start, they need to be grounded in clear expectations surrounding what are we going to get at the end of the day, and what is it going to cost us? And then you need to measure yourself against that.

Ms. WATSON. In 1996, Congress attempted to strengthen the IT investment management oversight process through new requirements for capital planning and investment that we use at agencies. Both agency procurement and information officers were charged with overseeing the following activities.

Would it be fair to say that ineffective review processes are the cause of wasted investments like the eMerge program, and is the investment review process at DHS broken? If so, how much of it is due to inadequate attention from agency leaders? And we will start with you, Ms. Duke.

Ms. DUKE. I think that we have a ways to go to deliver the robust acquisition review program that this country deserves, but I don't think it is because of a lack of attention. I really think that, right or wrong, when the Department was formed, it didn't exist. So the programs existed, the \$6 billion worth of IT investments existed, and the things that GAO and the IG are saying we should have didn't. And so programs came into the Department, and they didn't have cost scheduling and performance metrics.

So what we've had to do in setting up the program is go back and put those in place and then start measuring against them. So the result is that things have taken time because we can't measure performance until we actually put performance metrics into place.

And so in a lot of the first years of the Department, we've been in a remedial mode. We've been putting things into place. And now as we put them in place, we can measure against them and track performance. But we've been—I think that some people erroneously believe that we started out kind of zero, we start out in a hole. And I think we've dug ourselves out of the hole, but we're not to the preciseness that this country deserves yet.

Ms. WATSON. I understand that Senator Carper has introduced legislation that would make significant alterations to the IT investment management process, including increased requirements for budget justifications and transparency during the development life cycle. And should we be using firm financial benchmarks at DHS for determining when to pull the plug on programs with cost overruns or deficiencies beyond certain thresholds? And are there statutory changes that could be made to strengthen the oversight processes in place at DHS, or are there problems more related to the execution of current processes in place? And let me just start with the GAO, and then we will go on to the IG.

Mr. HITE. Madam Chair, my position on that is you shouldn't have to legislate good management.

Ms. WATSON. That is true.

Mr. HITE. And, in fact, legislating good management can sometimes be a dangerous thing to do, can sometimes have unintended consequences. What I believe is that the mechanisms are in place, they're understood. The issue comes in execution and implementation. And in the absence of implementation, it doesn't matter how great a process or a review board set-up that you have, you have to execute it.

So I would go back to something I've said many times is that for a program of this kind of magnitude to be successful, there are literally 100 stars that need to align, and any one of those stars can have a major impact on that program. So there are a lot of things that have to be done right, and oversight is one of those variables, but there are a whole lot of others in the equation that need to be done right. And the reason that some of these programs have fallen on hard times over the years is through a combination of these things.

And to Ms. Dukes's point about the fact that they inherited these agencies, these component agencies, and inherited their programs, and hence the Department didn't have its own institutional ways of overseeing, that is true. The components should have had their own, and the components should have been paying attention to them, and the components should have been doing those programs correctly, and that wasn't happening.

Ms. WATSON. Thank you.

Mr. Taylor.

Mr. TAYLOR. I would like to back us up. I think the most valuable service that a procurement office performs is helping management determine what its the requirements are in the first place.

What we've seen over time is a lack of firm, measurable requirements, that what is it we're trying to accomplish with this technology application, what is it we're trying to achieve? And we start with those kinds of problems, that and the constant pressure to respond, respond in terms of disasters, respond in terms of crisis at the border. We need to do something quickly, so we don't have time to really work through all of our requirements, and so the requirements change, and whenever that happens, you have serious problems with oversight.

You also have a problem where it's not so much that the Department doesn't have the infrastructure identified as being able to staff it as we've talked about, but it is also being able to followup and manage at the component level. So we need to focus the kinds of authorities we have in the CIO at the Department level on the component CIOs and have them responsible for identifying and managing IT budgets and staying on top of IT projects.

Ms. WATSON. Thank you.

And, Ms. Duke, would you like to add to that?

