AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

EXAMINING CHALLENGES AND WASTED TAXPAYER DOLLARS IN MODERNIZING BORDER SECURITY IT SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

FEBRUARY 6, 2014

Serial No. 113–50

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

88–024 PDF WASHINGTON : 2014

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
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania
MARK SANFORD, South Carolina
VACANCY

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

VACANCY, *Staff Director*
MICHAEL GEFFROY, *Deputy Staff Director/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
LOU BARLETTA, Pennsylvania
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana, *Vice Chair*
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, *Subcommittee Staff Director*
DEBORAH JORDAN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

The Honorable Jeff Duncan, a Representative in Congress From the State of South Carolina, and Chairman, Subcommittee on Oversight and Management Efficiency:
Oral Statement 1
Prepared Statement 3
The Honorable Ron Barber, a Representative in Congress From the State of Arizona, and Ranking Member, Subcommittee on Oversight and Management Efficiency:
Oral Statement 14
Prepared Statement 16
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Prepared Statement 4

WITNESSES

Mr. David A. Powner, Director, Information Technology Management Issues, U.S. Government Accountability Office:
Oral Statement 6
Prepared Statement 7
Mr. Charles R. Armstrong, Assistant Commissioner, Office of Information and Technology, Customs and Border Protection, U.S. Department of Homeland Security:
Oral Statement 17
Prepared Statement 19
Mr. Thomas P. Michelli, Chief Information Officer, Immigration and Customs Enforcement, U.S. Department of Homeland Security:
Oral Statement 22
Prepared Statement 24

APPENDIX

Questions From Chairman Jeff Duncan for David A. Powner 43
Questions From Chairman Jeff Duncan for Charles R. Armstrong 43
Questions From Chairman Jeff Duncan for Thomas P. Michelli 44

EXAMINING CHALLENGES AND WASTED TAXPAYER DOLLARS IN MODERNIZING BORDER SECURITY IT SYSTEMS

Thursday, February 6, 2014

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

The subcommittee met, pursuant to call, at 10:02 a.m., in Room 311, Cannon House Office Building, Hon. Jeff Duncan [Chairman of the subcommittee] presiding.

Present: Representatives Duncan, Barber, and O'Rourke.

Also present: Representative Jackson Lee.

Mr. DUNCAN. The Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency will come to order.

I will say that the Ranking Member is on his way. Attending the prayer breakfast this morning, and he is running a few minutes behind. So hopefully he will get here before I finish my opening statement. If not, we may pause and allow him to have an opening statement as we go because I think that is so important.

But the purpose of this hearing is to examine DHS's attempt to modernize key information technology systems in use by the U.S. Immigration and Customs Enforcement and the U.S. Customs and Border Protection, specifically the TECS Modernization program.

I now recognize myself for an opening statement.

During the first half of this Congress, our subcommittee has had a laser focus on how the Department of Homeland Security spends tax dollars and how efficient and effective the Department's programs are during a time when the Nation faces unparalleled debt and fiscal challenges. As Chairman, I believe DHS must not only protect the homeland but do so in a fiscally responsible way.

Yet, time and again, hearing after hearing, we have examined findings from Congressional watchdogs that show a Department with little interest in safeguarding taxpayer dollars. From duplicative programs, broken trust by airport screener misconduct, and ill-disciplined acquisition practices, effective management of DHS has consistently taken a backseat.

Unfortunately, today's hearing is no different: Another program in the ditch, desperately needing a tow. Today we will examine DHS's efforts to modernize key information technology, or IT systems, used by the Customs and Border Protection and Immigration

and Customs Enforcement, specifically to TECS Modernization program.

Having visited the border agents along the Southwest Border and actually in Mr. Barber's district, I know first-hand how important it is for CBP officers and ICE agents to have all the tools that they need to secure the border. I know Ranking Member Barber shares that view.

For the CBP officer on the border, TECS is an integral tool to secure the homeland. The system helps officers determine the admissibility of over 900,000 visitors and approximately 465,000 vehicles into the country daily, share critical information with other Federal law enforcement agencies, and alert officers to possible threats entering the United States. That is important. Nine hundred thousand visitors, 465,000 vehicles—that is an immense challenge. I get that.

For the ICE agent, TECS is the primary investigative tool used to document and build cases for prosecution. A legacy system in operation since 1987, TECS has become increasingly difficult and expensive to maintain due to the system's antiquated technology and its inability to support the requirements needed by CBP and ICE personnel in the field.

Despite TECS' critical importance to our security, CBP and ICE have failed to manage the modernization program effectively. As the Government Accountability Office, or GAO, recently reported, the result has been wasted taxpayer dollars, missed deadlines, and delays in fielding enhancements to CBP officers and ICE agents.

For instance, despite some success deploying functional capabilities to secondary inspection locations, GAO reported that CBP has revised its schedule and cost estimates because they were unachievable. CBP expects to complete the project by 2016 for a total cost of about $700 million.

GAO further found that CBP did not develop a master schedule that links work activities to the overall project schedule, despite the fact that numerous projects are being deployed concurrently. While CBP contends the remainder of its concurrent program upgrades will be operational by the beginning of 2016, I am concerned that, minus a sound master schedule, the project could be further delayed and over-budget, which could snowball into CBP officers not having the tools that they need to do their job.

Of even more concern are ICE's failures. Due to unmet requirements, ICE is starting over on redeveloping its requirements after spending some $60 million and failing to produce any deliverables. After about 4 years and $60 million, ICE has little to show for its efforts, doesn't yet know the revised total cost or what the program will achieve. The stakes are high because of a looming 2015 deadline that, if not met, will force DHS to spend more taxpayer dollars to maintain the system currently in use.

In addition, I am concerned that, despite numerous management layers, DHS headquarters still let the program proceed. The DHS chief information officer has increased oversight and governance of information technology by reviewing DHS component programs and acquisitions over the years. Yet the Office of Program Accountability and Risk Management, two executive steering committees, and the Office of Chief Information Officer's Enterprise Business

Management Office all failed to adequately address escalating problems associated with the TECS Modernization effort.

