DHS INFORMATION TECHNOLOGY: HOW EFFECTIVELY HAS DHS HARNESSED IT TO SECURE OUR BORDERS AND UPHOLD IMMIGRATION LAWS?

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MARCH 19, 2013

Serial No. 113–7

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

82–581 PDF WASHINGTON : 2013

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

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
KEITH J. ROTHFUS, Pennsylvania
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
YVETTE D. CLARKE, New York
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
RON BARBER, Arizona
DONDALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
ERIC SWALWELL, California

GREG HILL, *Chief of Staff*
MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

JEFF DUNCAN, South Carolina, *Chairman*

PAUL C. BROUN, Georgia
KEITH J. ROTHFUS, Pennsylvania
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
MICHAEL T. MCCAUL, Texas *(Ex Officio)*
RON BARBER, Arizona
DONALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

RYAN CONSAUL, *Staff Director*
DEBORAH JORDAN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Staff Director*

CONTENTS

DHS INFORMATION TECHNOLOGY: HOW EFFECTIVELY HAS DHS HARNESSED IT TO SECURE OUR BORDERS AND UPHOLD IMMIGRATION LAWS?

Tuesday, March 19, 2013

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:00 p.m., in Room 311, Cannon House Office Building, Hon. Jeff Duncan [Chairman of the subcommittee] presiding.

Present: Representatives Duncan, McCaul, Broun, Rothfus, Hudson, Daines, Barber, Thompson, Payne, and O'Rourke.

Mr. DUNCAN. The Committee on Homeland Security Subcommittee on Oversight and Management Efficiency will come to order. The purpose of this hearing is to closely examine the Department's critical information technology systems and their daily operations protecting the Nation's borders, preventing terrorists from entering the United States, and facilitating the legitimate flow of people and trade.

Before I begin my opening statement I would like to express the subcommittee's frustration with the DHS over not providing its written testimony on time. This is unfair to the Members and other witnesses. We expect the Department to provide their written statement in accordance with the committee rules moving forward.

I and other subcommittee Members are also disappointed that DHS's chief information officer, Mr. Richard Spires, was unable to testify today on these important issues. Mr. Spires has been outspoken in improving IT within DHS and ensuring transparency and meaningful oversight. We look forward to hearing from him on these issues at a future date.

Now I recognize myself for an opening statement. Before I do, I will mention that we do have votes at 2:15, so we are going to try to get through as much as we can before Members are required to leave.

The component agencies that make up the Department of Homeland Security rely heavily on information technology, or IT, to perform a wide range of missions. IT is especially important with regard to border security and immigration enforcement.

With one of the Federal Government's largest information technology budgets, DHS's component agencies such as Customs and

Border Protection, Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services rely on critical IT systems and their daily operations to protect the Nation's borders and prevent terrorists from entering the United States, and facilitate the legitimate flow of people and trade into and out of our country.

Having been down on the border at our ports of entry, I recognize the integral role IT infrastructure plays in the ability of ICE and CBP agents to carry out their missions. In fiscal year 2012 the Department of Homeland Security planned to spend nearly $5.6 billion in IT investments, $1.7 billion of which is for programs the Department considers to be major investments in CBP, ICE, and USCIS.

A few of the examples of these mission-critical programs related to border security and immigration enforcement include CBP's automated commercial environment and international trade data system, which will replace existing technology and increase efficiencies by serving as a central data collection system for Federal agencies needing access to international trade data in a secure, paper-free Web environment.

Similarly, both CBP and ICE are working on the respective portions of the Traveler Enforcement Compliance System, or TECS Modernization program, which will be an important upgrade to a legacy system developed in the 1980s by the U.S. Customs Service to support inspections and investigations. A similar effort is ICE's Detention and Removal Operations Modernization, which will significantly upgrade IT capabilities to support the efficient detention and removal of aliens who are in the custody of ICE.

Given the size of the Department's investment in IT, effective management and oversight of IT programs and expenditures is critical to ensure DHS is using taxpayer money efficiently and holding programs accountable for agreed-upon deliverables. Despite some successes by the Department and data center in network consolidation, as well as cloud-based service offerings and establishing IT centers of excellence, GAO and DHS Inspector General have identified numerous cases where the Department has yet to reduce cost and duplication through technology-based integration and modernization.

GAO reported in September 2012 that DHS's 68 major IT investments, roughly one-third, had not fully met their cost or scheduled targets. These delays can mean border agents will have to make due with legacy IT systems for longer periods. Similarly, the DHS Office of Inspector General has identified information technology management as a major challenge facing the Department, including attempts to create a unified information technology infrastructure for effective integration and agency-wide management of information technology assets and programs.

At the component level, the DHS Inspector General identified aging IT infrastructure, interoperability, and functionality at the CBP as specific challenges creating an environment difficult to support CBP's responsibility to secure the border. For instance, the IG reported that in some instances Border Patrol staff cannot communicate seamlessly from analog to digital platforms with Federal, State, and local partners in all sections of the country.

I personally find it alarming that after a decade after the Department was stood up and billions of dollars poured into securing our borders, preventing another September 11, that CBP staff in one location might not be able to reliably share information not only with local law enforcement officers, but also with other agencies within the DHS apparatus.

Similarly, a November 2011 DHS IG report details struggles by USCIS to transform its fragmented paper-based business process to a flexible, efficient, and electronic adjudication service. However, this transformation has yet to be fully implemented because of delays in strategy and system requirements, which ended up costing American taxpayers hundreds of millions of dollars. As a result, USCIS missed an opportunity to process immigration benefits more efficiently, combat identify fraud, and share critical information necessary to quickly identify criminals and possible terrorists.

I am happy to welcome our witnesses to the hearing today and look forward to hearing about the steps taken by the Department to develop an agile approach to IG development at these critical agencies and progress in eliminating duplication, consolidating existing technology, and improving the overall management of those IT projects of CBP, ICE, and USCIS, which will enhance DHS's mission of securing the border while upholding immigration laws.

It is absolutely critical that in a time of financial belt-tightening, particularly as the Congress begins to look at addressing the issue of comprehensive immigration reform, the DHS be able to meet IT investments and capabilities on time and on budget without posing a risk to the Department's ability to fulfill its mission of securing homeland.

I will just note that the total cost for the IT systems was projected at—I am turning to the number here, $5.6 billion. The complete St. Elizabeths site that we visited last Friday is budgeted at $4 billion. So, the IT systems is a billion—a little over a billion and a half more than the complete St. Elizabeths site. That is alarming to me at the cost. So I wanted to bring that up.

The Chairman will now recognize the Ranking Minority Member of the subcommittee, the gentleman from Arizona, Mr. Barber, for any opening statement he may have.

Mr. BARBER. Well, thank you, Mr. Chairman.

Thank you to the witnesses for being with us today.

Each year the Department of Homeland Security spends approximately 15 percent of its total budget on information technology systems. As the Chairman noted, in 2012 this was approximately $6 billion. Given the significance of this investment, it is critical that we are holding this hearing today in an effort to carry out our oversight functions and responsibilities for these very costly systems.

While the GAO and the Department of Homeland Security Officer of the Inspector General have generally found that most of the major IT investments by the Department are sound and are providing DHS the necessary tools to carry out its mission, it is clear that several IT projects are not going as promised. This is especially true of the technologies that have been used or attempted to be used to secure the border.

In my home district in southern Arizona, I have seen first-hand the extreme waste of taxpayer money on programs like SBInet, a

program that was designed without input from the people on the ground who know what is best in that community in that area. It seemed promising at the time. Yet at the ultimate cost of over $1.5 billion there has been little or no return on our investment. To my dismay, I would have to say the SBI successor, according to the GAO, the Arizona Border Technology Plan, appears to face similar challenges as SBInet and looks like it might be more of the same.

These are two examples that show that the Department must do more to improve its IT structure, governance, and the manner in which it develops IT systems. Hopefully recent changes to how IT decisions are made at the Department and managed will yield better results and budgetary savings, especially as it relates to border security.

Twenty-four hours a day, 365 days a year, as you know, the men and women of the Customs and Border Patrol and Immigration and Customs Enforcement put their lives on the line in very rugged environments to secure our borders and to prevent illegal trafficking and smuggling from across the line. If there are technology-based solutions that can help them fulfill their mission, it is essential that the Department and Congress provide them with those resources.

However, we must ensure that the technology we deploy is proven, is cost-effective, trustworthy, and meets the needs of those on the front line. I will repeat that when the implemented SBInet contract specifically prohibited the contractor from talking to agents on the ground, that can't happen again.

We must ask the end-user, No. 1, is this technology that is needed? No. 2, is this technology that would actually work in a border environment? When developing new IT systems I encourage the Department to utilize the services of its own Science and Technology Directorate in addition to leveraging the skills and knowledge that can be found in our Nation's universities.

In 2008 the University of Arizona became the co-lead of a research university team that have partnered to form the Center for Excellence of Border Security and Immigration. This partnership has yielded numerous successful endeavors that can stem the flow of drugs across the Southwest Border, aiding and protecting deception and malicious intent by those seeking to enter the United States and improve the effectiveness of our checkpoints.

As we seek to improve and harness new border-related IT systems, I urge the Department to continue to utilize the University of Arizona Center of Excellence and also engage ranchers and those living along the border and the working agents who work the border for first-hand information accounts of what works and what doesn't work.

I want to echo here the Chairman's comments about telecommunications. It became painfully clear to me in 2010 when I was district director to Congresswoman Giffords that we have a long way to go to ensure that the agents can communicate with each other and other law enforcement departments. The death of Rob Prince during that time was an example of how poor the telecommunications is, and I fear they may be not much better today.

I will encourage the Department to engage with Boeing and others who have worked on projects to secure the border in what has

worked and what has not. In closing, let me just say this: That while the use of technology to secure our border is needed and a sign of the times, nothing can replace actual boots on the ground.

You know I am very concerned, even though it is not the subject of our hearing today, that as a result of the budget sequestration issue we are now going to see less overtime, less time on the job for Border Patrol agents, the people who actually secure our border day-in and day-out. We have to make sure that we do not allow the progress we have made to be degraded by these budget cuts. As we evaluate technology on the border, which comes at a high financial cost, I would caution us to ensure that the Department is not exceeding IT cost estimates at the risk of putting Border Patrol agents out of work.

Thank you, Mr. Chairman. I yield back.

Mr. DUNCAN. Thank the Ranking Member. The other Members of the subcommittee are reminded that opening statements may be submitted for the record.

We are pleased to have a very distinguished panel of witnesses before us today on this important topic. What I will do is I will introduce each witness and then we will recognize you.

The first witness is Ms. Margie Graves. She is the deputy chief information officer for the Department of Homeland Security. In this capacity, Ms. Graves oversees the Department's IT portfolio of about $6 billion in IT programs.

Ms. Graves manages the operation of the Office of Chief Information Officer, which covers functional areas of applied technology enterprise, architecture, data management, IT, security infrastructure, operations, IT accessibility, budget, and acquisition. Prior to her selection as deputy CIO in 2008, Ms. Graves held numerous senior IT positions in the Department. Ms. Graves also has 20 years' experience in the management consulting industry.

Mr. David Powner—am I pronouncing that right, Powner? Okay—is the director of information technology, IT management issues at the Government Accountability Office or GAO. At GAO, Mr. Powner's work focuses on system development and acquisition, IT governance, IT reform initiatives and major IT modernization efforts. He also has led work on cyber critical infrastructure protection. During his time in the private sector, Mr. Powner held several executive-level positions in the telecommunications industry.

Mr. Charles Edwards is the deputy inspector general of the Department of Homeland Security. Mr. Edwards is the head of the Office of Inspector General, a role he first obtained when named acting inspector general in February 2011. Mr. Edwards has over 20 years' experience in the Federal Government, and has held leadership positions at several Federal agencies including TSA, the United States Postal Service's Office of Inspector General, and the United States Postal Service.

So, I thank all of you for being here today. The Chairman will now recognize Ms. Graves to testify.

STATEMENT OF MARGARET H. GRAVES, DEPUTY CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. GRAVES. Chairman Duncan, Ranking Member Barber, and Members of the subcommittee, thank you, and good afternoon. As deputy CIO at DHS I oversee an IT portfolio $5.4 billion in programs and manage OCIO operations. This has given me valuable insight and perspective to share with you on the efforts that we are making at DHS to ensure effective delivery of IT programs to support the missions of DHS.

When the DHS OCIO evaluates the health of an IT program we focus primarily on three areas.

The first area is whether a program has correct management structure and skilled and experienced individuals to fill key program management roles. It is critical to ensure that every large IT program has a qualified program manager or PMO, and additional core positions based on its level of complexity. The skills and experience of the staff and the PMO are the most heavily-weighted criteria in how we evaluate our IT programs.

The second area is proper alignment of key stakeholders and oversight to help address issues that may arise. Even the best program manager will have challenges if the governance model does not effectively support and provide guidance to the program.

Within DHS we have implemented a three-tiered governance structure. At the enterprise level we have a governance board known as the Acquisitions Review Board or ARB, which adjudicates major acquisitions decisions. In addition, portfolio steering committees and executive steering committees, or ESCs are chartered by the ARB and provide program governance.