Ms. DUKE. I agree with both the GAO and the IG. I guess in terms of what the GAO said about how it should be, I agree totally. Unfortunately as the execution person, I have to deal with reality and what is, not what should be and trying to get to what should be.

I think that we do—visibility into the budget by the CIO is very important, and we have instituted that through our performance review process. And I think that we have to put the performance measures in place, hold the program managers accountable and the components.

And I think also we have to have the discipline to be nimble and quick because our enemy is nimble and quick, but have the discipline to not just do things fast. One of the earlier cultural pressures on DHS was to do it fast, and that seemed to be the measure. And we're trying to right now hold the line at doing it fast enough to meet our threat, but do it well enough, and that is a tradeoff between cost, schedule and performance. And that is one of the biggest cultural changes we're in the midst of right now.

Ms. WATSON. Mr. Bilbray.

Mr. BILBRAY. Madam Chair, I'm going to yield my time to the Chair. I just want to say in all defense, we've gone through 8 years without another major attack, so I think we can say to DHS, congratulations, but at the same time understanding there are huge amounts of waste of resources, effort, critical resources that could be used in other locations.

So we've been successful. We don't know if that success is through accomplishment or dumb luck. But we will take it whatever, but let's move on and not depend on—let's make sure in the future that dumb luck is not what we're depending on. We have a responsibility to straighten this out and try to get into it and make it as effective as possible so we can move on from there.

And I yield to the Chair.

Ms. WATSON. Thank you so much.

Let me move on, and this will be our last item of questioning and information.

I would like to hear something about a detailed assessment on the lessons learned from the failed eMerge program and how we can be assured that its offspring, the transformation and systems consolidation, referred to as TASC program, will not become another abandoned project that wastes over \$50 million. So where is DHS in developing the necessary requirements for TASC? Has the TASC program been reviewed by the appropriate investment review boards and developed the appropriate justifications for funding and mission needs? And how did and why did we wait so long before terminating the original eMerge program, and what information was missing to determine that it would not be effective? And what are your life-cycle cost estimates for this program and estimated date of completion?

So any of you can jump in, but I would like to start with Ms. Duke.

Ms. DUKE. Regarding eMerge, the two biggest lessons learned from the original program that was done within the first year of the Department was, one, it was a noble objective. We have severe weaknesses in financial systems in many of our components to the point where we cannot get to a clean financial audit with the current systems. That has to be corrected.

Second, we learned from industry that a single—or a shared financial system is essential to an effective merger, and so we need some type of communication between our financial systems to be

the mature Department that this committee and the country wants us be to.

What we did in the initial eMerge was I'll say two lessons learned. One, we took what we call the nuclear approach. We said we're starting over. Give us a brand new system that's the utopic system, one system deployed quickly within months in the Department, and it is too complicated to do effectively in that type of wholesale just quick-hit approach.

The second thing we learned from it is that we're relying too much on industry for the solution. So it's good to rely on industry to deliver the solution and work out the specific ways of delivering, but we hadn't come up with our requirements well enough. And so then you're at the mercy of industry to deliver whatever solution. And so our regrouping and our time has mostly been focused on the requirements.

The current program, TASC, that is being overseen by leadership in significant detail. The RFP is out on the street. There will be another acquisition review board this calendar year to look at the next date.

I'll have to get back to you on life-cycle cost estimate, but it's a multibillion-dollar program if executed throughout the Department. But it does allow for a more staggered approach so that we really balance risk. So it is really a total revision of the approach to financial system management.

Ms. WATSON. Yes. Mr. Hite, please.

Mr. HITE. Just a quick thought on that. We have ongoing work looking at the TASC program for the House Homeland Security Committee and for the House Appropriations Committee. I believe it is scheduled to be issued this fall, so it is coming to a conclusion. And what it's doing is looking at the six recommendations that we had made relative to moving forward on the son of eMerge2. And so we will be able to speak to what the Department is doing relative to defining a strategy for the program, developing a concept of operations, putting in place the means by which the processes—by which they're going to manage it, etc.