Further, the lack of complete, timely, and accurate data from the components to DHS chief information officer, as reported by the GAO, negatively affected the Department's ability to make informed and timely decisions on the program.

Even the best governance framework won't improve outcomes if the senior DHS leaders don't have the discipline to enforce it. DHS must hold programs accountable, and if they fail, then we will hold DHS accountable.

With the speed with which technology advances today, it shouldn't take DHS 8 years to complete an IT project. Private-sector CEOs likely wouldn't tolerate such poor performance and management; neither should DHS. It is an affront to the American taxpayer, and it is time for DHS to do better.

[The statement of Chairman Duncan follows:]

STATEMENT OF CHAIRMAN JEFF DUNCAN

FEBRUARY 6, 2014

During the first half of this Congress, our subcommittee has had a laser focus on how the Department of Homeland Security (DHS) spends taxpayer dollars and how efficient and effective the Department's programs are during a time when the Nation faces unparalleled debt and fiscal challenges. As Chairman, I believe DHS must not only protect the homeland but do so in a fiscally responsible way. Yet time and again, hearing after hearing, we've examined findings from Congressional watchdogs that show a Department with little interest in safeguarding taxpayer dollars. From duplicative programs, broken trust by airport screener misconduct, and ill-disciplined acquisition practices, effective management of DHS has consistently taken a back seat. Unfortunately, today's hearing is no different . . . another program in the ditch desperately needing a tow.

Today, we will examine DHS's efforts to modernize key information technology (IT) systems used by Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE), specifically the TECS modernization program. Having visited with border agents along the Southwest Border, I know first-hand how important it is for CBP officers and ICE agents to have the tools they need to secure the border. I know Ranking Member Barber shares that view.

For the CBP officer on the border, TECS is an integral tool to secure the homeland. The system helps officers determine the admissibility of over 900,000 visitors and approximately 465,000 vehicles into the country daily, share critical information with other Federal law enforcement agencies, and alert officers to possible threats entering the United States. For the ICE agent, TECS is a primary investigative tool used to document and build cases for prosecution. A legacy system in operation since 1987, TECS has become increasingly difficult and expensive to maintain due to the system's antiquated technology and its inability to support the requirements needed by CBP and ICE personnel in the field.

Despite TECS's critical importance to our security, CBP and ICE have failed to manage the modernization program effectively. As the Government Accountability Office (GAO) recently reported, the result has been wasted taxpayer dollars, missed deadlines, and delays in fielding enhancements to CBP officers and ICE agents.

For instance, despite some success deploying functional capabilities to secondary inspection locations, GAO reported that CBP has revised its schedule and cost estimates because they were unachievable. CBP expects to complete the project by 2016 for a total cost of about $700 million. GAO further found that CBP did not develop a master schedule that links work activities to the overall project schedule, despite the fact that numerous projects are being developed concurrently. And while CBP contends the remainder of its concurrent program upgrades will be operational by the beginning of 2016, I am concerned that minus a sound master schedule, the project could be further delayed and over budget which could snowball into CBP officers not having the tools they need to do their job.

Of even more concern are ICE's failures. Due to unmet requirements, ICE is starting over on redeveloping its requirements after spending some $60 million and failing to produce any deliverables. After about 4 years and $60 million, ICE has little

to show for, doesn't yet know the revised total cost, or what the program will achieve. The stakes are high because of a looming 2015 deadline that if not met will force DHS to spend more taxpayer dollars to maintain the system currently in use.

In addition, I am concerned that despite numerous management layers, DHS headquarters still let the program proceed. The DHS chief information officer has increased oversight and governance of information technology by reviewing DHS component programs and acquisitions over the years. Yet the Office of Program Accountability and Risk Management; two Executive Steering Committees; and the Office of the Chief Information Officer's Enterprise Business Management Office all failed to adequately address escalating problems associated with the TECS modernization effort.

Further, the lack of complete, timely, and accurate data from the components to the DHS chief information officer as reported by the GAO negatively affected the Department's ability to make informed and timely decisions on the program. Even the best governance framework won't improve outcomes if senior DHS leaders don't have the discipline to enforce it. DHS must hold programs accountable. If they fail, then we will hold DHS accountable.

With the speed with which technology advances today, it shouldn't take DHS 8 years to complete an IT project. Private-sector CEOs likely wouldn't tolerate such poor performance and management. Neither should DHS. It's an affront to the American taxpayer and it's time DHS do better.

Mr. DUNCAN. So I will recognize the Ranking Member when he comes in. While we are waiting on him, let me just go ahead and remind Members of the subcommittee that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

FEBRUARY 6, 2014

Thank you, Chairman Duncan, for convening this hearing.

I also thank the witnesses for appearing today and look forward to hearing their testimony.

When the Department of Homeland Security was created in 2002, there was a merger of not only agencies and the people employed by those agencies, but also technology and the systems used by legacy agencies to keep our country safe and secure.

One such technology was TECS. As the largest law enforcement tool used throughout the United States, TECS is a vital component to our homeland security efforts.

It is used at the border to ensure that legitimate travelers and trade are welcomed into our country and terrorists, drugs, and weapons are prevented from entering the United States. It is also used away from the border by more than 20 Federal agencies to create and access terrorist "lookouts," track financial crimes, and disseminate intelligence reports.

Unfortunately, given the age of this system and the way that it is structured, it has become outdated, and, in some ways obsolete. Its inefficiency has at times hindered our border security efforts by increasing wait times and producing false positives that create further delay.

Like many legacy systems now in use at DHS, TECS is currently undergoing a modernization effort that by some calculations is expected to cost more than $1.5 billion. By all accounts, an improved TECS is well overdue; however, the Department's implementation is cause for serious concern.

For example, rather than having one program office, established at the Headquarters level, this major acquisition is being carried out by two separate components—Customs and Border Protection (CBP) and Immigrations and Customs Enforcement (ICE)—simultaneously.

As a result, we have two separate program offices, two separate program managers, two separate funding streams and the need for a limited acquisition workforce to conduct oversight over two separate major investments.

Under this structure, I am concerned that duplication, redundancy, and the inability for one hand to know what the other hand is doing.