The third and final area is whether a program is leveraging program, project, and technical best practices to minimize program risk and therefore maximize its chance for success. Within DHS we are implementing such a model under which we call our acquisition and program management Centers of Excellence. These Centers of Excellence provide a number of services to programs, including sharing best practices and materials, training programs and mentoring, and expert in subject matter support.

DHS IT programs are now governed by these principles. As examples I would like to highlight four of our programs.

First example is CBP's Automated Commercial Environment or ACE, which is modernizing how CBP secures U.S. borders, speeds the flow of legitimate shipments and targets illicit goods. In 2010 the program was placed on OMB's list of troubled Federal IT projects.

Since that time the PMO addressed skill gaps and embedded business expertise. The governance model has been strengthened, and the program has worked closely with a number of COEs to gain expertise. Strong program governance and organizational changes, active stakeholder engagement and support, and implementing agile development and sound funding strategies have placed the program on the right course.

My second example is CBP's TECS Modernization which is a key border enforcement system supporting the screening of travelers entering the United States and the screening requirements at other

Federal agencies that use the information for law enforcement and benefit purposes. TECS Mod, which is modernized incrementally with five projects that focus on major functional areas, and is on a schedule to be complete by the end of fiscal year 2015.

The third program I would like to highlight is CIS's Electronic Immigration System or ELIS. The program was put in place to transition the agency from a fragmented, paper-based operational environment to an integrated, paperless, electronic environment. Unfortunately there were difficulties on the first release.

But under the direction of the ARB we set up an ESC to oversee the program, participate in test stat review in conjunction with the Federal CIO, created a life-cycle cost estimate and an integrated master schedule, and facilitated the program's migration to DHS provided cloud services. Since then, CIS successfully developed the technology architecture to better support agile development and has delivered two additional ELIS projection release, which should enable CIS to stay within estimated cost and schedule.

The final program I would like to highlight is ICE's Detention and Removal Operations Modernization or DROM. It was initiated in late 2006 to improve the operational effectiveness of enforcement and removal operations, or ERO, and to strengthen the alignment of the ERO mission with the Secured Border Initiative. Despite technical and operational challenges, DROM is targeted to move into full sustainment by fiscal year 2014, providing full operational capability while coming in under budget.

At DHS we are working hard to mature our ability to deliver new capabilities by improving the skills of our staff to manage programs, effectively overseeing these programs and harnessing the best practices in how we run those programs, ultimately increasing our ability to support the homeland security enterprise. Thank you. I am pleased to address your questions.

[The prepared statement of Ms. Graves follows:]

PREPARED STATEMENT OF MARGARET H. GRAVES

MARCH 19, 2013

Chairman Duncan, Ranking Member Barber, and Members of the subcommittee, thank you and good afternoon. Today I will discuss efforts we are making at headquarters and across the components at the Department of Homeland Security (DHS) to ensure effective delivery of IT programs to support the missions of DHS. My experience in public-sector large-scale IT organizations has given me unique insight in how to effectively leverage IT to support the mission and business needs of a large organization.

I will first describe what DHS is doing as an enterprise to support delivery of mission capabilities, with particular emphasis on how we are working to systemically improve our acquisition and program management capabilities to ensure successful delivery of programs. Second, I will highlight four major programs that support our border security and immigration missions, namely the United States Custom and Border Protection's (CBP) TECS Modernization, CBP's Automated Commercial Environment (ACE), U.S. Citizenship and Immigration Service's (USCIS) Transformation, and U.S. Immigration and Custom Enforcement's (ICE) Detention and Removal Operations Modernization (DROM).

IMPROVING DHS'S ABILITY TO DELIVER SUCCESSFUL IT PROGRAMS

When I evaluate the health of an IT program, I focus on three areas: Whether a program has the correct management structure and the proper set of skilled and experienced individuals to fill key program management roles; proper alignment of key stakeholders and oversight to help address issues that may arise; and whether the program is leveraging program, project, and technical best practices to minimize

program risk and therefore maximize its chance for success. It is important to note during this period of fiscal austerity that all three contribute directly to a program's ability to deliver as efficiently and cost-effectively as possible. Below I provide more detail on each of these three key areas, with particular focus on how DHS is, as an enterprise, working to mature our institutional capability in each.

Program Management Structure, Skills, and Experience

Programs are not successful when they lack experience and skills in critical program management positions or a solid program management office (PMO). For large, complex IT programs, having a program manager (PM) who has successfully managed and delivered numerous IT programs is vital.

Large, complex IT programs vary greatly, so there is not one model that fits every program. While every program should have a qualified program manager, additional positions vary based on its complexity and should be considered on a case-by-case basis. The following positions, however, are typically core, and programs lacking solid individuals filling these positions at higher risk: Systems architect; data architect; requirements manager; development and integration manager; test manager; configuration manager; operations manager; contracting officer; and contracting officer's representative.

In addition to the above core positions, when organizations embark on large IT programs, it is critical to ensure the right business or mission owner involvement. It is necessary to have full-time representatives of the business who can not only successfully work within the program to define requirements of the system, but also help the PMO make the trade-off decisions that are a constant in a program. In assessing a program, I look for individuals who are steeped in the current process end-to-end, who have true credibility with senior management, and who demonstrate flexibility to deal with unending change as a program unfolds and matures. While we often need strong contractor teams to help execute large complex programs, successful PMOs are staffed with strong Government staff who can provide the leadership and oversight necessary to direct the work. It is essential that each program find the approximate mix of Federal and contractor personnel to staff their PMO and ensure the PMO is fully integrated.

DHS is taking aggressive steps to ensure that we can properly staff our major IT programs with skilled and experienced personnel. We have a number of training programs, most notably a PM certification course. In addition to a standard PM certification, we have additional specialty courses for PMs that run IT programs. Further, we have course tracks in other key skill areas as outlined above, to include requirements engineering, systems engineering, and test and evaluation methodologies. Finally, we have built into our program evaluation criteria the recognition that the PMO is key to success. The skills and experience of the staff in the PMO is the most heavily-weighted criteria in how we evaluate our IT programs.

Program Governance

Even the best program manager will have challenges if the governance model does not work. Governance drives alignment amongst key decision makers in an organization. We have heard for decades that IT programs fail because of ill-defined requirements or poorly-managed requirements scope throughout the life cycle of a program. While true, this is a symptom of a more fundamental underlying cause: The inability for all key stakeholders in a program to be "on the same page" in defining desired outcomes and approaches to meet those outcomes.

Change is inevitable in all IT programs, so achieving such alignment is not a one-time event occurring at the start of a program. Alignment is an on-going process that is critical throughout an investment's strategic planning, design, and development, as well as its implementation; hence, governance must be viewed as a full life-cycle process. Sometimes the change is significant, making on-going alignment even more crucial to successfully driving the promised Return on Investment (ROI) and ensuring accountability. Further, for complex IT systems, there are at least a half-dozen stakeholder organizations that must be aligned, to include the strategy organization, business or mission owner of the system, IT, finance, procurement, security, and privacy. Ensuring all key stakeholders are involved in key decisions is an essential element to assuring genuine alignment.

Based on my experience, establishing a strong, active program governance board is required to ensure such alignment. Program governance boards provide guidance, decision making, and oversight of one or more programs. The function of the program governance board is not to usurp the authorities of the PM, but rather to provide a forum by which the PM can bring key issues and trade-off decisions to an informed, empowered body that has a vested interest in that program's success and that views the PM as a trusted advisor and true subject-matter specialist. In today's

environment of more modular and agile development, a program in design or development should have a program governance board that meets no less than monthly, and in some cases weekly, depending on the type of program and life-cycle stage of the investment. Not only does an active program governance board support accountability, it also fosters transparency.

Within DHS, we have developed a management directive and are maturing our program governance processes. At the enterprise level, we have a governance board known as the Acquisition Review Board (ARB), chaired by the DHS Under Secretary for Management and with all the DHS Lines-of-Business as members, which has ultimate authority over all DHS programs. DHS has embarked on a tiered governance model in which Executive Steering Committees (ESCs) are chartered by the ARB to provide governance of a program or related set of programs. While not fully implemented across all programs, the ESC structure is chartered for programs rated at higher risk. Of the 88 major IT programs, my office (DHS Office of the Chief Information Officer or OCIO), working with the DHS Program Accountability and Risk Management Office (PARM), has identified 16 programs that would immediately benefit from the governance model of an ESC. I am pleased to write that all 16 of those programs now have the oversight of an ESC. Further, I am personally involved or have a senior representative from my office as a member of each of these ESCs.

In addition to the tiered governance model, DHS OCIO partners with PARM to monitor all major programs based on monthly status reporting from each program. If a major IT program is showing negative indicators in monthly reporting, we will hold a Techstat on the program, which is a program review to identify the issues affecting the program along with a set of remediation actions to address the issues. Within the last 2 weeks, a Techstat on one program resulted in 11 remediation actions, to include the establishment of an ESC for the program.

IT Program and Technical Best Practices

Even with a solid PMO and proper governance, it is critical that IT programs leverage the practices and tools that are appropriate for the work at hand. Using the proper methods to capture requirements, complete a systems design, implement a configuration management process, and properly test the system are just a handful of the myriad practices that must be implemented in a large IT program. Even a skilled and experienced set of individuals cannot be expected to deeply understand current best practices in all areas, so it can be greatly beneficial for programs to acquire guidance and help from subject matter experts in varied disciplines that cross the program, project, and technical disciplines.

Within DHS, we are implementing such a model under what we call our Acquisition and Program Management Centers of Excellence (A&PM COEs). The COEs provide a number of services to programs to include: (1) Development or adoption of proven practices, guidance, document templates, and examples; (2) support program management workforce development through development of training programs and mentoring; (3) expert support (support the stand-up of new programs; support program reviews; and provide subject matter expertise for programs that have skills gaps or are struggling; (4) identification and development of enterprise tools to enable more effective program management; and (5) identification of program health criteria that recognizes what program success looks like.

To date, DHS has established eight COEs to support programs, including COEs for program management (to include schedule and risk management as well as life-cycle logistics), cost estimating and analysis, enterprise architecture, systems engineering, requirements engineering, test and evaluation, privacy, and accessibility. A key to making this work is to draw from expertise across DHS, so individuals from each component can participate in their particular area of expertise. Through this federation, we work to create communities of practice bringing ideas from across DHS that strengthen the work of each COE. While we have made significant progress in establishing COEs, we continue to work on maturing our efforts, and plan to review the need for additional COEs in years to come.

KEY DHS PROGRAMS SUPPORTING BORDER SECURITY AND IMMIGRATION

The remainder of the testimony highlights a number of key IT programs, both in terms of how they support DHS missions in border security and immigration, and how we are leveraging the work outlined above to improve the delivery of these major IT programs.

CBP—Automated Commercial Environment (ACE)

ACE is a multi-year program with sunk costs of $3.2 billion to modernize the business processes essential to securing U.S. borders, speeding the flow of legitimate

shipments, and targeting illicit goods. ACE modernizes and enhances trade processes and forms the backbone for the "single window" through which the international trade community will electronically provide all information needed by Federal agencies for the import and export of cargo. The ACE program is essential to improving the ability of CBP's agents and officers and those of 47 Partner Government Agencies (PGAs) to assess cargo for security, health, and safety risks, while speeding the flow of legitimate trade and ensuring compliance with U.S. trade laws.

Cost and Schedule Performance

In 2010, the program was placed on the Office of Management and Budget's (OMB) list of 26 troubled Federal IT projects. In addition, the DHS ARB placed ACE on a pause status while the program worked to address its issues. Since that time, CBP, with the support of DHS and OMB, has worked aggressively to turn the program around. While parts of ACE are in operations and maintenance, much functionality remains to be developed. Therefore, working with DHS, CBP has developed a plan for the completion of core trade processing capabilities in ACE and decommissioning the legacy system within approximately 3 years. A key component of this plan is the implementation of an agile software development methodology which focuses on the production of smaller pieces of functionality more frequently, resulting in a more flexible user-focused development process. CBP's plan addresses the priorities identified by internal system users as well as key trade community and PGA stakeholders: Cargo release, entry summary edits, and exports.

With respect to the program's funding strategy, CBP has made great progress in reducing ACE Operations and Maintenance (O&M) costs and identifying internal sources of CBP funds to support remaining ACE development and migration.

Challenges

CBP has addressed a number of basic organizational and governance challenges as it administered the ACE program. Based on direction from the ARB and with DHS's support, CBP responded with program changes as documented in the ACE Improvement Plan submitted to OMB. Specifically, CBP has:

- Established an ACE Business Office in the Office of International Trade to better define business needs through an enhanced business requirements process.
- Increased stakeholder engagement through the establishment of an Executive Steering Committee (ESC) that includes all levels of DHS and CBP leadership.
- Also increased engagement with all impacted CBP program offices, volunteer Government field personnel serving as ACE Ambassadors, the Trade Community, and Partner Government Agencies.
- Defined baseline needs through an enhanced business requirements process.
- Executed a new approach for the development of functionality by building in modular components that treat each piece of distinct functionality as a separate project for frequent delivery of smaller segments of functionality.
- Conducted more effective oversight of contractors through greater internal controls and governance.