Ms. WATSON. I'm just going to throw out some of the other programs, too, and you can just across the board just comment on them. The Automated Commercial Environment Program, and it did not meet its cost schedule or commitments, and the costs went up. And then another program, Rescue 21, is plagued by cost overruns and so on. So can you comment on what happened with those?

Ms. DUKE. Before I comment, I would also offer to brief you or your staff on specific programs at their convenience so they can get a—

Ms. WATSON. And I just want you to know we're holding these hearings so we can fix what went wrong and how—we're putting together this humongous DHS. We want to get it right. So what we want to find out is how we—and I don't think it has been mentioned—do it through legislation. We just hope that the leadership in the various agencies and departments will be able to improve.

Ms. DUKE. Automated commercial environment, ACE, we just held an acquisition review of that. Probably the fundamental or baseline problem of ACE has been evolving requirements. It's a

major system, and we keep finding new ways to work with the shippers. And so that is OK, it's OK for a program to evolve over time. What we're trying to do now is be more disciplined about making the cost schedule tradeoffs rather than just adding requirements. And so right now we're in a period where we're having ACE reassess its requirements, its cost estimate and its program metrics before proceeding forth with any of the planned enhancements.

In Rescue 21, one of the fundamental problems with the initial part of Rescue 21 is there were some COTS solutions, as this committee has talked about, to the control system, and the initial way we moved forward with Rescue 21 was to develop a unique developmental control system. And so one of the things we've learned on Rescue 21 to get that back on track is we've gone away from that developmental system similar to the approach we talked about on SBInet. And that change in strategy, which I think is good for the program in the long run to have a commercial system, did cause some cost increases.

Ms. WATSON. And I would like to have GAO comment on the SBInet and where you see it.

Mr. HITE. It was about 8, 10 months ago we reported on where SBInet was at that time. And our message then, it was unclear what was going to be delivered by when, at what cost, to what locations. It was constantly shifting. What it was going to be was shrinking without becoming more specific. When it was going to be delivered was moving further out to right on the timeline, and the costs were a veritable unknown at that time.

In addition to that, there were issues surrounding the ambiguity of the requirements. If you have unclear requirements, it is a recipe for failure, because what you'll learn over time is it is very difficult to design and develop a system to a requirement that's not clear. And then if you learn about those kind of things downstream after you, in fact, have developed software or integrated commercial products, and you're trying to test them to see whether they meet the requirements, it is a whole lot more expensive to fix them than it would have been at the beginning.

There were issues associated with the testing at that time. Component tests were occurring on individual parts of SBInet—or, I'm sorry, had not occurred yet. Tests were occurring on the integration of components, which is kind of out of order. So there was a range of program management weaknesses associated with it at the time, and it headed on a track for just flat out not being successful.

We raised these risks to the Department. As part of our recommendations we wanted the then IRB, Investment Review Board, now the Acquisition Review Board, to get involved and conduct oversight of it. I'm happy to say that has occurred to a considerable extent. The IRB has looked at it. The IRB as issued directives, decision directives, to the program on what it needs to do in order to bring itself back. There has been a wholesale change in that program in terms of the leadership on it. The new program director for that is an exceptionally qualified individual.

So I think we're moving in the right direction there. We have ongoing work looking at the extent to which the very specific program weaknesses that we identified in terms of being able to put together a good estimate of what it is going to cost, a good schedule

of what's going to get done when, and to do good requirements, management, good testing. We have work going on now for the House Homeland Security on all of those fronts. We're probably about 3 or 4 months away from reporting on that, and because of our protocols with the Congress, I can't disclose what the results of that work is right now. We will be exiting with the Department and sharing the results of that work in the next probably 30 to 60 days. And so when we're in a position to, I will be happy to share that information with the committee as well.

Ms. WATSON. Mr. Bilbray.

Mr. BILBRAY. I have no questions.

Ms. WATSON. Mr. Taylor, would you like to comment? One of the questions that is still rolling around among us is that when do we pull the plug on programs with cost overruns or deficiencies beyond certain thresholds?