Furthermore, both components continue to face challenges that further reduce my confidence in the management of this billion-dollar-plus acquisition.

CBP continues to be challenged by scheduling delays, and although it insists that the portions of TECS Modernization that have not been delivered will be ready by 2015, the program is still running without a master schedule and a clearly-defined time line for what will happen when.

ICE has made the disconcerting decision to halt its efforts after operating for years without established requirements, resulting in testing failures and the expenditure of $20 million developing a system that was ultimately of no use.

That is $20 million of scarce homeland security funds that can never be recovered that has simply "gone down the drain."

These issues and others have caused the Government Accountability Office in a recently-released report to state that: "After spending millions of dollars and over 4 years on TECS modernization, it is unclear when it will be delivered and at what cost."

Hopefully, today's witnesses can shed some light on how this effort can be put on a better track and inform this subcommittee on how much TECS modernization is expected to cost, when it will be delivered, and when Federal, State, and local law enforcement officials can stop relying on a 30-year-old, obsolete system while our security hangs in the balance.

I yield back the balance of my time.

Mr. DUNCAN. We are pleased to have a very distinguished panel of witnesses before us today on this important topic.

Let me remind the witnesses that their entire written statement will appear in the record. I will go ahead and introduce each of you first and then recognize you for your testimony.

Our first panelist is Mr. David Powner. He is the director of IT management issues at the U.S. Government Accountability Office. Mr. Powner is responsible for a large segment of GAO's information technology work, including systems development, IT investment management, health IT, and cyber critical infrastructure protection reviews. At GAO, Mr. Powner has led teams reviewing major IT modernization efforts at Cheyenne Mountain Air Force Station, the National Weather Service, the Federal Aviation Administration, and the IRS.

Our second panelist is Mr. Charles Armstrong. He is the assistant commissioner for the Office of Information and Technology at U.S. Customs and Border Protection. Mr. Armstrong's responsibilities include software development, infrastructure services and support, tactical communications, research and development functions, and IT modernization initiatives. Mr. Armstrong has led the office since June 2008. He manages a budget of $184 million and a workforce of about 6,000 Federal employees and contractors.

Prior to serving as assistant commissioner, Mr. Armstrong was DHS's deputy CIO, where he worked on the Department's IT initiatives for improving the agency's secure information-sharing capabilities. Mr. Armstrong has over 30 years of technology experience in the operations and management of IT.

Our third panelist is Mr. Thomas Michelli.

Did I pronounce that right?

He is the chief information officer for U.S. Immigration and Customs Enforcement, where he is the agency's top technology administrator and responsible for critical IT initiatives, modernizing IT systems, and providing IT solutions throughout ICE.

Prior to joining the Department, Mr. Michelli served as executive director of enterprise solutions for the Defense Logistics Agency. In the private sector, Mr. Michelli served as director of international IT operations and chief information officer for the real estate firm

Cushman & Wakefield. He also served as chief technology officer at General Dynamics Information Technology.

Folks, thank you for being here.

I will now go ahead and recognize Mr. Powner to testify. Keep in mind that if Mr. Barber comes in between testimonies, I will let you finish, but then we will recognize him for a statement.

So Mr. Powner can testify.

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

Mr. POWNER. Chairman Duncan, we appreciate the opportunity to testify this morning on DHS's efforts to improve its ability to secure our borders, prevent terrorism, and enhance our intelligence functions.

The primary system used for admitting persons to the United States and one of our Nation's most important law enforcement systems, known as TECS, provides CBP officers and ICE agents with critical information. This system has over 70,000 users, is accessed by 10 departments, interfaces with over 80 systems, including terrorist watch lists, and screens nearly 1 million visitors and 500,000 vehicles daily.

This system is in need of a major overhaul because it is expensive to maintain, does not quickly support mission requirements, and needs major functional improvements like enhanced searches and better algorithms to match names.

In 2008, CBP and ICE each pursued separate acquisitions to address these shortfalls. Collectively, these two acquisitions were to cost over $1.5 billion to build and operate. Mr. Chairman, we issued a report at your request last month on those acquisitions, which I will briefly summarize, starting with CBP.

CBP planned to deploy functionality in five separate increments and, to their credit, deployed the first increment related to enhanced secondary inspections at all air and sea ports in 2011 and land ports in 2013. The remaining four increments were to be deployed concurrently in 2015, but the program is being rebaselined for the second time in the past year, meaning that what will be delivered when and at what cost is changing.

When we issued our report, DHS was working on new cost and schedule estimates. We understand that DHS has a new requirements document, cost estimate, and program baseline that shows them achieving full operating capability now in 2016, and the lifecycle cost has dropped slightly to just below $700 million. CBP has spent over $225 million to date on this effort.

Turning to ICE, ICE planned to deploy an initial release in December 2013 and annual releases after that but in 2010 began experiencing technical problems that led to them deferring 3,000 of the 4,300 requirements for the first release. That is 70 percent of the first release being deferred. This led to a review that determined the system was not technically viable in June 2013, and the program decided to start over.

We understand there has been an independent technical assessment of the program and that a new cost estimate and baseline is expected in the April–May time frame. ICE reported only having

spent about $20 million on their program when we conducted our review, but today's testimony discloses that $64 million have been spent to date.

So what went wrong with the two acquisitions? Our report highlights two major areas: No. 1, poor fundamental program management; and, No. 2, ineffective governance. Both acquisitions put in place robust requirements management processes too late, and that was definitely more evident with the ICE program. In addition, both programs did not effectively escalate program risks in a timely or aggressive fashion. We thought CBP should have been addressing scheduling and contractor risks and ICE should have been identifying the requirements backlog and technical solution risks much better.

Regarding governance, multiple groups are in place to oversee these acquisitions: CBP and ICE each have an executive steering committee, the CIO performs monthly ratings on these acquisitions, and the under secretary for management oversees major acquisitions.

These governance bodies clearly were not getting complete information to assess programs risks, and their assessments were way too rosy. The under secretary's assessment for both acquisitions were deemed low-risk in July 2013. The latest CIO assessments were better, but not much, calling the CBP acquisition moderately low-risk and the ICE program medium-risk. It was quite clear during our review that the ICE program was high-risk at that time.