Program Outlook

CBP has taken significant steps to reposition ACE for success. Skills gaps in the ACE PMO were identified and are being addressed; the PMO is working well and has embedded business expertise. As noted above, the governance model has been strengthened with the addition of an ESC chaired by the Deputy Commissioner. Finally, the program has worked closely with a number of the PM COEs to ensure best practices are being leveraged across the program. For instance, technical complexity is being reduced by transitioning the program to a simplified architecture that relies less on a large stack of complex proprietary solutions and more on a few well-proven open-source technologies. This will greatly simplify development, and allow rapid integration of the solution so that it can be quickly fielded in an incremental fashion.

The program is also embedding domain knowledge experts in the development process to help ensure frequent and timely feedback to developers as the solution is produced, greatly reducing requirements uncertainty and allowing for the program to adjust to changing requirements rapidly. The program is using a feature-based approach to manage requirements to achieve formal software releases every 6 months. This shorter and iterative release cycle is being mandated to ensure value is quickly realized by the CBP agents and officers along with other PGAs in the field on a regular recurring schedule.

The strong program governance and organizational changes, active stakeholder engagement and support, and sound funding strategy demonstrate that the program is on the right course.

CBP—TECS Modernization

TECS (no longer an acronym) is a key border enforcement system supporting the screening of travelers entering the United States and the screening requirements of other Federal agencies used for law enforcement and benefit purposes. TECS supports more than 70,000 users who represent more than 20 Federal agencies responsible for traveler processing, investigations, vetting, entry/exit, and research requirements. The TECS Modernization program is primarily focused on modernizing server infrastructure, databases, and user interfaces to sustain and improve current screening capabilities well into the future. The program also provides for highly scalable functionality that meets constantly emerging screening requirements. Some of the mission benefits of modernizing TECS include: Enhancing the capability to protect the Nation from the entry of individuals who may pose a threat to National security or public safety; ensuring the efficient flow of lawful people crossing U.S. borders; and enabling effective decision-making through improved information sharing.

The modernization of the legacy TECS system is being accomplished through two separate programs, one within CBP and the other within ICE. Each is funded and being executed separately. While both modernization programs remain focused on continued support of each agency's unique mission, each program coordinates common interests regarding planning, development, and data migration efforts.

COST AND SCHEDULE PERFORMANCE

TECS Mod began the 8-year modernization effort in 2008, and is on track to complete the project in 2015 as scheduled. TECS is being modernized incrementally with five projects that focus on major functional areas. These projects are: Secondary Inspection (SI); High Performance Primary Query and Manifest Processing (HPPQ); Travel Document and Encounter Data (TDED); Lookout Record Data and Services (LRDS); and Primary Inspection Processes (PIP).

Functionality, such as Secondary Inspection, has already been delivered and is being used successfully at ports of entry. In 2013, TECS Mod will deliver additional capabilities that were designed and developed in previous years. Operational Testing for the High Performance Primary Query, Travel Documents and Encounter Data, and the Lookout Records and Data Services Projects will begin in 2014.

PROGRAM OUTLOOK

Currently the TECS Modernization program is on schedule to complete by the end of fiscal year 2015 as detailed in the Acquisition Program Baseline. Some of the major accomplishments to date include:

- LRDS Watch List Service, which provides terrorist records to DHS, activated August 2010;
- Secondary Inspection to all Air/Sea Ports Of Entry (POEs) implemented May 2011 and deployed Secondary Inspection to two Land ports of entry (POEs) in November 2012 for operational testing;
- High Performance Primary Query (HPPQ) Service for Advance Passenger Information System activated in November 2012;
- HPPQ Initial Operation Capability (IOC) met on February 1, 2013.

USCIS—Transformation

In 2008, USCIS embarked on a program to transition the agency from a fragmented, paper-based operational environment to an integrated, paperless, electronic operational environment. The new operational environment, known as USCIS Electronic Immigration System (ELIS), enables customers to file requests for immigration benefits and USCIS officers to adjudicate those benefit requests within the same system. USCIS ELIS heavily leverages proven methods from the Government and the private sector to meet mission requirements for improved efficiency, quality, customer service, and features that support our National security. USCIS ELIS is a person-centric system that is already improving collaboration and information sharing within DHS and with other Federal agencies.

USCIS launched the first release of USCIS ELIS in May 2012. This release delivered the foundational technology components and basic end-to-end capabilities for applicants for certain benefit types using Form I–539, "Application to Extend/Change Nonimmigrant Status." This release included capabilities for on-line account set-up, electronic filing, security checks, case management, direct electronic correspondence with customers, and issuance of notices and decisions to customers. Feedback on USCIS ELIS performance from USCIS staff and customers has been positive.

Cost and Schedule Performance

The USCIS Transformation, when started in 2008, used a traditional "waterfall" approach to development and a single contractor as a lead systems integrator. The initial requirements development process took almost 2 years and development for the first release required an additional 14 months, including 7 months of testing and defect remediation. Although the initial release included much of the basic functionality to support the future development of additional benefit product lines, USCIS determined that such an approach was not sustainable in the long-term.

After the initial release in May 2012 USCIS decided to temporarily reduce the size of the contractor team while it transitioned to an agile development process and put in place improved governance mechanisms, with the intention of ramping up the program up again once these were in place. During 2012, as the program improved its agile approach, the number of agile teams was increased from three to six. The program intends to eventually scale up to 12 agile teams of approximately 10 developers and testers each, in order to reach Final Operating Capability as quickly as possible. A Life-Cycle Cost Estimate (LCCE) and a roadmap have been completed for the program.

Challenges

The difficulties in delivering the first release prompted USCIS, in collaboration with the DHS OCIO, PARM, and the Federal Chief Information Officer (CIO) to conclude that there were fundamental issues in the USCIS Transformation program management structure and skills, the role and performance of the lead systems integrator, the overall governance framework, the technical architecture of the solution, and the development approach. Under the direction of the ARB, the DHS CIO's Office worked with USCIS to set up an ESC to oversee the program, with the DHS CIO as a voting member. DHS also participated in a Techstat review of the program with the Federal CIO, worked with USCIS to create a Life-Cycle Cost Estimate (LCCE) and an Integrated Master Schedule (IMS), and facilitated the program's adoption of technical best practices by assisting it in migrating to DHS-provided cloud services.

Since late 2011, USCIS, in conjunction with my office and under the direction of the ARB, has taken significant steps to address each of its challenges, including:

- Revamped the program management office to take on more of the program's management and add needed skills.
- Modified the role of the lead systems integrator to drive improved performance.
- Modified the governance framework to include establishment of an Executive Steering Committee, chaired by the Director of USCIS.
- Create a Life-Cycle Cost Estimate (LCCE) and Integrated Master Schedule (IMS).
- Simplified the ELIS architecture to be more modular and to leverage open source software to the extent possible.
- Transitioned to modular framework, with releases delivered under an agile approach.

Program Outlook

Since May 2012, USCIS has successfully delivered one schedule two additional USCIS ELIS production releases using the agile development approach and with all planned functionality completed. The first agile release was delivered in September 2012 and the second in January 2013. These releases provided additional enhancements to I–539 functionality and technology that had been delayed in order to deploy the initial release in May 2012. The next two agile releases are scheduled for May and July 2013. Each release will add a new benefit type to USCIS ELIS.

In March 2013, USCIS completed successful development and modifications to the technology architecture that should better support agile delivery. In addition to modifying the architecture, USCIS is also transitioning away from a single large contract to a series of smaller contracts that will better support agile development and delivery. In May 2013, USCIS intends to begin agile development of the first production release under the modified architecture. After the modified architecture is completed, new capabilities will be released into USCIS ELIS approximately every 4 months. The modifications to the architecture and the new contracting approach should enable USCIS to stay within estimated costs and schedule.

ICE—Detention and Removal Operations Modernization (DROM)

The DROM Program was initiated in late 2006 to improve the operational effectiveness of Enforcement and Removal Operations (ERO), formerly Detention and Removal Operations (DRO), and to strengthen the alignment of the ERO mission with the Secure Border Initiative (SBI).

Through improved interoperability, enhanced and new capabilities, and an expansion of data exchange and sharing with its enforcement partners, DROM empowers ERO operations and field agents/officers by providing the technical tools necessary to execute ERO's primary mission of upholding U.S. immigration laws through adequate and appropriate custody management of detainees in a cost-effective manner. DROM applications produce expected business outcomes to monitor and support improvements such as:

- Reduction in the length of stay for detainees.
- Increased bed-space availability.
- Faster document processing and transmission.
- More accurate, complete, and flexible data reporting.
- Elimination of data redundancy.

With its overall primary goal of increasing the throughput of detainees from apprehension to case adjudication and removal, the DROM Program and its applications have streamlined ERO operations, resulting in significant cost and time savings. For example, the electronic Travel Documents (eTD) project has reduced the time to issue documents identifying a detainee's country of origin and authorizing his or her repatriation, from over 14 days to 8 days on average for participating countries (i.e., Dominican Republic, El Salvador, Guatemala, and Honduras). Including Mexico, participating countries account for approximately 90 percent of aliens repatriated.

The electronic Online Bonds System (eBonds), which automates the posting of surety bonds, allows ERO field personnel to process those bonds within hours instead of days. The Online Detainee Locator System (ODLS), an application highlighted in the White House's 2011 Blueprint to Immigration Reform for its ingenuity in facilitating the proposed reforms, has significantly reduced phone inquiries to field offices from family members, attorneys, and other interest parties. Finally, Operations Management Module 2 (OM2), formerly the Fugitive Case Management System (FCMS), will be integrated into the ENFORCE Alien Removal Module (EARM) before the end of fiscal year 2013. This integration will improve architecture and security compliance and provide a robust application with a more scalable and flexible design and greater operational efficiencies.

Cost and Schedule Performance

The DROM Program and its applications are expected to reach its full sustainment phase by fiscal year 2014. With an adjusted life-cycle cost estimate of roughly $320 million DROM has achieved most of its major goals, moving to full sustainment ahead of schedule, and has produced new and enhanced capabilities that improved the operational effectiveness of ERO. Additionally, DROM has supported, through data sharing, the high-priority effort to detain and remove criminal aliens.

Challenges

ERO's implementation of a new series of detention reform initiatives in 2009 required the program to restructure its schedule and re-define deliverables. The overarching key objectives remain intact; however, the reform initiatives changed the program direction, producing new capabilities and terminating specific projects.

In addition, EARM, the core module of the suite of ERO applications, has grown exponentially within a short period of time. The decision was made to use EARM as the framework and portal for all DROM applications with over 12 interfaces to internal and external Government entities. As a result of the rapid growth and redefinition, the build environment of EARM has become very large, making it harder to manage. Coding, debugging, and testing have become more complex as developers are required to understand the logic of the entire code base and the intrinsic dependencies within that logic. These challenges became more apparent during the test phase of releases, causing minor schedule shortfalls. ICE OCIO has taken the following steps to mitigate future potential schedule slippages related to these issues:

- Condense schedule to allow testing to occur in parallel with other activities.
- Early involvement of ERO users to ensure that capabilities meet their business needs.
- Daily collaboration with internal stakeholders to ensure faster resolution to unexpected technical issues.
- Prioritization of capabilities for potential de-scoping effort to meet schedule constraints.

Finally, delays of EARM 3.0 release 2 and EARM 4.0 releases for higher-priority initiatives as the data center migration consolidation and the Risk Classification Assessment (RCA) module resulted in ERO delaying deployment of existing require-

ments within those packaged releases. In honoring those requests, some re-work and schedule slippage were necessary.

Program Outlook

Despite the technical and operational challenges, DROM is targeted to move into full sustainment by fiscal year 2014, providing full operating capabilities of the DROM applications while coming in under budget based on the prior year cost estimate. In addition, the final software release is estimated to bring down the Operations and Maintenance cost by integrating most functionality into the core module, EARM, thus reducing the need to have separate operating support costs for individual applications. In summary, DROM has accomplished its mission by streamlining and executing more cost-efficient operations within ERO.

CONCLUSION

The ability for an IT organization to support its mission and business customers is highly dependent on its ability to field new capabilities that are developed in partnership with those customers. At DHS, we are working hard to mature our ability to deliver such capabilities, through improving the skills of our staff to manage programs, through effective oversight of those programs, and through harnessing of best practices in how we run those programs. We continue to drive this maturation through harnessing good work and talent across DHS, and its components, increasing our ability to support the Homeland Security Enterprise.

Thank you and I am pleased to address your questions.

Mr. DUNCAN. Thank you so much.

I apologize to the witnesses, but it is my understanding that we have been interrupted by votes. So without objection, the subcommittee is in recess as subject to the call. The Chairman of the committee will reconvene approximately 10 minutes after the conclusion of the last vote. So with that we will just adjourn subject to the call of the Chairman.

[Recess.]

Mr. DUNCAN. Committee on Oversight and Management Efficiency will come back to order. I want to thank the panelists for their patience during the votes, and the subcommittee will reconvene now. I must inform you that they are talking about another round of votes maybe 3:45-ish. So we are going to get through as much as we can.

So the Chairman will now recognize Mr. Powner to testify.

STATEMENT OF DAVID A. POWNER, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Chairman Duncan, Ranking Member Barber, and Members of the subcommittee, we appreciate the opportunity to testify on the status of DHS's major IT investments that among other things are to better secure our borders and enforce immigration laws.