Mr. TAYLOR. That's an excellent question. The problem we run into in some of these programs, and you've seen it at DHS and other places, I'm sure, but at DHS we have had a problem because we don't know what the definition of what we're asking for in the first place is. We know we have an operational requirement we need to support, but we haven't defined what it is we're trying to use that application for and what we're trying to achieve.

So we keep evolving the requirement, and things change as we're going along, and the costs add up over time. You saw it with some of the other projects. You saw it with the original Pearson contract before DHS's time, the original Pearson contract with TSA to train TSA screeners. You saw it with Deepwater. You see these things evolving. We're concerned about the financial system for those kinds of reasons and other projects.

You have to require a real definition of requirements. You have to have those requirements in place so that you know what you're getting so you can measure those costs against it, and that's the biggest weakness right now.

Ms. WATSON. Mr. Connolly, is there a question or statement you'd like to make at this point? And welcome.

Mr. CONNOLLY. Thank you, Madam Chair, and thank you for holding this hearing. Forgive me for being late. I had a caucus meeting, and then I gave a 5-minute on the floor, so I'm just coming back from the floor. I do have a prepared statement I would be glad to enter into the record.

Ms. WATSON. You can submit it for the record.

Mr. CONNOLLY. And just welcome, folks, here. Obviously the whole question of the deployment of technology in our Federal Government is very critical moving forward both to this committee and certainly in my district. So I'm going to be very interested in looking at the testimony and following this issue, and I again thank you for holding this hearing.

Ms. WATSON. Thank you.

Let us now conclude with Ms. Duke. You've heard the input from not only questions we asked, but from the GAO and the IG. What would your overall view be of the progress we've made at DHS? And where do we have to go? You only have an hour to tell us.

Ms. DUKE. I think my assessment of the progress varies from day to day. I think when we look at the limited resources we've had,

the challenges we faced, I'm very proud and amazed at the progress we made.

Ms. WATSON. Let me just say this: This new administration has been accused of growing government, and I really don't know what that means, because here is a prime example of why we want to grow government for homeland security. It just makes sense to me. I come from Los Angeles, and you really need to get there 2 hours in advance because you've got to go through security. And I look back at the line, just to get up to the sensors, there must have been 300 people in three lines side by side, and we were there very early. We get the 7:40 flight out.

And so I'm saying you should upload the first team at each one of the security gates so that you can process these people for their flights. They had to come through and say, is anyone leaving on the 7:05 a.m. flight? And we stood there long enough for the crew to change. Then it went faster.

I said, if you got all these people in line, then we ought to put the security force—really double it on the early morning flights. And these are the things that have to work down through the system. We're talking about investments for the most part.

But there are a lot of things that need to be done to make this a true working Department that secures our homeland. So we're not trying to throw all of this and get questions for you at one time. Where do we need to go? And that might have been minor, my experiences, but we do it every single week. And I'm saying by now, we should have figured this out. So I understand it takes time, it takes money, and when we talk about growing government, we have to be sure that we use taxpayers' dollars wisely.

So we want you to tell us how to use those dollars wisely.

Ms. DUKE. One of the things we're working on is rightsizing our work force and the balance between Federal and contractor employees. Our Senate Homeland Security Committee, this was a bipartisan issue since the last Congress, and we've identified positions in DHS that would be more appropriately done by Federal employees. That's going to be huge in delivering the mission effectively. And it's not big government, it's doing the right thing and having our core capabilities done by Federal employees.

I think the thing we have to do in acquisition and management is sustain the discipline and the tenacity to go through this. What we learn as children is that decisions have consequences, and we have to be good and disciplined after we put the fundamentals in place about making the cost schedule and performance tradeoffs so that we have a disciplined approach, and if it means slowing down a program, then that is the right decision, and that we have the ability and the data to stand up and say we're purposely slowing it down or whatever, we're doing it to make the right decision.