Moving forward, Mr. Chairman, both programs need to establish solid baselines so that Congress clearly knows what we are spending and what exactly is being delivered when to better support our CBP officers and ICE agents. Once these decisions are made and approved, DHS needs to tighten program management processes and executive-level governance practices to deliver needed improvements and to keep these acquisitions within their cost and schedule estimates.

This subcommittee's oversight will play a critical role in ensuring that the new approaches are focused on what is most needed, cost-justified, and delivered as soon as possible.

Mr. Chairman and Ranking Member Barber, thank you for your leadership on these critical acquisitions, and I would be pleased to respond to questions.

[The prepared statement of Mr. Powner follows:]

PREPARED STATEMENT OF DAVID A. POWNER

FEBRUARY 6, 2014

GAO HIGHLIGHTS

Highlights of GAO–14–3M42T, a testimony before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

DHS's border enforcement system, known as TECS, is the primary system for determining admissibility of persons to the United States. It is used to prevent terrorism, and provide border security and law enforcement, case management, and intelligence functions for multiple Federal, State, and local agencies. It has become increasingly difficult and expensive to maintain and is unable to support new mission requirements. In 2008, DHS began an effort to modernize the system. It is being managed as two separate programs by CBP and ICE.

In December 2013, GAO reported that DHS needed to strengthen its efforts to modernize these key enforcement systems. This statement summarizes that report. Specifically, it covers: (1) The scope and status of the two TECS Mod programs, (2) selected program management practices for TECS Mod, (3) the extent to which DHS is executing effective oversight and governance of the two TECS Mod programs, and (4) the importance of addressing our recommendations for improving DHS's development efforts.

What GAO Recommends

GAO is making no new recommendations in this statement. In its December 2013 report, GAO recommended that DHS improve its efforts to manage requirements and risk, as well as its governance of the TECS Mod programs. DHS agreed with all but one of GAO's eight recommendations, disagreeing with the recommendation about improving CBP's master schedule. GAO continues to believe improvements are necessary to validate schedule commitments and monitor progress.

BORDER SECURITY.—DHS NEEDS TO STRENGTHEN ITS EFFORTS TO MODERNIZE KEY ENFORCEMENT SYSTEMS

What GAO Found

The schedule and cost for the Department of Homeland Security's (DHS) border enforcement system modernization program known as TECS Mod that is managed by Customs and Border Protection's (CBP) continue to change; while the part managed in parallel by Immigration and Customs Enforcement (ICE) is undergoing major revisions to its scope, schedule, and cost after discovering that its initial solution is not technically viable. CBP's $724 million program intends to modernize the functionality, data, and aging infrastructure of legacy TECS and move it to DHS's data centers by 2016. To date, CBP has deployed functionality to improve its secondary inspection processes to air and sea ports of entry and, more recently, to land ports of entry in 2013. However, CBP is in the process of revising its schedule baseline for the second time in under a year. Further, CBP has not developed its master schedule sufficiently to reliably manage work activities or monitor program progress. These factors raise questions about the certainty of CBP's remaining schedule commitments. Regarding ICE's $818 million TECS Mod program, it is redesigning and replanning its program, having determined in June 2013 that its initial solution was not viable and could not support ICE's needs. As a result, ICE largely halted development and is now assessing design alternatives and is revising its schedule and cost estimates. Program officials stated the revisions will be complete in spring 2014. Until ICE completes the replanning effort, it is unclear what functionality it will deliver, when it will deliver it, or what it will cost to do so, thus putting it in jeopardy of not completing the modernization by its 2015 deadline.

CBP and ICE have managed many risks in accordance with some leading practices, but they have had mixed results in managing requirements for their programs. In particular, neither program identified all known risks, nor escalated them for timely management review. Further, CBP's guidance reflects most leading practices for effectively managing requirements, but important requirements development activities were underway before such guidance was established. ICE, meanwhile, operated without requirements management guidance for years, and its requirements activities were mismanaged, resulting in testing failures and delays. ICE issued requirements guidance in March 2013 that is consistent with leading practices, but it has not yet been implemented.

DHS's governance bodies have taken actions to oversee the two TECS Mod programs that are generally aligned with leading practices. Specifically, they have monitored TECS Mod performance and progress and have ensured that corrective actions have been identified and tracked. However, a lack of complete, timely, and accurate data have affected the ability of these governance bodies to make informed and timely decisions, thus limiting their effectiveness. Until these governance bodies base their performance reviews on timely, complete, and accurate data, they will be constrained in their ability to effectively provide oversight.

Chairman Duncan, Ranking Member Barber, and Members of the subcommittee: I am pleased to be here today to discuss the Department of Homeland Security's (DHS) border enforcement system, known as TECS.[1] TECS has been used since the 1980's for preventing terrorism, providing border security and law enforcement, and

[1] TECS was created as a system of the Customs Service, which was then a component within the Department of the Treasury. The term TECS initially was the abbreviation for the Treasury Enforcement Communications System. When the Customs Service became part of DHS under the Homeland Security Act, TECS became a DHS system, and thereafter has simply been known as TECS.

sharing information about people who are inadmissible or may pose a threat to the security of the United States, and today still provides traveler processing and screening, investigations, case management, and intelligence functions for multiple Federal, State, and local agencies. Over time, however; it has become increasingly difficult and expensive to maintain because of technology obsolescence and its inability to support new mission requirements. DHS estimates that TECS's licensing and maintenance costs are expected to be $40 million to $60 million per year in 2015.

In 2008 the Department initiated TECS Modernization (TECS Mod) to modernize existing system functionality, address known capability gaps, and move the program's infrastructure to DHS's new data centers. TECS Mod is managed as two separate programs working in parallel: U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) are each modernizing existing functionality specific to their respective roles and missions within the Department. Both programs had planned to be fully operational by September 2015.