Late last year we issued two key reports for the subcommittee that highlighted DHS improvements to its IT governance and the status of nearly 70 IT acquisitions. This afternoon I will provide an overview of DHS's IT spending and the importance of these investments to improve mission performance, the cost and schedule status of these investments, steps underway to improve outcomes, and recommendations moving forward.

DHS spends over $5.5 billion annually on over 350 investments. Of these, 68 are major IT acquisitions that comprise about $4 billion of the total spend. These 68 systems are essential to improving DHS missionaries like screening travelers and cargo entering the

country, monitoring our borders, and sharing information to combat terrorism.

A specific example of how these systems improve mission performance can be seen with the US–VISIT application. The portion deployed to date that includes matching fingerprints against an FBI database has resulted in thousands of individuals being denied entry and hundreds of arrests. Therefore, delivering on-time and within budget on these IT acquisitions is vitally important to securing our homeland.

Last year we reported that 47 of the 68 acquisitions were meeting cost and schedule goals; 21, or 30 percent were not. These 21 include important acquisitions that are to improve cargo screening, the detention of terrorists, and the screening of travelers.

The four acquisitions highlighted by Ms. Graves are included in our list of 21 not meeting cost and schedule goals. My written testimony highlights the specific reasons why each of these acquisitions are off-course, and these reasons include poor cost and schedule estimates, undisciplined requirements, processes, and various technical issues.

To DHS's credit, they have several important improvement initiatives that I would like to highlight. But I would like to start by acknowledging their IT leadership, both Mr. Spires and Ms. Graves. Although not here today, I would like to take the opportunity to mention that Mr. Spires, that DHS, CIO, we have worked with him both while he was at IRS and now DHS. Our Government is fortunate to have his service.

Turning to improved initiatives, DHS has corrective action plans to address their performance shortfalls, have created Centers of Excellence where program offices can seek assistance. Their new tiered governance structure follows best practices. These initial steps have resulted in a better IT acquisition performance.

For example, OMB's IT dashboard, which provides transparency on the performance of about 800 major IT investments across the Government, shows that DHS is trending in the right direction. Meaning that recently they have less projects at risk than they have had in the past.

However, despite this progress, DHS still has too many critical IT acquisitions where cost and schedule performance is not cutting it. Our report last year highlighted about a billion dollars associated with these 20 investments that are at risk. Therefore, several IT management practices still need significant improvements.

Specifically, DHS needs to have corrective action plans for all projects whose cost and schedule variances are unacceptable. DHS needs to have IT and business executives partner in aggressively overseeing their IT acquisitions by implementing more completely their new governance process.

DHS also needs to tackle the core root cause areas associated why programs are not meeting their cost and schedule commitments by utilizing and expanding on their Centers of Excellence. Also DHS needs to mature its program management disciplines, including areas like requirements management and risk management. Finally, DHS needs to approach more of these investments on a smaller, more manageable increment to deploy key functionality more quickly.

In summary, Mr. Chairman, DHS technology acquisitions play a vital role in improving the security of our homeland. Although DHS' ability to deliver on these systems is improving, there are still ways to go to ensure that this annual investment of $4 billion is yielding the near-term return our country needs.

This concludes my statement, and I would be pleased to respond to questions.

[The prepared statement of Mr. Powner follows:]

PREPARED STATEMENT OF DAVID A. POWNER

MARCH 19, 2013

GAO HIGHLIGHTS

Highlights of GAO–13–478T, a testimony before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

DHS has responsibility for the development and operation of the IT systems for the agencies and offices under its jurisdiction that are key to, among other things, securing the Nation's borders and enforcing immigration laws. DHS reported having 363 such IT investments. Of these investments, 68—with budgeted annual costs of about $4 billion—were under development and classified by DHS as a "major" investment requiring special management attention because of its mission importance.

GAO was asked to testify on the progress DHS has made and challenges it faces in meeting cost and schedule commitments for its major IT investments, including those for Customs and Border Protection, Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services. Specifically, GAO was asked to focus on its September 2012 report that determined: (1) The extent to which DHS investments are meeting their cost and schedule commitments, (2) the primary causes of any commitment shortfalls, and (3) the adequacy of DHS's efforts to address these shortfalls and their associated causes.

What GAO Recommended

In its report, GAO recommended that the Secretary of Homeland Security direct the appropriate officials to address guidance shortcomings and develop corrective actions for all major IT investment projects having cost and schedule shortfalls. In commenting on a draft of the report, DHS concurred with GAO's recommendations.

INFORMATION TECHNOLOGY.—DHS NEEDS TO ENHANCE MANAGEMENT OF MAJOR INVESTMENTS

What GAO Found

Approximately two-thirds of the Department of Homeland Security's (DHS) major IT investments were meeting their cost and schedule commitments. Specifically, out of 68 major IT investments in development, 47 were meeting cost and schedule commitments. The remaining 21—which DHS had estimated to cost about $1 billion—had one or more subsidiary projects that were not meeting cost and/or schedule commitments (i.e., they exceeded their goals by at least 10 percent, which is the level at which the Office of Management and Budget (OMB) considers projects to be at increased risk of not being able to deliver planned capabilities on time and within budget.)

The primary causes for the cost and schedule shortfalls were (in descending order of frequency):

- inaccurate preliminary cost and schedule estimates,
- technical issues in the development phase,
- changes in agency priorities,
- lack of understanding of user requirements, and
- dependencies on other investments that had schedule shortfalls.

Eight of the investments had inaccurate cost and schedule estimates. For example, DHS's Critical Infrastructure Technology investment had a project where actual costs were about 16 percent over the estimated cost, due in part to project staff not fully validating cost estimates before proceeding with the project. In addition, six investments had technical issues in the development phase that caused cost or schedule slippages. For example, DHS's Land Border Integration investment had

problems with wireless interference at certain sites during deployment of hand-held devices used for scanning license plates, which caused a project to be more than 2 months' late.

DHS often did not adequately address cost and schedule shortfalls and their causes. GAO's investment management framework calls for agencies to develop and document corrective efforts to address underperforming investments and DHS policy requires documented corrective efforts when investments experience cost or schedule variances. Although 12 of the 21 investments with shortfalls had defined and documented corrective efforts, the remaining 9 had not. Officials responsible for 3 of the 9 investments said they took corrective efforts but were unable to provide plans or any other related documentation showing such action had been taken. Officials for the other 6 investments cited criteria in DHS's policy that excluded their investments from the requirement to document corrective efforts. This practice is inconsistent with the direction of OMB guidance and related best practices that stress developing and documenting corrective efforts to address problems in such circumstances. Until DHS addresses its guidance shortcomings and ensures each of these underperforming investments has defined and documented corrective efforts, these investments are at risk of continued cost and schedule shortfalls.

Chairman Duncan, Ranking Member Barber, and Members of the subcommittee, I am pleased to be here today to discuss our past work examining the Department of Homeland Security's (DHS) progress and challenges in acquiring, developing, and managing the information technology investments and systems used by its agencies and offices, including those used by U.S. Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS). Since its creation in 2002, DHS has spent billions of dollars on IT infrastructure used to fulfill its mission to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. We recently reported [1] that, during fiscal year 2012, DHS planned to spend about $5.6 billion on approximately 363 on-going IT investments. Of these 363 investments, 68 were under development and were classified by DHS as a "major" investment [2] that required special management attention because of its importance to the Department's mission. My testimony today focuses on the key findings of that work, including: (1) The extent to which DHS investments are meeting their cost and schedule commitments, (2) the primary causes of any commitment shortfalls, and (3) the adequacy of DHS's efforts to address these shortfalls and their associated causes.

This statement is based on our report of September 2012. In that report, we discussed how each of the 68 major investments was performing against its cost and schedule commitments as reported by the Department to the Office of Management and Budget (OMB). We also reviewed project plans and related documentation and interviewed responsible DHS officials to identify the primary causes for the shortfalls and whether any corrective efforts had been developed and documented to address the shortfalls. We conducted the performance audit from October 2011 to September 2012 in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

DHS spends billions of dollars each year on IT investments to perform both mission-critical and support functions that frequently must be coordinated among components and external entities. Of the $5.6 billion that DHS planned to spend on 363 IT-related investments in fiscal year 2012, $4.4 billion was planned for the 83 the agency considers to be a major investment; namely, costly, complex, and/or mission-critical.

Of these 83 major IT investments, 68 are under development and were estimated to cost approximately $4 billion for fiscal year 2012. Examples of major investments under development that are being undertaken by DHS and its components include:

- *CBP*.—The Automated Commercial Environment/International Trade Data System is to incrementally replace existing cargo processing technology systems with a single system for land, air, rail, and sea cargo and serve as the central data collection system for Federal agencies needing access to international trade data in a secure, paper-free, web-enabled environment.

---

[1] GAO, *Information Technology: DHS Needs to Enhance Management of Cost and Schedule for Major Investments,* GAO–12–904 (Washington, DC: Sept. 2012).

[2] DHS defines a major IT investment as one with a cost of $50 million or more and is complex and/or mission-critical.

- *ICE and CBP*.—TECS Modernization is to replace the legacy mainframe system developed by the U.S. Customs Service in the 1980s to support its inspections and investigations. Following the creation of DHS, those activities were assigned to CBP and ICE, respectively. CBP and ICE are now working to modernize their respective portions of the system in a coordinated effort with separate funding and schedules. For example, ICE's portion of the investment will include modernizing the investigative case management and related support modules of the legacy system.

We have previously reported on the cost and schedule challenges associated with major DHS IT investments, such as those with CBP's Secure Border Network (SBInet) and NPPD's United States Visitor and Immigrant Status Indicator Technology (US–VISIT).[3] In these reports, we made recommendations to address these challenges and keep these investments on schedule and within cost.

DHS MET COST AND SCHEDULE COMMITMENTS FOR MOST MAJOR IT INVESTMENTS

The success of major IT investments are judged by, among other things, the extent to which they deliver promised system capabilities and mission benefits on time and within cost. Our research in best practices and extensive experience working with Federal agencies and Office of Management and Budget (OMB) guidance stress the importance of Federal IT investments meeting cost and schedule milestones.

Approximately two-thirds of DHS's IT investments met their cost and schedule commitments; the remaining one-third had at least one subsidiary project that was not meeting its commitments. Specifically, out of the 68 major investments under development, 47 were meeting their cost and schedule commitments.

The remaining 21 investments—which totaled about $1 billion as of March 2012—had one or more subsidiary projects that were not meeting cost and/or schedule commitments (i.e., they had exceeded their goals by at least 10 percent, which is the level at which OMB considers projects to be at an increased risk of not being able to deliver planned capabilities on time and within budget.) Table 1 lists the major investments with a cost and/or schedule shortfall.

Specifically, of the 21 investments with a shortfall, 5 had one or more subsidiary project with a cost shortfall, 18 had one or more project with a schedule shortfall, and 2 had a project with both a cost and schedule shortfall. These shortfalls place these investments at increased risk of not delivering promised capabilities on time and within budget, which, in turn, pose a risk to DHS's ability to fully meet its mission of securing the homeland.

[3] See, for example, GAO, *Secure Border Initiative: SBInet Expenditure Plan Needs to Better Support Oversight and Accountability,* GAO–07–309 (Washington, DC: Feb. 15, 2007); *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program,* GAO–10–340 (Washington, DC: May 5, 2010); and *Homeland Security: Key US–VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed,* GAO–10–13 (Washington, DC: Nov. 19, 2009).

Table 1: DHS Major IT Investments with Cost and Schedule Shortfalls (dollars in millions)

Component	Investment	One or more projects with a cost shortfall	One or more projects with a schedule shortfall	One or more projects with a cost and schedule shortfall	Total planned project cost[a]
CBP					
	Automated Commercial Environment/International Trade Data System		✓		$124.26
	Land Border Integration		✓		20.9
	Non-intrusive Inspection Systems Program		✓		332.3
	Northern Border, Remote Video Surveillance System		✓		8.2
	TECS Modernization		✓		43.03
DHS Office of the Chief Information Officer					
	Human Resources IT	✓			8.52
FEMA					
	Disaster Assistance Improvement Plan	✓	✓	✓	50.5
ICE					
	Detention and Removal Operations Modernization		✓		8.62
NPPD					
	Critical Infrastructure Technology and Architecture	✓			20.55
	Infrastructure Security Compliance-Chemical Security Assessment Tool	✓			72.76
	National Cybersecurity Protection System		✓		262.6
	Next Generation Networks Priority Services		✓		63.06
	US-VISIT: Arrival and Departure Information System		✓		7.18
	US-VISIT: Automated Biometric Identification System		✓		33.24
TSA					
	Air Cargo Security	✓	✓	✓	4.09
	Federal Air Marshal Service Mission Scheduling and Notification System		✓		5.43
	Hazmat Threat Assessment Program		✓		4.09
	Security Technology Integrated Program		✓		27.99
USCG					
	CG Business Intelligence		✓		.86
USCIS					
	Naturalization: CLAIMS 4		✓		2.36
USSS					
	Information Integration and Technology Transformation		✓		43.61
TOTAL	21	5	18	2	$1,144.14[b]

Source: GAO analysis of OMB's federal IT Dashboard data.

[a] These are the total planned costs of all investment projects in development as of March 8, 2012.

[b] Differences in total are rounded off.