I think that we have the building blocks in place, and I think we have a great Federal work force in at DHS. I was a career Fed for 26 years before my appointment, and we have some of the finest people. And I think we have the people to do it. We have the leadership in place that will support them. And I think that we do have the oversight of our committees that help, because it helps us keep the focus on it.

So my personal opinion after being in the Department is the building blocks are in place, and the proof is in, as both GAO and the IG have said, in the doing and the discipline to keep it up, and have the discipline to make the hard decisions when they need to be made.

Ms. WATSON. We're going to send out to you the questions that were raised by Mr. Cuellar, and we would appreciate the answers. And if any other members of the committee would like to have any concerns or questions answered, we will send them out to you.

Yes, Mr. Connolly.

Mr. CONNOLLY. Madam Chairman, we will, with your consent, submit some written questions for the record.

Can I add one little thing since you're describing your experience at LAX?

Ms. WATSON. Please do.

Mr. CONNOLLY. I would just plead with DHS, it may seem like a small thing, but every time I've traveled, I've been impressed with sort of an unevenness about the training of handling the public by security personnel. It's just as easy, maybe even easier, to get compliance with hard-pressed travelers waiting in long lines, understanding that security is an issue, when there is a "please" affixed to the request. I've been stunned at how many airports I go through where TSA folks act in ways that are profoundly disrespectful to the public, where they were barking orders and making demands, and it is, frankly, just lack of training. And the public is not the adversary. The public is, in fact, just as much concerned about security as TSA and wants to be cooperative. But it makes it a little harder, and gets people's back up, and creates needless stress when, frankly, we don't treat the public with the respect they deserve. We're serving that public.

And so I would plead with the DHS, it may seem like a little thing, but I don't think it is. I think if you want the public's full cooperation, support and sympathy for the mission, then treat them with the respect they deserve. And I would plead with you to start to try to have that ethos better imbued in the training programs and in the mentality of some of the folks who serve the public. Some are great and try to use good humor and treat people with respect. But all too many do not. And this is the United States of America. The public is in charge.

Thank you, Madam Chair.

Ms. WATSON. I have to followup on that, too, because that's what I was referring to. The TSA has to do a better job in selecting the people that work at first contact. You go, you get your ticket, and then you get in that line. So they really are the first contact, as far as I'm concerned.

They yell continuously at people, rather than saying, "Take your shoes off and place them on the belt." That's what we have to do in L.A. Here you can put them in the bin. And it changes every airport you go in, and I can understand that.

But you really need to treat the public a little differently than we get treated. We travel twice a week, 5 hours and 15 minutes for me. And I said to them yesterday, you know, I'm going to see what we can do about making the process more useful and smoother and not as antagonistic as it appears to be. That really irks me,

someone who flies all the time. That's minor, but it means a lot to the passengers.

And one of the things that annoys me is the personal conversation among the employees when there could be someone there who really needs to be checked out. And I don't need to hear about what you did last night, and your personal problems, and who is saying what, and that's the conversation you have to stand and listen to.

So we need more focus. We need more, shall I say, accuracy, and we need more detection. And not everyone is an intended terrorist, but that's the way we're treated. However, that is rather minor, but it is an important issue to start thinking about.

I want to say to the panel that we appreciate your input, and this is a hearing to gather information to make this particular service to the people, DHS, the best ever, because you've heard the complaints out there in the streets. And it's like we're the biggest, shall I say, interfering Big Brother into people's business. We're growing government, and we're endangering people's future, their children, their grandchildren, their great-grandchildren. We're destroying our Nation. That is not our intent. Our intent is to build the Department of Homeland Security to be the best in the world and to protect our country, and that's the reason why we're holding these hearings.

I appreciate your input. And just know we're here to get the information that you need. And if we have to do it through policy, we'll do it that way. But I think these hearings will help us to give the information out to you and let you handle it the best way. And I know we're driving the CIO crazy, but we appreciate your feedback to us so we can manage the public's dollars better and have better results.

And with that, if there are no more questions, then we will adjourn this meeting, and thank you so much.

The meeting is adjourned.

[Whereupon, at 11:25 p.m., the subcommittee was adjourned.]