In December 2013, we reported that DHS needed to strengthen its efforts to modernize these key border enforcement systems.[2] In that report, we issued multiple recommendations aimed at improving DHS's efforts to develop and implement its TECS Mod programs. My testimony today will summarize the results of that report. Specifically, I will cover: (1) The scope and status of the two TECS Mod programs, (2) selected CBP and ICE program management practices for TECS Mod, (3) the extent to which DHS is executing effective executive oversight and governance of the two TECS Mod programs, and (4) the importance of addressing our recommendations for improving DHS's development efforts.

The work on which my testimony is based was conducted from December 2012 to December 2013. Further details on the scope and methodology for the previously-issued report are available within that published product. In addition, we analyzed recently-received documentation from DHS on the status of the two TECS Mod programs. All work on which this testimony is based was performed 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

TECS is an information technology (IT) and data management system that supports DHS's core border enforcement mission. According to CBP, it is one of the largest, most important law enforcement systems currently in use, and is the primary system available to CBP officers and agents from other departments for use in determining the admissibility of persons wishing to enter the country. In addition, it provides an investigative case management function for activities carried out by ICE agents, including money-laundering tracking and reporting; telephone data analysis; and intelligence reporting and dissemination.

Over time, TECS has evolved into a multi-faceted computing platform that CBP describes as a system of systems. This mainframe-based system dates back to the 1980s and interfaces with over 80 other systems from within DHS, other Federal departments and their component agencies, as well as State, local, and foreign governments. It contains over 350 database tables, queries, and reports (e.g., querying law enforcement records to determine if a traveler appears on a terrorist watch list), and multiple applications (e.g., ICE's existing investigative case management system). CBP agents and other users access TECS via dedicated terminals. The system is managed by CBP's Office of Passenger Systems Program Office and is currently hosted at CBP's data center.

On a daily basis, the system is used by over 70,000 users and handles more than 2 million transactions—including the screening of over 900,000 visitors and approximately 465,000 vehicles every day. In addition, Federal, State, local, and international law enforcement entities use TECS to create and disseminate alerts and other law enforcement information about "persons of interest." Ten Federal departments and their numerous component agencies access the system to perform a part of their missions.

The current TECS system uses obsolete technology, which combined with expanding mission requirements, have posed operational challenges for CBP and others. For example, users may need to access and navigate among several different sys-

[2] GAO, *Border Security: DHS's Efforts to Modernize Key Enforcement Systems Could be Strengthened,* GAO–14–62 (Washington, DC: Dec. 5, 2013).

tems to investigate, resolve, and document an encounter with a passenger. In addition, CBP identified that TECS's search algorithms do not adequately match names from foreign alphabets. TECS's obsolescence also makes it difficult and expensive to maintain and support. Specifically, DHS estimates that TECS's licensing and maintenance costs are expected to be $40 million to $60 million per year in 2015.

In 2008, DHS initiated efforts to modernize TECS by replacing the mainframe technology, developing new applications, and enhancing existing applications to address expanding traveler screening mission needs, improving data integration to provide enhanced search and case management capabilities, and improving user interface and data access. DHS's plan was to migrate away from the existing TECS mainframe by September 2015 to avoid significantly escalating support costs. The modernization effort is managed by two program offices—one at CBP and the other at ICE—working in parallel, with each having assumed responsibility for modernizing the parts of the system aligned with their respective missions.

CBP expects that its modernization efforts will yield certain improvements over the existing system, including the following.

- Enhancements to TECS's search algorithms to better match names from foreign alphabets; address gaps in current processes that could result in missing a person of interest. This includes an improved ability for inspectors to update information on travelers at air and sea borders at the time of encounter.
- Improvements in the flow and integration of data between CBP and its partner agencies and organizations. This is intended to aid the agency's inspectors by providing timely, complete, and accurate information about a traveler during the secondary inspection process.

CBP planned to develop, deploy, and implement these capabilities incrementally across five projects from 2008 to 2015.

- *Secondary Inspection*.—This project is to support processing of travelers referred from primary inspection for either enforcement or administrative reasons. According to CBP, this project's functionality was fully deployed to all air and sea ports of entry in 2011, and was fully deployed to all land ports of entry in 2013.
- *High Performance Primary Query and Manifest Processing*.—This project is intended to improve TECS data search results in order to expedite the processing of manifests from individuals traveling to the United States on commercial or private aircraft, and commercial vessels. It is to be fully operational by March 2015.
- *Travel Document and Encounter Data*.—This project is intended to improve CBP's ability to query and validate travel documentation for both passengers and their means of conveyance. It is to be fully operational by March 2015.
- *Lookout Record Data and Services*.—This project is intended to improve the efficiency of existing data screening and analyses capabilities. It is to be fully operational by March 2015.
- *Primary Inspection Processes*.—This project is intended to modernize the overall inspection process and provide support for additional or random screening and communication functions. It is to be fully operational by March 2015.

As part of each of these projects, CBP is also developing an on-line access portal, called TECS Portal, for authorized users to access information remotely using a modern web browser, along with security and infrastructure improvements, and the migration of data from the current system to databases in the new environment at the DHS data center. Ultimately, TECS Mod functionality is to be deployed to over 340 ports of entry across the United States.

ICE's TECS Mod effort is to focus on specific law enforcement and criminal justice functions; tools to support ICE officers' collection of information, data analysis, and management operations; enhanced capabilities to access and create data linkages with information resources from elsewhere in DHS and other law enforcement agencies; and capabilities to better enable investigative and intelligence operations, corresponding management activities, and information sharing. Similar to CBP, ICE intended to deliver functionality in multiple phases:

- *Phase 1: Core Case Management*.—This phase was to encompass all case management functions currently residing in the existing TECS system. ICE planned to develop and deploy these functions in three releases beginning in 2009, and was scheduled to deploy Release 1 by December 2013, with additional releases following about every 12 months, in order to achieve independence from the existing TECS platform by September 2015. Specific capabilities that were to be provided include:
  - Basic electronic case management functions, including opening cases, performing supervisory review of cases, and closing cases within the system;

- Development of reports for use as evidentiary material in court proceedings arising from ICE agents' investigations;
- Maintenance of records relating to the subjects of ICE investigations; and,
- Audit capabilities to monitor system usage.