CAUSES OF INVESTMENT COST AND SCHEDULE SHORTFALLS VARIED

The primary causes of the shortfalls in cost and schedule associated with DHS's 21 major IT investments were (in descending order of frequency): Inaccurate preliminary cost and schedule estimates, technical issues in the development phase, changes in agency priorities, lack of understanding of user requirements, and dependencies on other investments that had schedule shortfalls. A summary of these causes by investment and component are shown in table 2.

Table 2: Primary Causes of Shortfalls Experienced by Major DHS IT Investments (in descending order of frequency)

Causes		Inaccurate preliminary cost/schedule estimates	Technical issues in development phase	Changes in agency priorities	Lack of understanding of user requirements	Dependencies on other investments	Other causes
Component	Investment						
CBP	Automated Commercial Environment / International Trade Data System		✓				
	Land Border Integration		✓				
	Non-Intrusive Inspection Systems Program	✓					
	Northern Border, Remote Video Surveillance System	✓					
	TECS Modernization				✓		
DHS Office of the Chief Information Officer	Human Resources IT	✓					
FEMA	Disaster Assistance Improvement Plan	✓	✓			✓	
ICE	Detention and Removal Operations Modernization		✓		✓		
NPPD	Critical Infrastructure Technology and Architecture	✓					
	Infrastructure Security Compliance: Chemical Security Assessment Tool						✓
	National Cybersecurity Protection System	✓					
	Next Generation Networks Priority Services	✓		✓			
	US-VISIT: Arrival and Departure Information System			✓			
	US-VISIT: Automated Biometric Identification System			✓			
TSA	Air Cargo Security		✓			✓	
	Federal Air Marshal Service Mission Scheduling and Notification System						✓
	Hazmat Threat Assessment Program	✓					
	Security Technology Integrated Program		✓				
USCG	CG Business Intelligence			✓			
USCIS	Naturalization-CLAIMS 4				✓		
USSS	Information Integration and Technology Transformation					✓	
Totals		9	6	3	3	3	2

Source: GAO analysis of agency data.

In our past work on DHS's investments and related IT management processes, we have identified some of these same causes and made recommendations to strengthen management in these areas. For example, with regard to cost estimating, we reported that forming a reliable estimate of costs provides a sound basis for measuring against actual cost performance and that the lack of such a basis contributes to variances.[4] To help agencies establish such a capability, we issued a guide in March 2009[5] that was based on the practices of leading organizations. In a July

[4] GAO, *Information Technology Cost Estimation: Agencies Need to Address Significant Weaknesses in Policies and Practices,* GAO–12–629 (Washington, DC: July 2012).

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

2012 report[6] examining how well DHS is implementing these practices, we reported that the Department had weaknesses in cost estimating. Accordingly, we made recommendations to DHS to strengthen its cost estimating capabilities, and the Department has plans and efforts under way to implement our recommendations.

We have also reported[7] that developing sufficient requirements is key to effectively delivering systems on time and within budget and that DHS has experienced project delays and cost overruns resulting from initial requirements not being defined properly. To address this challenge, DHS had begun, as part of defining and implementing a new IT governance process, to establish Centers of Excellence to provide investment officials with expert assistance in requirements development and other essential IT management disciplines.[8]

ABOUT HALF OF DHS'S PROJECTS WITH SHORTFALLS DID NOT HAVE WELL-DEVELOPED CORRECTIVE EFFORTS

A variety of best practices exist to guide the successful acquisition of IT investments, including how to develop and document corrective actions for projects experiencing cost and schedule shortfalls. In particular, GAO's Information Technology Investment Management framework[9] calls for agencies to develop and document corrective efforts for underperforming projects. It also states that agencies are to ensure that, as projects develop and costs rise, the project continues to meet mission needs at the expected levels of cost and risk; if projects are not meeting expectations or if problems have arisen, agencies are to quickly take steps to address the deficiencies.

DHS developed and documented corrective efforts for 12 of the 21 major investments with a shortfall, but the remaining 9 did not have corrective efforts documented. Table 3 depicts the investments with shortfalls and whether corrective efforts had been developed and documented.

Table 3: Extent to Which DHS Had Developed and Documented Corrective Efforts for Investment Shortfalls

Adequately developed and documented corrective efforts?		Yes	No
Component	Investment		
CBP	Automated Commercial Environment / International Trade Data System	✓	
	Land Border Integration	✓	
	Non-Intrusive Inspection Systems Program	✓	
	Northern Border, Remote Video Surveillance System	✓	
	TECS Modernization	✓	
DHS Office of the Chief Information Officer, Human Resources IT			✓
FEMA	Disaster Assistance Improvement Plan	✓	
ICE	Detention and Removal Operations Modernization	✓	
NPPD	Critical Infrastructure Technology and Architecture	✓	
	Infrastructure Security Compliance: Chemical Security Assessment Tool	✓	
	National Cybersecurity Protection System		✓
	Next Generation Networks Priority Services		✓
	US-VISIT: Arrival and Departure Information System		✓
	US-VISIT: Automated Biometric Identification System		✓
TSA	Air Cargo Security		✓
	Federal Air Marshal Service Mission Scheduling and Notification System		✓
	Hazmat Threat Assessment Program	✓	
	Security Technology Integrated Program	✓	
USCG	Coast Guard Business Intelligence		✓
USCIS	Naturalization-CLAIMS 4		✓
USSS	Information Integration and Technology Transformation	✓	
Total		12	9

Source: GAO analysis of DHS data.

With regard to the investments with shortfalls, three were unable to provide us with documentation, even though project officials stated that they had developed some corrective efforts, and six did not engage in corrective efforts to address shortfalls. Of the three investments, officials from TSA's Federal Air Marshal Service

[6] GAO–12–629.

[7] GAO, *Department of Homeland Security: Assessments of Selected Complex Acquisitions,* GAO–10–588SP (Washington, DC: June 2010).

[8] GAO–12–818.

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

Mission Scheduling and Notification System investment, for example, reported that they had addressed the project's schedule shortfall—which was due, in part, to a support contractor not having adequate staffing—by performing the work within the agency instead of relying on the contractor. Further, according to TSA officials, the cost and schedule shortfalls on the Air Cargo Security investment, which were due to technical complications and dependencies on other investments, were addressed by establishing a new cost and schedule baseline. Nonetheless, this lack of documentation is inconsistent with the direction of DHS's guidance and related best practices, and it shows a lack of process discipline and attention to key details, which raises concerns about the thoroughness of corrective efforts.

Of the six investments without any corrective efforts, officials from these investments (namely, the Office of the Chief Information Officer's Human Resources IT investment, NPPD's US–VISIT Automated Biometric Identification System and Arrival and Departure Information System investments, USCG's Business Intelligence investment, NPPD's National Cybersecurity Protection System, and USCIS's Claims 4 investment), stated that they did not develop and document corrective efforts because they believed DHS's guidance does not call for it in their circumstances. Specifically, the officials said that although DHS's guidance [10] calls for corrective actions to be developed and documented when an investment experiences a life-cycle cost or schedule variance, the variances on their project activities thus far were not large enough to constitute such a variance.

The impact of this approach is that multiple projects can continue to experience shortfalls—which increases the risk that investments will experience serious life-cycle cost and schedule variances—without having to develop and document corrective actions to alert top management about potential problems and associated risks. This is inconsistent with the direction of OMB, which requires agencies to report (via the IT Dashboard) on the cost and schedule performance of their projects and considers those projects with a 10 percent or greater variance to be at an increased level of risk of not being able to deliver promised capabilities on time and within budget, and thus they require special attention from management. It is also inconsistent with our best practices research and experience at Federal agencies, which stresses that agencies report to management when projects are not meeting expectations or when problems arise and quickly develop and document corrective efforts to address the problems. Further, our research and work at agencies has shown that waiting to act until significant life-cycle variances occur can sometimes be risky and costly, as life-cycle schedules are typically for multi-year periods, allowing the potential for underperforming projects to continue to vary from their cost and schedule goals for an extended amount of time without any requirement for corrective efforts. Consequently, until these guidance shortcomings have been addressed and each underperforming project has defined and documented corrective actions, the Department's major investments these projects support will be at an increased risk of cost and schedule shortfalls.

DHS NEEDS TO ADDRESS GUIDANCE AND COST AND SCHEDULE SHORTFALLS

To help ensure that DHS investments meet their cost and schedule commitments, we recommended that the Secretary of Homeland Security direct the appropriate officials to: (1) Establish guidance that provides for developing corrective efforts for major IT investment projects that are experiencing cost and schedule shortfalls of 10 percent or greater, similar to those identified in our report, and (2) ensure that such major projects have defined and documented corrective efforts.

DHS concurred with our recommendations and estimated that they would implement the first recommendation by September 30, 2013, and the second one immediately. We are currently in the process of following up with DHS to assess the extent to which these recommendations have been implemented.

In summary, most of the projects comprising DHS's 68 major IT investments were meeting their cost and schedule commitments, but 21 major investments—integral to DHS's mission and costing approximately $1 billion—had projects experiencing significant cost and schedule shortfalls. These shortfalls place these investments at increased risk of not delivering promised capabilities on time and within budget, which, in turn, pose a risk to DHS's ability to fully meet its mission of securing the homeland. DHS guidance does not require projects experiencing significant cost and schedule shortfalls to develop and document corrective efforts until they cause a life-cycle cost and schedule variance. This increases risk and is contrary to effective IT investment practices. Given that DHS is currently establishing and implementing

[10] Department of Homeland Security, *Acquisition Management Directive 102–01 and Capital Planning and Investment Control Guide,* version 7.2.

new IT governance processes, the Department is positioned to address the guidance shortfalls.

Chairman Duncan and Ranking Member Barber and Members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

Mr. DUNCAN. Thank you, Mr. Powner.

The Chairman will now recognize Inspector General Edwards for 5 minutes.

STATEMENT OF CHARLES K. EDWARDS, DEPUTY INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. EDWARDS. Chairman Duncan, Ranking Member Barber, and Members of the subcommittee, thank you for the opportunity to discuss the Office of Inspector General's work to address the Department's IT management challenges. Today I will discuss our work to improve management, oversight, and efficiencies at the Department level, and to ensure that CBP and USCIS have adequate management practices and technology to effectively support mission needs.

The Department relies heavily on IT, spending about $6 billion a year for IT systems on infrastructure. Effective oversight and management of IT expenditures is 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 of a centralized management of IT and providing the CIO with authority and oversight of components IT investments.

With regard to IT systems and operational efficiencies, component CIOs face challenges to ensure that IT environment fully meets mission needs. Often we find that limited interoperability and functionality of components, aging technology infrastructures hinder personnel from conducting activities.

For example, in June 2012 we reported that CBP faced challenges with systems' availability, including periodic outages of critical security systems. This was due in part to its aging infrastructure. Furthermore, the interoperability of the IT infrastructure was not sufficient to support CBP mission activities.

As a result, staff created workarounds or employed alternate solutions. In some cases CBP assigned agents to perform duplicative data entry instead of enforcement duties in the field. In other instances CBP staff operated stand-alone, non-approved IT. Such activities may hinder CBP's ability to safeguard borders and ensure officer safety. We recommended that CBP CIO develop a funding strategy for the replacement efforts of outdated IT infrastructure.

USCIS faces similar challenges with an IT environment that does not effectively support its mission's operations. We reported in July 2009 and again in November 2011 that USCIS continues to rely on paper-based processes to support its mission.

On any given day, USCIS processes about 30,000 applications for immigration benefits. Yet, USCIS provides nearly all of its services using paper forms. This hinders USCIS personnel from processing immigration benefits efficiently, combating identity fraud and providing partner agencies the information needed to identify criminals and possible terrorists.

Although the current transformation program is meant to transition the agency from a paper-based system to an account-based environment, implementation has been delayed repeatedly over the past 8 years. We recommended that USCIS complete business and technology process documentation to provide the detail necessary to implement the transformation program effectively.

We also recommended that USCIS revise its governance structure to enable more streamlined decision making for its agency-wide IT modernization effort. In November 2011 we reported that although USCIS establish a transformation governance structure, this structure has weaknesses that have contributed to transformation delays.

Transformation leadership told us the Government structure was too complex, that too many stakeholders and boards involved in making decisions. USCIS did not have the sufficient governance mechanism in place to ensure effective acquisition of IT resources. We are encouraged by the steps taken by USCIS to address our recommendation.

In conclusion, our audits have identified weaknesses in IT management functions and widespread IT function limitation across the Department. Although there remain resource constraints that limit the Department, progress has been made in addressing these areas over the past few years.

Mr. Chairman, this concludes my prepared remarks, and I would be happy to answer any questions that you or the Members may have. Thank you.

[The prepared statement of Mr. Edwards follows:]

PREPARED STATEMENT OF CHARLES K. EDWARDS

MARCH 19, 2013

Mr. Chairman and Members of the subcommittee: Thank you for the opportunity to discuss DHS' information technology (IT) issues. My testimony today will address the predominant IT management issues we have reported on over the past 2 years.