- *Phase 2: Comprehensive Case Management*.—This phase was to expand on the features delivered as part of Phase 1 and to be delivered in four increments starting in 2016, with an estimated completion date in fiscal year 2017.

DHS Oversight of Major IT Programs

DHS's Office of the Chief Information Officer (CIO) and the Office of the Under Secretary for Management are to play key roles in overseeing major acquisition programs like TECS Mod. For example, the CIO's responsibilities include setting Departmental IT policies, processes, and standards; and ensuring that IT acquisitions comply with DHS IT management processes, technical requirements, and approved enterprise architecture, among other things. Within the Office of the CIO, the Enterprise Business Management Office has been given primary responsibility for ensuring that the Department's IT investments align with its missions and objectives. As part of its responsibilities, this office periodically assesses IT investments like TECS Mod to gauge how well they are performing through a review of program risk, human capital, cost and schedule, and requirements.

In October 2011, DHS's under secretary for management established the Office of Program Accountability and Risk Management. This office is to ensure the effectiveness of the overall program execution governance process and has the responsibility for developing and maintaining DHS's Acquisition Management Directive.[3] It is also responsible for periodically providing independent assessments of major investment programs—called Quarterly Program Accountability Reports—as well as identifying emerging risks and issues that DHS needs to address.

In December 2011, DHS introduced a new initiative to improve and streamline the Department's IT program governance. This initiative established a tiered governance structure for program execution. Among other things, this new structure includes a series of governance bodies, each chartered with specific decision-making responsibilities for each major investment. Among these are executive steering committees, which serve as the primary decision-making authorities for DHS's major acquisition programs. ICE chartered its steering committee in September 2011 and it has been meeting since December of that year. CBP established its steering committee in early 2013 and it held its first meeting in February.

SCHEDULE AND COST OF BOTH TECS MODERNIZATION PROGRAMS ARE UNCLEAR

CBP has begun delivering functionality to its users; however, its schedule and cost commitments continue to change and are still being revised. Specifically, CBP intends to modernize the functionality, data, and aging infrastructure of legacy TECS and move it to DHS's data centers. CBP plans call for developing, deploying, and implementing these capabilities in five distinct projects that are to be delivered by 2015. To date, CBP has completed one of these five projects, having completed its deployment of functionality to improve its secondary inspection processes to air, sea, and land ports of entry in 2013. CBP is in the process of revising its schedule baseline for the second time in under a year, making it unclear when the program ultimately intends to deliver needed functionality.

Exacerbating this situation is the fact that CBP has not developed its master schedule sufficiently to effectively manage work activities or monitor the program's progress.[4] Specifically, the program has not linked all the work activities in the individual project schedules, nor has it defined dependencies that exist between projects in the master schedule: Approximately 65 percent of CBP's remaining work activities were not linked with other associated work activities. Thus, any delays early in the schedule do not "ripple" (i.e., transmit delays) to activities later in the schedule, meaning that management will be challenged to determine how a slip in the completion date of a particular task may affect the overall schedule. In our report, we also noted that CBP had not yet developed a detailed schedule for signifi-

[3] The Acquisition Management Directive provides the overall policy and structure for acquisition management within the Department and is used in planning and executing acquisitions.

[4] Our research has identified, among other things, that a key element associated with a complete and useful schedule or roadmap for executing a program such as TECS Mod is to logically sequence all work activities so that start and finish dates of future activities, as well as key events based on the status of completed and in-progress activities, can be reliably forecasted. See GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules, Exposure Draft,* GAO–12–120G (Washington, DC: May 2012).

cant portions of the program. CBP reported in January 2014 that it has now completed that work.

Program officials stated these deficiencies existed because the program has only two staff members with skills needed to properly develop and maintain the schedules, and that fully documenting all the dependencies would be time-consuming, and in their view, not sufficiently important to warrant the additional resources necessary to complete them. However, without a complete and integrated master schedule that includes all program work activities and associated dependencies, CBP is not in a position to accurately determine the amount of time required to complete its TECS modernization effort and develop realistic milestones.

The program's cost estimates have also changed as a result of rebaselining and are also being revised. The program's baselined life-cycle cost estimate[5] was approximately $724 million, including $31 million for planning management, $212 million for development, and $481 million for operations and maintenance. As of August 2013, the program reported that it had expended about $226 million. However, as previously stated, the program is in the process of revising its estimate, and thus, it is unclear how much it will cost to complete the program. In January 2014, CBP reported that its revised estimates should be approved internally and submitted to DHS for its approval by the end of January 2014.

Meanwhile, ICE is replanning its $818 million TECS Mod program, having determined in June 2013 that the system under development was not technically viable and could not support ICE's needs—this coming after having already reduced the scope of its initial program installment by about 70 percent due to protracted technical difficulties and schedule delays. Specifically, ICE determined that, after spending approximately $19 million, the system under development could not be fielded as part of ICE's eventual solution due to on-going technical difficulties with the user interface, access controls, and case-related data management. Instead of continuing with the existing technical solution, the program manager explained that ICE would scrap a significant portion of the work done to date and start over. As a result, ICE halted most development work in June 2013 and has since been assessing different design and technical alternatives. In January 2014, ICE reported that it had rebaselined its program requirements and that it anticipates having its revised cost and schedule estimates finalized this coming spring. Nevertheless, given the time lost in developing the current technical solution, as well as the already-reduced program scope, ICE cannot say what specific features it will release to users, when this functionality will be delivered, or how much such efforts will cost. As such, ICE is at significant risk of not achieving independence from the existing system by 2015.

TECS MODERNIZATION'S RISK MANAGEMENT IS GENERALLY CONSISTENT WITH LEADING PRACTICES, BUT REQUIREMENTS MANAGEMENT HAS HAD MIXED RESULTS

Both CBP and ICE implemented risk management practices that are generally—though not fully—consistent with leading practices, and both had mixed results in managing program requirements. Of four leading practices associated with effective risk management, CBP and ICE each fully implemented two (establishing documented risk management processes and assigning roles and responsibilities for managing risks) and partially implemented the other two (capturing all known risks and managing risk mitigation efforts through to completion). Specifically, neither program identified all known risks, nor escalated them for timely review by senior management.

Further, of four leading practices for managing program requirements, CBP fully implemented three (establishing a requirements management process, assigning roles and responsibilities for requirements development and management activities, and defining a change control process) while partially implementing the one other (eliciting user needs). However, CBP began executing key requirements activities before such practices were established, and as a result, CBP officials reported that some TECS Mod requirements were not as consistently well-formed or detailed because their process during that time lacked rigor. In ICE's case, management weaknesses and the lack of appropriate guidance for the program's requirements management process led to technical issues, testing failures, and ultimately, the deferral and/or deletion of about 70 percent of the program's original requirements. ICE issued new requirements guidance for the program in March 2013 that is consistent with leading practices, but has yet to demonstrate that these have been fully implemented.

---

[5] This estimate is in the program's November 2012 acquisition program baseline.

DHS'S GOVERNANCE BODIES HAVE TAKEN ACTIONS ALIGNED WITH LEADING PRACTICES, BUT INCOMPLETE AND INACCURATE DATA HAVE LIMITED THEIR EFFECTIVENESS

DHS's governance bodies have taken actions to oversee the two TECS Mod programs that are generally aligned with leading practices. Specifically, they have monitored TECS Mod performance and progress and have ensured that corrective actions have been identified and tracked. However, a lack of complete, timely, and accurate data have affected the ability of these governance bodies to make informed and timely decisions, thus limiting their effectiveness. For example:

- *Steering committees*.—In an April 2013 meeting, the CBP program manager briefed the steering committee on its target milestone dates; even though the agency told us a month later that it had not fully defined its schedule, raising questions about the completeness and accuracy of the proposed milestone dates upon which the committee based its oversight decisions.
- *The Office of the CIO*.—In its most recent program health assessments, the Enterprise Business Management Office partially based its rating of moderately low-risk on CBP's use of earned value management; however, the program manager stated to us that the CBP program is not utilizing earned value management because neither it nor its development contractor had the capability to do so. Similarly, even though ICE had not reported recent cost or schedule data for its program—an issue that may signal a significant problem—the Office of the CIO rated ICE's program as medium-risk. The reliance on incomplete and inaccurate data raises questions about the validity of the risk ratings.
- *Office of Program Accountability and Risk Management*.—In the July 2013 Quarterly Program Accountability Report, DHS's Office of Program Accountability and Risk Management rated both TECS Mod programs as high-value with low risk. However, CBP's low-risk rating was based in part on the quality of the program's master schedule and acquisition program baseline; however, as we stated earlier, problems with the agency's schedule raise questions about the validity and quality of those milestones. Further, the low-risk rating it issued for ICE was based, in part, on its assessment of ICE's performance between April and September 2012, which rated the program's cost performance with the lowest possible risk score. Yet, during that same time period, program documents show that ICE TECS Mod's cost and schedule performance was declining and varied significantly from its baseline. For example, program documents show that, as of June 2012, ICE TECS Mod had variances of 20 percent from its cost baseline and 13 percent from its schedule baseline.

  Moreover, the Quarterly Program Accountability Report is not issued in a timely basis, and as such, is not an effective tool for decision-makers. For example, the most recent report was published on July 7, 2013, over 9 months after the reporting period ended and therefore did not reflect that, since then, ICE has experienced the issues with its technical solution described earlier in this report. As discussed, these issues have caused the program to halt development and replan its entire acquisition. Consequently, the newly-issued report is not reflective of ICE's current status, and thus is not an effective tool for management's use in providing oversight.

Until these governance bodies base their reviews of performance on timely, complete, and accurate data, they will be limited in their ability to effectively provide oversight and to make timely decisions.

IMPLEMENTATION OF RECOMMENDATIONS COULD IMPROVE DHS'S EFFORTS TO DEVELOP AND IMPLEMENT ITS TECS MOD PROGRAMS

In our report, we made several recommendations to improve DHS's efforts to develop and implement its TECS Mod programs. Specifically, we recommended that the Secretary of Homeland Security direct the CBP commissioner to: (1) Develop an integrated master schedule that accurately reflects all of the program's work activities, as well as the timing, sequencing, and dependencies between them; (2) ensure that all significant risks associated with the TECS Mod acquisition are documented in the program's risk and issue inventory—including acquisition risks mentioned in our report—and are briefed to senior management, as appropriate; (3) revise and implement the TECS Mod program's risk management strategy and guidance to include clear thresholds for when to escalate risks to senior management, and implement as appropriate; and (4) revise and implement the TECS Mod program's requirements management guidance to include the validation of requirements to ensure that each is unique, unambiguous, and testable. In January 2014, CBP provided documentation that it had taken steps to begin addressing the second, third, and fourth recommendations.

We further recommended that the Secretary of Homeland Security direct the Acting Director of ICE to: (1) Ensure that all significant risks associated with the TECS Mod acquisition are documented in the program's risk and issue inventory—including the acquisition risks mentioned in our report—and briefed to senior management, as appropriate; (2) revise and implement the TECS Mod program's risk management strategy and guidance to include clear thresholds for when to escalate risks to senior management, and implement as appropriate; and (3) ensure that the newly-developed requirements management guidance and recently revised guidance for controlling changes to requirements are fully implemented.

We also recommended that the Secretary of Homeland Security direct the under secretary for management and acting chief information officer to ensure that data used by the Department's governance and oversight bodies to assess the progress and performance of major IT acquisition programs are complete, timely, and accurate.

DHS concurred with all but one of our recommendations, disagreeing with the recommendation regarding the weaknesses in CBP's schedule. In response, DHS stated that CBP's scheduling efforts for TECS Mod were sound. However, given the weaknesses in CBP's master schedule, we continue to believe that management will be unable to determine how a slip in the completion date of a particular task may affect the overall project or program schedule, and thus, absent any changes, continuing to use it as a tool to track progress will remain ineffective.