The majority of information that I will provide is contained in our reports, *Customs and Border Protection Information Technology Management: Strengths and Challenges* (OIG–12–95), *DHS Information Technology Management Has Improved, But Challenges Remain* (OIG–12–82), *U.S. Citizenship and Immigration Services' Progress in Transformation* (OIG–12–12), *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG–11–108), *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG–11–69), and *U.S. Secret Service's Information Technology Modernization Effort* (OIG–11–56). I will also provide an update on the progress made by DHS on implementing some of the report recommendations.

DHS budgets over $6 billion a year for its IT. This represents nearly 15 percent of the DHS overall budget. The 22 component agencies that currently make up DHS rely extensively on IT to perform a wide range of mission operations, including counterterrorism, border security, and immigration benefits processing, among others. Given the size and significance of DHS' IT investments, effective management of Department-wide IT expenditures is critical.

DHS' IT MANAGEMENT OVERSIGHT

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] The Department has since strengthened the CIO's responsibilities for oversight and centralized management of IT, which has helped provide the authority for leading com-

[1] *Improvements Needed to DHS' Information Technology Management Structure* (OIG–04–30, July 2004). *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG–08–91, September 2008).

ponent CIOs toward a more unified IT direction. Specifically, we reported in May 2012 that the DHS Office of the CIO has improved oversight of IT programs and key IT management functions, such as acquisition and portfolio reviews, to improve CIO decision making.[2] As a result, the DHS CIO has better visibility of Department-wide IT programs and assets thus enabling the CIO to identify opportunities for reducing costs and duplication across the Department's IT environment.

In the same report, we concluded that DHS had further defined the CIO's authority and responsibility. For example, the DHS deputy secretary issued a memorandum in May 2011, which directed the CIO to take a greater role in the review and execution of all IT infrastructure investments.[3] The expansion of DHS CIO authority was due in part to the Federal CIO's IT reform plan, which requires agency CIOs to implement initiatives to improve management of large-scale IT programs.[4] Additionally, Office of Management and Budget Memorandum M–11–29, *Chief Information Officer Authorities,* states that agency CIOs must drive the investment review process for IT investments. To formalize this guidance, the DHS under secretary for management began an effort to update the Delegation of Authority for the DHS CIO, which included oversight of the Department's IT programs.

The CIO has increased oversight of Department-wide IT programs and investments by conducting annual IT program reviews and in-depth reviews of selected IT programs. These reviews enable the CIO to make strategic recommendations for reducing costs and duplication across the Department's IT environment. For example, the DHS CIO issued 90 recommendations to the deputy secretary for the 2013 budget year for 81 IT investments continue as planned, eight investments be continued but modified, and one be suspended. The CIO also made program-specific recommendations, such as to reinstate $10 million in funding per year for the Customs and Border Protection (CBP) Traveler Enforcement Compliance System Modernization in order to prevent further schedule delays, as well as a recommendation that the Federal Emergency Management Agency (FEMA) suspend work on its National Flood Insurance Program Information Technology Systems and Services until business requirements were better defined.

In addition, the DHS CIO has increased oversight of IT software, hardware, and infrastructure purchases through the IT acquisitions review process. The volume of IT acquisition reviews has increased from 243 in fiscal year 2007 to 387 in fiscal year 2011. The number of approvals for IT acquisition requests has increased from 129 in fiscal year 2007 to 311 in fiscal year 2011. These reviews have increased the DHS CIO's ability to verify compliance with technical standards and to ensure program and project alignment with Department-wide IT policy, standards, objectives, and goals.

The Department has also achieved infrastructure integration milestones through data center and network consolidation. Specifically, the Office of the CIO (OCIO) continues its efforts to consolidate data centers across the Department, integrate disparate component networks into a single DHS network, and create centralized email and collaboration services to improve information sharing. As of November 2011, DHS headquarters, FEMA, the Transportation Security Administration (TSA), and CBP had migrated applications from eight sites to one DHS enterprise data center. Additionally, DHS has established an enterprise network, OneNet, as well as a primary and secondary network operations center and security operations center. The OCIO has also begun offering centralized IT services housed at the two enterprise data centers, such as email and Microsoft SharePoint, to achieve economic savings through consolidation. Some components are already realizing cost savings from the data center consolidation and DHS enterprise service offerings.

Finally, the Department matured key IT management functions, such as strategic planning, Capital Planning and Investment Control (CPIC), enterprise architecture, and portfolio management. For example, the OCIO developed an IT strategic plan for fiscal year 2011–2015. In addition, the DHS OCIO has continued to execute its CPIC process effectively, which is DHS' primary process for making decisions about the systems in which the Department should invest. The OCIO has also continued to execute Department-wide enterprise architecture efforts, such as the development of a Homeland Security Enterprise Architecture and specific segment architectures, which provide the CIO with a foundation for making better-informed decisions. Finally, the DHS Portfolio Management process, which establishes portfolios based on DHS' mission areas and business functions, helps the OCIO to align IT investments

---

[2] *DHS Information Technology Management Has Improved, But Challenges Remain* (OIG–12–82, May 2012).

[3] DHS Deputy Secretary, *Information Technology Efficiency,* May 5, 2011.

[4] *The 25 Point Implementation Plan To Reform Federal Information Technology Management,* December 9, 2010.

with portfolios and identify redundancies or gaps. Over the past 2 years the DHS OCIO has begun conducting an annual portfolio analysis to align IT investments to its 13 existing portfolios and identify redundancies or gaps. At the time of our audit, the OCIO had aligned more than 650 IT investments with the 13 portfolios.

MAJOR CHALLENGES

Although DHS has made significant progress in improving IT management functions, challenges remain for CIO involvement in component IT budget planning. For example, the DHS CIO conducts a review of all components' IT budgets as part of the DHS IT budget formulation process, which provides opportunity to confirm that component plans are in line with Departmental priorities. However, the CIO is not involved during the component IT budget planning process when initial planning activities are taking place. As such, the CIO IT budget reviews do not directly affect the amount of funding components receive, meaning components can obtain funding for IT investments regardless of the decisions made during the budget review process. For example, a review of one component's IT budget revealed a funding request for approximately $6 million to improve IT infrastructure. Yet, the OCIO had requested $91 million from the component for data center migration costs for the same budget year, highlighting a discrepancy in funding plans.

To address this issue we recommended that the deputy under secretary for management assign the DHS CIO centralized control over the Department's IT budget planning process to review, guide, and approve IT investments. Since this recommendation was made, the DHS CIO has been delegated the authority to review and approve IT budgets for delivering and maintaining enterprise IT solutions and mission IT systems and services throughout the Department in coordination with the DHS CFO. The recommendation was closed in September 2012.

COMPONENT-SPECIFIC CHALLENGES

Insufficient IT management practices, need for CIO IT budget authority, fragmented and aging IT infrastructures, and inadequate governance mechanisms have been long-standing issues for several DHS components.

Component IT Management Practices Need Improvement

Although DHS and its components have made progress establishing effective IT management practices, several DHS components have not fully implemented key IT management functions needed to guide agency-wide IT programs. For example, in June 2012 we reported that CBP had developed an enterprise architecture to align with the Department's architecture and guide CBP's IT environment.[5] However, the Office of IT had not yet developed a target "To-Be" business architecture to analyze business processes. Without a complete view of CBP's target enterprise architecture, the CIO faces increased risks to efforts to modernize the way OIT provides support to CBP. We recommended the CBP OIT provide the necessary resources to complete required enterprise architecture activities.

Similarly, we reported in April 2011 that FEMA had not yet completed its enterprise architecture. Specifically, the agency had not completed efforts to document its business functions, information resources, and IT systems as part of its baseline enterprise architecture.[6] Also, the IT architecture remained undocumented for many program areas and the standards on the OCIOs website were at least 2 years out-of-date. We also determined that FEMA did not have a comprehensive IT strategic plan with clearly-defined goals and objectives or guidance for program office initiatives. Without these critical elements in place, FEMA is challenged to establish an effective approach to modernize its information technology infrastructure and systems. We recommended FEMA complete and implement an enterprise architecture and develop a comprehensive IT strategic plan. Each of these recommendations were closed in January 2013 when FEMA produced evidence of a completed baseline architecture and an updated IT Strategic Plan.

Likewise, we reported in March 2011 that the United States Secret Service (USSS) had not updated its IT Strategic Plan since 2006.[7] As a result, its plan was not sufficient to address its system weaknesses or integrate with DHS' technology direction. For example, the plan did not describe how the USSS will leverage specific DHS enterprise-wide solutions such as DHS Consolidated Data Centers and OneNet. Additionally the IT Strategic Plan did not accurately reflect Information In-

[5] *CBP Information Technology Management: Strengths and Challenges* (OIG–12–95).
[6] *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG–11–69).
[7] *U.S. Secret Service's Information Technology Modernization Effort* (OIG–11–56).

tegration and Transformation Program activities such as planned upgrades to technology platforms. We recommended that the deputy director, USSS create effective planning documentation.

Component CIOs Need Additional Budget Authority and Oversight

Most of the major component CIOs lack IT budget authority and oversight of technology spending across programs and activities within their agency. For example, in our June 2012 review of CBP we found that the CIO did not have full oversight of IT spending across all programs and activities within CBP.[8] Specifically, CBP component offices submit IT spending requests that were processed by procurement without going through the CIO's IT acquisition review process, thus increasing the risk of security issues or enterprise alignment challenges. Likewise, in April 2011 we reported that FEMA's program offices and regional offices continue to develop IT systems independent of the OCIO due in part to decentralized IT budget and acquisition practices. Specifically, the manner in which IT programs are funded and developed within FEMA hindered the OCIO's efforts to establish a complete inventory and manage IT capital planning and investment. For example, during fiscal year 2010, FEMA spent $391 million for agency-wide IT needs, but the OCIO accounted for only 29 percent of total spending. We recommended the FEMA CIO establish an agency-wide IT budget planning process to include all FEMA program technology initiatives and requirements.

In September 2011, we reported that the United States Coast Guard (USCG) CIO had limited authority over IT assets and spending.[9] Specifically, the CIO does not have sufficient oversight of IT spending by field units. Without this authority, the CIO cannot fully ensure that the Coast Guard IT environment is functioning effectively and efficiently. We recommended that Coast Guard chief of staff transition IT personnel and oversight of field IT spending under the CIO. Likewise, in our March 2011 review of USSS[10] we determined that the USSS did not position its CIO with the necessary authority to review and approve IT investments. Specifically, the CIO was not a member of the director's management team and therefore does not play a significant role in overseeing IT systems development and acquisition efforts. We recommended the deputy director, USSS provide the CIO with agency-wide IT budget and investment review authority to ensure that IT initiatives and decisions support accomplishment of the USSS and Department-wide mission objectives.

Outdated IT Does Not Effectively Support Component's Missions

Component CIOs are challenged to ensure that the IT environment fully supports its agencies mission needs. Commonly, interoperability and functionality of component's aging technology infrastructures have not been sufficient to support mission activities. For example, in June 2012 we reported that the CBP Office of IT (OIT) faced challenges with system availability, including periodic outages of critical security systems.[11] Systems outages have occurred in part because of aging infrastructure, which has not been updated as required because of funding reductions. In addition, the interoperability and integration of the IT infrastructure were not sufficient to support CBP mission activities fully, due to lengthy requirements-gathering and technology insertion processes. As a result, staff created workarounds and employed alternative solutions, including assigning agents to perform duplicative data entry—instead of enforcement duties in the field—and operating stand-alone, nonapproved IT. We recommended the CBP CIO develop a funding strategy for the replacement of outdated infrastructure. As of February 2013, the CBP OIT was continuing to assess the needs across CBP to present additional requirements for funding consideration and prioritization against all other CBP priorities.

Also, we reported in September 2011 that Coast Guard systems and infrastructure did not fully meet mission needs due to aging infrastructure that is difficult to support, and stove-piped system development.[12] Specifically, Coast Guard field personnel do not have sufficient network availability, the aging financial system is unreliable, and command center and partner agency systems are not sufficiently integrated. As a result, field personnel rely on inefficient work-arounds, such as having to enter the same information twice, to accomplish their mission. We recommended the Coast Guard CIO address the IT systems and infrastructure needs

---

[8] *CBP Information Technology Management: Strengths and Challenges* (OIG–12–95).

[9] *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG–11–108).

[10] *U.S. Secret Service's Information Technology Modernization Effort* (OIG–11–56).

[11] *CBP Information Technology Management: Strengths and Challenges* (OIG–12–95).

[12] *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG–11–108).

by implementing a plan to ensure system redundancy to meet availability requirements, implement a strategy to improve ease of use and availability of the financial systems, and ensure that new tools address requirements for improved integration. Since that time, the recommendation to ensure that new tools address requirements for improved integration was closed in April 2012.

In April 2011, we reported that FEMA's systems were not integrated, did not meet user requirements, and did not provide the information technology capabilities agency personnel and its external partners needed to carry out disaster response and recovery operations in a timely or effective manner.[13] Specifically, limited progress had been made in modernizing the agency's critical mission support systems due to uncertainty of Department-wide consolidation plans. As a result, FEMA's legacy systems were not able to effectively support disaster response functions in a timely and effective manner. As a result, FEMA personnel were using paper forms and relying on manual data entry to process grants. These manual work-arounds may suffice during minor events; however, they may not sustain the increased workload and level of information sharing required to support major disasters. We recommended the FEMA CIO establish a consolidated modernization approach for FEMA's mission-critical IT systems, to include DHS plans for integrated asset management, financial, and acquisition solutions. As of December 2012, FEMA had included modernization plans in its 2012 IT Strategic Operations Plan; however, the recommendation remains open until the OCIO develops a modernization approach for FEMA's mission-critical IT systems.

The United States Citizenship and Immigration Services (USCIS) faces similar challenges to establish an IT environment that can effectively support its mission needs. We reported in November 2011 that USCIS continued to rely on paper-based processes to support its mission, which made it difficult for USCIS to process immigration benefits efficiently, combat identity fraud, and provide other Government agencies with the information required to identify criminals and possible terrorists quickly.[14] On any given day, USCIS processes 30,000 applications for immigration benefits. Yet, USCIS provides nearly all of its services using paper forms: Customers submit paper application forms; USCIS adjudications officers determine whether an applicant is eligible for benefits by reviewing the paper documentation; and USCIS issues paper evidence of benefits. USCIS staff also must use automated and manual methods to conduct background checks on applicants. An enterprise-wide transformation program is under way to transition the agency from a paper-based operational environment to an account-based environment using electronic adjudication. However, implementation of the transformation has been delayed repeatedly over the past 8 years. We recommended that the Office of Transformation Coordination complete business and technology process documentation to provide the detail necessary to implement the transformation program effectively. Since that time, USCIS provided process documentation in July 2012 and the recommendation was closed.

Better IT Governance Needed for IT Modernization Efforts

Components implementing transformation efforts are hindered by insufficient governance and decision-making mechanisms to effectively direct agency-wide transformation program activities. In our March 2011 report, we found that the USSS did not implement an effective IT governance approach for its Information Integration and Transformation Program, which had an estimated cost of $1.5 billion.[15] Specifically, the agency did not have a formal Department-level IT governance mechanism to provide integrated feedback and direction for the transformation program effort. Without a formal mechanism for integrated governance, the USSS reached out individually to DHS offices and received conflicting advice and did not sufficiently consider DHS enterprise-wide solutions. We recommended that the deputy director, USSS formalize an Executive Steering Committee and ensure that the Information Integration and Transformation Program is in alignment with the USSS and DHS strategic goals and objectives. Since that time, the USSS has provided updates on its ongoing efforts to implement an Executive Steering Committee which includes USSS Senior Management and DHS members from the offices of the CIO, the chief procurement officer, and the Acquisition, Planning, and Management Directorate.

Likewise, our April 2011 review of USCIS Transformation concluded that USCIS' transformation governance structure did not promote timely and effective decision

---

[13] *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG–11–69).

[14] *U.S. Citizenship and Immigration Services' Progress in Transformation* (OIG–12–12).

[15] *U.S. Secret Service's Information Technology Modernization Effort* (OIG–11–56).

making.[16] Specifically, the governance structure was overly complex and required too many formal meetings and checkpoints for review, hindering decision making. We recommended that the chief, Office of Transformation Coordination revise its current governance structure to enable more streamlined program decision making. Since that time, USCIS has continued to revise its governance structure to include a Transformation Executive Steering Committee and a Product Management Team.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or Members of the subcommittee.

Mr. DUNCAN. Thank you, Mr. Edwards.

Thanks to everyone for their testimony. I will now recognize myself for 5 minutes of questions.

First thing I want to point out is in the GAO report, Mr. Powner. I was looking at the primary causes for cost and schedule shortfalls and inaccurate preliminary cost and schedule estimates. What attributed to that? Had they changed the needs? Did they not think through the whole IT process appropriately? I ask that question in light of going out to St. Elizabeths and the cost overruns there.

Mr. POWNER. A couple things. One is when you look—when we look at cost and schedule estimating, requirements is a big area. So if you look at requirements many times, as I know Ranking Member Barber, you mentioned about getting the user requirements up front with systems like SBInet. So, getting the requirements nailed down that definitely affects your cost and schedule estimate up front.

Also, we look at the complexity where if you have interdependencies from other systems, and some of these projects have you know various components that need to work together. We look for critical pass and how they manage that. It is a very disciplined process when you look at the complexity involved with some of these acquisitions, Mr. Chairman. We find holes in that discipline when it comes to both the cost and schedule estimating.

But again, requirements is key, making sure you have—because if you don't have the requirements up front, you could have discipline processes. You are still going to have a poor estimate.

Mr. DUNCAN. Well, I have never built a house, but I was a banker for 8½ years, and financed a lot of them, and saw a lot of wives and husbands make changes to the house as it was being built. When you change the priorities going forward in any kind of project you are going to run into cost overrun. So, you have got changes in agency priorities. Can you elaborate?

Mr. POWNER. There are—again, several of those systems, these are the 21 systems that were not within 10 percent of cost and schedule estimates. So we saw that again. This is tied to requirements too. There is a link to requirements. But we saw some of these systems.

There was a change in priorities for the agency. So, for instance, when you start looking at you know a good example—I mean this wasn't, but if you go back to like our US–VISIT work, you know one time you are focused on exit and entry, you are focused on a biometric. Then all of a sudden we start going with a smaller focus.

One of the things I would like to highlight when you look at these priorities is it is very important to go smaller; smaller increments on these projects because Mr. Edwards mentioned many

[16] *U.S. Citizenship and Immigration Services' Progress in Transformation* (OIG–12–12).

times—many of the past problems had been they tried to do so much all at once. If you look at the corrective action plans currently in DHS's statement, there is typically deliverables within 12 months. So we want to see more of that incremental approach to things because then it is more manageable. Then that way we can stick to the priorities if it is smaller.

Mr. DUNCAN. Thank you for your work on that. I am going to shift to yours in just a minute because the TECS system is something I am very, very interested in, Traveler Enforcement, and how we are screening the folks that are coming into this country, the databases we are building on each of those individuals, but how that information is shared between the front-line people that are doing visa applications or screening with the State and ICE and also there at the border, particularly airports, coming into this country.

So, I will ask Ms. Graves, how did—or how will modernizing the TECS system benefit those ICE agents? How does ICE coordinate with the CBP in that effort?

Ms. GRAVES. Well, luckily, sir, there is a joint program office effort that works together with ICE and CBP that looks at the case management aspect of the TECS Modernization, which is the ICE piece of equation, as well as the modernization of how the derogatory databases are pulled together to provide that data to the front-line officers for their adjudication and for their identification of possible entrants into the country that have derogatory information against them.

Some of the modernizations that are going on in the TECS—in the TECS Modernization program are going to provide some additional functionality, and particularly there are going to be some improvements made that are going to help with the efficiencies of the front-line officers. Those include the fact that when the primary adjudication is done that that affirmation is going to be packaged and passed in an automated fashion to the secondary adjudicator.

That adjudicator will be able not only to have that immediately available, but be able to build upon that by adding additional datasets from the Department of Agriculture, from other areas that were not included in the first primary screening.

So, that would streamline the process. The secondary adjudicator wouldn't be starting over. It also feeds directly into once the adjudication is made into the case management aspect within ICE so that if there is a derogatory finding that would be the—would enter into the case management process.

Both of those systems are being modernized in an integrated fashion. The expectation is to exit the mainframe technology with both of those systems being off the mainframe technology in concert in 2015.

Mr. DUNCAN. Yes. I have been down to Nogales to the vehicle crossing there and stood in the phone booth-type apparatus where the Customs and Border Patrol Agents are screening those cars and the occupants. I want to make sure, and I know you do as well, but that the information they have on those occupants as they scan their ID cards or their passports is accurate and we know that they have got every—every bit of information, even if it is derogatory to-

wards apprehending illegals or terrorists or others that are coming into this country.

I think the American people would want us to make sure that those Border Patrol agents have up-to-date and complete information on suspected terrorists that might be coming in, or other individuals. So I am looking forward to seeing how TECS Modernization goes forward. I appreciate your testimony.

With that I will yield to Mr. Barber, the Ranking Member.

Mr. BARBER. Well, thank you, Mr. Chairman. I wanted to ask Ms. Graves a question related to lessons learned and how we might improve processes going forward.

As you know, I noted that we, unfortunately prohibited the end-users or the Border Patrol agents from having impact on the initial SBInet effort. So, given that experience, and knowing that we spent a billion dollars that really didn't get us too far, what plans is the Department or steps the Department taking to include the end-users fairly early on in the future development of IT? Can you elaborate on what you are doing to change that approach?

Ms. GRAVES. Yes, absolutely. I am pleased to be able to tell you that—I will use the ACE program as an example. We met last week and what we are doing in implementing the Agile methodology, the Agile development methodology for IT is we are creating user stories. The source of that user story, Mr. Powner spoke about requirements. But in the Agile methodology the requirements are actually drafted into these user stories that are actually developed in concert with the embedded operational entities that will work with the program throughout its development cycle.

These users are developing along with the developers. They are sitting with the developer. They are talking through the use cases. They are testing at appropriate times when functionality is actually delivered. They are providing immediate feedback, which is continuously incorporated into the development cycle so that they are constantly at the table.

There is no separation of church and state. There is no indication that there is going to be a quick conversation with a user base and then you develop over in the corner and you come back later on and you find that you really haven't hit the mark. It is a continuous process. It is continuous integration, continuous user stories. What they also do by having the users at the table is to understand how those priorities change.

We talked about one of the things that drives cost overruns in the changing requirement landscape and the shift in priorities. With the users constantly at the table we have the opportunity to have the business mission side of the equation adjudicate what is going to be the next user story that is actually developed. In that case it allows us to shift or transfer workload accordingly, driven by the business imperative.

Mr. BARBER. I appreciate the steps. Hopefully they will ensure that we go forward with a full understanding of what the end-users need and can actually help us design.

This is a question specific to one of the—Ms. Graves, for you, specific to one of the 21 projects that are problematic. I am focusing here on the National Cybersecurity Protection System. This committee, the overall Committee on Homeland Security, I know the

Chairman and I am also very concerned about where we are going with this.

The President issued an Executive Order recently putting some priority on this for DHS. But, this is one of the 21 that is not doing so well. What steps are being taken subsequent to the President's Executive Order to give priority to the cybersecurity IT system?

Ms. GRAVES. We have an executive steering committee. As I spoke earlier about our tiered governance process, we have an executive steering committee which has actually got the leadership of NPPD, the component that owns that system at the table.

Also, there has a lot of what I would consider to be stakeholder involvement from the ISPs, the internet service providers out in the commercial sector because that particular system has to be developed in concert with them. There has to be a full understanding of the requirements base as well as the expectation of what the capability is going to be at the end of delivery.

So, I think what we are going through now is that ESC is looking at those requirements bases and they are making the appropriate adjustments along with the ISPs. Some of the conversations for the ISPs are on-going and still have to be concluded. So I would put for the record that we could come back and speak to that when that has occurred.

Mr. BARBER. You just have a few seconds left, but I just want to elaborate on that question as we look at sequestration and what is happening to the Department's budget. How are you going to—or how are you prioritizing projects, given what you are facing with sequestration?

Ms. GRAVES. With sequestration the Department will prioritize the requirements based on the Secretary's goal priorities. That of course, as she has stated repeatedly in public forums is front-line mission. Many of those front-line missions are the ones that we have discussed today.

So I have no doubt that those will be prioritized. It really is about the law enforcement officer on the ground and about fully outfitting that officer with the communications capability and the IT information capability in order to effectively do their job.

Mr. BARBER. Thank you, Mr. Chairman.

Mr. DUNCAN. Thank you.

The Chairman now recognizes the gentleman from Big Sky Country, Mr. Daines, for questioning.

[Off mike.]

Mr. DAINES. We will try this one. That is better.

There has been a lot of discussion here about cost and schedule, which I completely appreciate and respect. I spent 28 years in the private sector, in fact 12 years of a cloud computing company delivering projects. So I have seen it from both sides.

There has been—you know the discussion has been on cost and on schedule, an important role certainly of the CIO of an organization in project management and delivery. But a project is still a means to a greater end. I would—as a taxpayer and representative of taxpayers of America, there has been investments made. But I want to talk to you about the return on that investment, assuming for a moment that we do hit projects on schedule and at or below budget.

Let me talk, Ms. Graves, about the two or three best examples where we have really seen a return on investment for the taxpayer on completed projects.

Ms. GRAVES. Again, I will go back to—I will start with ACE and then I will segue into a couple of the other programs that we have talked about today.

Particularly for ACE what we have seen in terms of real metrics and measurable outcomes that are associated with the improvements that have been made in that program would include faster border crossings. The ACE truck manifest capability today provides 30 percent faster processing time. Industry cash savings, of course here with ACE we are dealing primarily with the trade community.

So today ACE provides for monthly interest-free duty payments accounting for over 60 percent of all duty and fee payments. So that is a savings to the trade industry. Single window of capability for the ACE partners in trade to come into the system and get all of the services that are provided by the unified system. So, those are just a few with ACE.

When we look at CIS transformation what we are talking about there is an instantaneous improvement with the ability to do automated benefits approaches. In the sense of the customer, the person asking for adjudication of either benefits or citizenship, it provides an automatic account setup.

It provides an ability to take what they input into that automated account setup in terms of their name, date of birth, other personal information. That information will flow to other transactions that they might have with CIS in the future, which makes it more customer-friendly. It allows them to look up the status of their application. It also provides a customer interface that is—has been—the tires have been kicked, it is very user-friendly.

CIS has proved the outcome as being positive by actually going back to the users that have used the new automated system and asking them to complete a survey. That survey has indicated a 94 percent positive response saying that this is much better than what they have had to deal with in the past.

Mr. DAINES. I am glad to hear there is metrics there. What was the total investment on ACE, roughly?

Ms. GRAVES. I think it is about—hold on just a moment, sir, I might have that. If I don't, I will get it back for the record. But I think it is about $1.2 billion to date——

Mr. DAINES. With $1.2 billion, are you able to quantify any specific monetary savings for that investment?

Ms. GRAVES. I don't have that information readily available. But I can certainly get that back for the record.

Mr. DAINES. I would appreciate just looking—and I realize that there may be some more qualitative kind of savings versus quantitative because you talk about customer satisfaction. But I think it is just helpful as we think about the investment around what is quantifiable in terms of return, you know from a dollar viewpoint. I would appreciate seeing that information.

Ms. GRAVES. Yes, sir.

Mr. DAINES. Any other positive benefits that you maybe could comment on relating to the adoption of cloud computing, or move to that platform?

Ms. GRAVES. I am smiling because this is kind of the wheelhouse of the OCIO. So I am very happy to talk about that.

We have established at DHS two secure data centers, and we are consolidating 42 separate data centers into those. We have completed 18 at this point. The way that we are doing that is we have adopted a methodology where establishing cloud services and particularly platform-as-a-service, software-as-a-service within those two data centers so that we can migrate our components to those. I will give you two recent examples.

One, we are in the midst of our enterprise consolidation of our email systems and we have moved four of our primary components onto that system at this point in time. We have 109,000 users with approximately another 120 to go. In that process we have saved—we established a service that is essentially $7.00 a mailbox.

That has been benchmarked against external companies that are providing the same type of service. But in fact, ours is enhanced because of the security requirements of DHS. But we benchmarked that against Google and against Microsoft, et cetera. From the posture that our components had that have already moved in, we have documented the savings and I can provide those to you in, again, in a question for the record.

Also we have—I will give you an example of FEMA. We went from $24 a mailbox down to $7.00. So these are really quantifiable savings that we can talk about. We have 12 of these enterprise cloud services, each one of which has its story attached to it.

Mr. DAINES. Okay. I yield back.

Mr. DUNCAN. Thank you.

The Chairman will recognize Mr. Payne, from New Jersey.

Mr. PAYNE. Thank you, Mr. Chairman. Good afternoon.

Mr. Powner and Ms. Graves, I represent the 10th District in New Jersey, which encompasses the Port of Newark and Port of Elizabeth, which makes up the New York-New Jersey port system.

So as you know—as you can imagine, I am very concerned about the safety of the port and whether we are doing everything we can to make sure that our ports have the most up-to-date technologies and IT systems that ensures the CBP, as well as local law enforcement, have the tools to be able to do their jobs efficiently and effectively to prevent illegal and dangerous materials from coming into our country, all the while expediting the flow of commerce.

The—a system is being developed with the goal to streamline port entry and for legitimate trade, but also to ensure our safety and our ports. Could you explain the advances in the ACE technology? I know you alluded to some of it this morning, Ms. Graves. Include how these advances will achieve the goal or streamline trade protecting our ports.

Ms. GRAVES. Certainly. The key here is to provide a platform that allows us to operate in the information-sharing environment. It is the whole reason why DHS was warned in the first place, because the failure to share certain information may have resulted in 9/11.

When we look across the landscape of what is being provided by ACE, they are pulling information from not only within DHS but also from cargo manifests, from the screening that gets done at the ports themselves. If you are familiar with NIIS, which is the actual

screening for rad/nuclear and other explosive materials, that gets done at each port.

All of that information feeds into the commercial environment, the automated commercial environment. What it allows the individual officers to do is truly develop a risk profile. So the more information that they have on individual companies with the longevity of how they have dealt with them in the past and the myriad of information that they have collected on those companies, as trade moves in and out of the port they have a profile of individual transactions.

That helps them develop that risk-based approach to where they should spend their time, their officers' eyes on the prize in terms of that risk-based analysis. It allows them to develop a set of trusted partners, trusted shippers, and then concentrate on the area where there is not as much information or where there may be some derogatory information that would you know be better—time would be better spent there to try to prevent anything from happening.

Mr. PAYNE. Okay. Where do the shortfalls in implementing ACE continue to exist?

Ms. GRAVES. At this point in time we are in a pilot stage of doing the first few sprints in the Agile methodology. I think what this will do is it will solve some of the problems that we talked about at the very beginning. The ability is to be flexible in terms of the changing requirements.

One of the things that I believe got ACE into trouble in the first place was the changing priorities of the trade organization, some legislative changes that required that the system be updated and configured in a different fashion to support those changing legislative requirements. In this methodology I believe we will be able to address those more effectively.

Mr. PAYNE. Okay. Well I will—in the interest of time I will yield back.

Mr. DUNCAN. Thank the gentleman for yielding back.

The Chairman will now recognize Mr. O'Rourke from Texas.

Mr. O'ROURKE. I wanted to follow up on some of the questions asked and comments made about return on investment. I know, Mr. Powner, in your testimony you pointed to arrests made and entry denied as return on the investment made in I believe the Century program.

What about—and Ms. Graves, you talked about in terms of ACE getting more efficiencies in crossings—in legitimate crossings. That is the subject I am really interested in, how we increase throughput of legitimate trade, people, and privately-owned vehicles at our crossings. Do you have any specific measures for what these investments turned into?

Because we know in El Paso, and I think those of us who are interested in trade in this country understand that the more we get through our ports of entry, the more jobs we create here. There is a number that we can ascribe to that return. Can you do that against the investment that you have made in these different platforms and softwares and programs and technologies that have been adopted?

Ms. GRAVES. Yes, we do have performance measures that are in place for each one of these programs. If they are specifically designed the way you described, I will have to go back and look. I can certainly do that for the record.

But to the point of the streamlining and the reduction in the process time and things of that nature, as—you know as working in the finance arena I believe you could quantify those back to dollars. I will check into that.

Mr. POWNER. If I could add, the discussion about return on investment, we focus a lot on cost and schedule and stuff. This is exactly the right focus that is needed. So if you look at the—we spent—DHS spends $4 billion annually on 68 systems. CBP, ICE, and CIS, there is 32 investments about $2 billion. Okay, 32 investments, $2 billion; that is a lot of money for 32 systems.

I think the key question for DHS is those 32 systems, what are we getting in 2013 for a $2 billion investment in those three organizations? Or for these 68 systems that we spent $4 billion on, what are we getting?

Mr. O'ROURKE. Right.

Mr. POWNER. Two-thousand thirteen. What did we get last year?

So, some of the documentation goes to OMB to justify the investments. There is some pretty good data in there and some metrics that DHS provides—that I provided in my oral statement on the US–VISIT application. But I think one of the things is DHS moves towards its incremental development. It is great that we are going incremental, but the bottom line is if we are going to spend $2 billion on 32, what are we getting in 2013, what is the plan in 2014?

Then there is follow up that in fact that functionality was delivered. Very few Federal agencies and departments—we call that like an integrated deployment plan or an integrated release plan. That would be very valuable for this committee if you had something like that. I think they have it by system. I don't think they have it for the collection of systems.

Ms. GRAVES. Right——

Mr. O'ROURKE. Yes. I was also looking at the numbers related to ELIS or E–L–I–S. The over $700 million spent and processed through that system I think 16,000 applicants, and realized it is not fully implemented yet, but that you know obviously should concern all of us. I am glad that the Ranking Member mentioned SBInet and some of the boondoggles that DHS has been involved in, in the past.

So, my question for the inspector general, or GAO, for Ms. Graves, is—when do you know when it is time to pull the plug on something and when you are not achieving that return that warrants additional money spent, especially in a time of tight budgets? Especially when we can't get enough CBP officers manning our ports of entry in El Paso?

Mr. EDWARDS. Well, basically it is the triple constraint. If you have the scope and schedule and cost, and if the scope deviates, naturally the cost and the schedule is going to deviate.

What DHS in the past has been doing was this big-bang approach, and not having a complete cost for the—lifetime costs for the systems in place. But in the last few years, with Rafael Borras

now, the Secretary and Deputy Lute, they have not looked at IT just as IT, but looked—have a holistic approach.

The IT piece and the acquisition; they want to create a group program called Accountability and Risk Management. Every IT requisition or request needs to go through this review board. They need to come prepared with the entire life-cycle cost of what it takes, and did they really meet that or not.

So they have a good process in place. It is going to take some time for them to get where they need to be.

Mr. O'ROURKE. I yield back.

Mr. DUNCAN. Thank you.

Thank you. Unfortunately we do have another vote series, about 10 minutes left on the clock.

So, Mr. Edwards, I thought you were going to get through the whole hearing without having to answer a question, but you got in there at the end.

So I want to thank the witnesses for your valuable testimony, and the Members for their questions today. It is a learning process for this committee on how IT is being integrated for the Department. We want to see some successes there because it is very important to the safety and security of this Nation.

Mr. Daines asked some questions that weren't answered. So if you could provide those in writing. The Members of the committee may have additional questions for the witnesses, and we will ask you to respond of these questions in writing.

Without objection, the committee will be adjourned. Thank you.

[Whereupon, at 3:53 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR MARGARET H. GRAVES

Question 1. What additional authorities could help the DHS CIO ensure border security and immigration IT programs are delivered on time, on budget, and meet/exceed capabilities?

Answer. Response was not received at the time of publication.

Question 2. What steps has DHS taken to ensure that legacy border and immigration IT systems can effectively share data and "speak to one another"? What concerns, if any, do you have on information sharing between legacy systems and how might these concerns impact border and immigration officers in the field?

Answer. Response was not received at the time of publication.

Question 3. CBP's Northern Border Remote Video Surveillance System was delayed by 2 months. How did this affect our security along the Northern Border? What is the current status of the program?

Answer. Response was not received at the time of publication.

Question 4. The DRO Modernization effort is supposed to make detention and removal more efficient. What does this mean in plain English? Should the American people be prepared for a higher number of detainee releases once this effort is completed in the future?

Answer. Response was not received at the time of publication.

Question 5. What is the status of IT efforts associated with the Secure Communities program? What have been the key IT challenges as the program has been deployed across the Nation? Are State and local infrastructures capable of properly supporting the program?

Answer. Response was not received at the time of publication.

QUESTION FROM HONORABLE RICHARD HUDSON FOR MARGARET H. GRAVES

Question. We frequently read about the inability of newly-deployed systems to communicate with one another and their predecessors once deployed. What is DHS doing to ensure that systems like TECS, a system of records that include temporary and permanent enforcement, inspection, and operational records relevant to the antiterrorism and law enforcement mission of numerous Federal agencies, will be able to interface with the existing systems at DHS as well as other Federal, State, and local agencies?

Answer. Response was not received at the time of publication.

QUESTION FROM HONORABLE BETO O'ROURKE FOR MARGARET H. GRAVES

Question. Although we recognize that RFID requirements for passports involves addressing globally-accepted standards, I understand that Ready Lanes used at our ports of entry to increase inspection efficiencies cannot use readers to scan RFID-enabled passports. The passport card, the laser visa/border crossing card, and the permanent resident card, however, all can be scanned at out ports of entry.

What is being done to better coordinate technology acquisition when used across multiple agency platforms?

How do we best address these inefficiencies?

How is CBP educating the public on the benefits of a U.S. passport card versus a regular passport book for admissions?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR DAVID A. POWNER

Question 1. What grade (A,B,C,D,F) would you give CBP, ICE, and USCIS in their development and implementation of major IT programs based on their ability to meet mission needs, cost, and schedule?

How would you rate DHS's performance in delivering IT systems against other Federal agencies?

Answer. Response was not received at the time of publication.

Question 2. Do DHS and its components (CBP, ICE, USCIS) have a shared vision and strategy for its IT programs?

If not, what impact does this have on their success?

Answer. Response was not received at the time of publication.

Question 3. IT management was highlighted in GAO's recently-issued "High-Risk List". According to GAO, the Department still has only partially addressed 4 of 6 IT management outcomes. Is DHS heading in the right direction to fix these deficiencies?

Why hasn't more progress been made on these outcomes?

Answer. Response was not received at the time of publication.

QUESTION FROM HONORABLE RICHARD HUDSON FOR DAVID A. POWNER

Question. We frequently read about the inability of newly-deployed systems to communicate with one another and their predecessors once deployed. What is DHS doing to ensure that systems like TECS, a system of records that include temporary and permanent enforcement, inspection, and operational records relevant to the antiterrorism and law enforcement mission of numerous Federal agencies, will be able to interface with the existing systems at DHS as well as other Federal, State, and local agencies?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR CHARLES K. EDWARDS

Question 1. What grade (A,B,C,D,F) would you give CBP, ICE, and USCIS in their development and implementation of major IT programs based on their ability to meet mission needs, cost, and schedule?

How would you rate DHS's performance in delivering IT systems against other Federal agencies?

Answer. Response was not received at the time of publication.

Question 2. What steps does DHS need to take to ensure IT programs supporting our border agents and immigration officers are efficient and effective moving forward?

Answer. Response was not received at the time of publication.