In conclusion, after spending nearly a quarter billion dollars and over 4 years on its two TECS Mod programs, it remains unclear when DHS will deliver them and at what cost. While CBP's program has delivered one of the five major projects that comprise the program, its commitments are being revised again and the master schedule used by the program to manage its work and monitor progress has not been fully developed. Moreover, ICE's program has made little progress in deploying its system, and is now completely overhauling its original design and program commitments, placing the program in serious jeopardy of not meeting the 2015 deadline and delaying system's deployment. The importance of having updated cost and schedule estimates for both the CBP and ICE programs cannot be understated, as this important management information will provide Congress and DHS with visibility into the performance of these vital border security investments. Further, while both agencies have defined key practices for managing risks and requirements, it is important that the programs fully implement these critical practices to help ensure that they deliver the functionally needed to meet mission requirements and minimize the potential for additional costly rework. Finally, until DHS's governance bodies are regularly provided complete and accurate data for use in their performance monitoring and oversight duties, their decisions may be flawed or of limited effectiveness.

Chairman Duncan, Ranking Member Barber, and Members of the subcommittee, this concludes my statement. I would be happy to answer any questions at this time.

Mr. DUNCAN. Yeah. Thank you, Mr. Powner.

We are going to pause, and I am going to recognize the gentleman from Arizona, Mr. Barber, the Ranking Member, for his opening statement.

Mr. BARBER. Well, good morning. I apologize for being late. All the streets get closed down, you know, when the President is moving around. So I just came from the National Prayer Breakfast and ran a little bit late, so I appreciate your indulgence on that.

I want to thank the Chairman for convening this hearing on a very important topic. We frequently talk here about the many systems that are part of the infrastructure at DHS, and today we are going to be talking about one that is critical and on which myself and the Chairman wrote a letter last month expressing our concerns about where we are.

Technology, infrastructure, and personnel are obviously three key elements in securing our borders and ensuring the safe and legal entry of people and goods into the United States.

I can tell you, from my perspective as 1 of the 9 Members from a Southwest Border district, that we have significant problems in

processing, expediting people coming into the country, particularly at our ports of entry in Nogales, which is a neighboring district, in my own district at the Douglas port of entry, partly due to the lack of numbers of Customs agents, but, also, I believe, due to the cumbersome nature of the technology that is used by our personnel in DHS to process people into the country.

Employees from U.S. Customs and Border Protection and ICE utilize, as you know, many different types of technology to carry out their mission. One of the largest IT systems currently in use is TECS, which is the primary border enforcement system supporting the screening of travelers entering the United States.

As you also know, the use of TECS goes well beyond CBP and ICE. It is currently used by over 20 Federal agencies, resulting in over 70,000 users conducting more than 2,000 transactions each and every day.

According to the CBP, which maintains TECS, it is the largest and most important law enforcement system currently in use by the Federal, State, and local law enforcement agents. It supports law enforcement lookouts, border screening, reporting for CBP primary and secondary inspection processes, money-laundering tracking, and reporting telephone and data analysis and intelligence reporting and dissemination. In sum, TECS is a vital asset to homeland security.

However, TECS is a legacy system that has been plagued with problems based upon both the age of the system and the outdated and, I would say, obsolete technology. As a result, the Department of Homeland Security is in the process of modernizing this 34-year-old border security tool through a multi-billion-dollar project known as TECS Mod. Given the importance of TECS and its widespread use throughout the law enforcement community at every level, I support the modernization and look forward to the day when it can actually be used with speed, efficiency, and reduced likelihood of false positives, which are also frequent.

Unfortunately, 4 years after beginning the TECS Mod, ICE is not much closer to developing a solution than it was on Day 1. Not only that, but CBP is still unable to determine its costs or schedule with sufficient detail. Furthermore, DHS's management of this project and the lack of stated requirements have led to the waste of millions of dollars of scarce Homeland Security funds—not very good stewardship of the taxpayers' money.

This concerns me because, as Ranking Member of this subcommittee, it is my responsibility, as it is all of our responsibilities, to ensure that the Department is spending taxpayer dollars efficiently and that its programs are actually doing what they are supposed to do and are keeping southern Arizonans and all Americans safe. Ultimately, the Department of Homeland Security is at risk of spending an additional $45 million to $60 million per year to maintain the aging system due to its outdated technology and exorbitant maintenance costs.

CBP is the Nation's largest law enforcement entity, and its thousands of law enforcement officials or agents across the United States rely on this system. Yet they rely on it in order to get their jobs done and keep us safe from harm, and it just doesn't work very well.

Our Border Patrol agents and Customs officers and other border security officials in the field are doing their part every single day to keep our country safe and secure, and we owe it to these front-line personnel to provide them with the technological tools they need to carry out their mission.

At present, TECS Mod is being managed under the direction of two separate program offices within DHS: ICE and CBP. Although we have been advised that these offices coordinate—and the initial decision may have made sense on paper, to divide the mission—I am very concerned that this decision has and will result in duplication, unnecessary costs, and uneven results, which ultimately affect the end-user.

When you put two separate components in charge of the same program, it is difficult to determine who should be held accountable. When more than one person is in charge, then essentially no one is in charge. This could lead to jurisdiction conflict or, worse, the inability to track accountability.

According to the GAO, the schedule and costs of both programs are still unclear, making it much more difficult for those who rely on TECS to do their jobs. CBP states that the project will be completed in 2015, but the GAO report casts doubt on that as a possibility. ICE cannot determine the date because it has halted all work on TECS until an independent contractor can determine the life-cycle costs and the necessary requirements. As a result, the 2015 completion date is in serious doubt.

In sum, Mr. Chairman, the Department has work to do to turn this effort around and put it on the right track. I look forward to hearing both from CBP and ICE on how they plan to move TECS Mod forward effectively and efficiently, including how they will define key requirements and identify and manage risks and accurately estimate the completion date for full modernization. This is essential to our Nation and to the mission of the Department.

Thank you, Mr. Chairman. I yield back.

[The statement of Ranking Member Barber follows:]

STATEMENT OF RANKING MEMBER RON BARBER

FEBRUARY 6, 2014

Technology, infrastructure, and personnel are three key elements to securing our borders and ensuring the safe and legal entry of people and goods into the United States.

Employees from the U.S. Customs and Border Protection (CBP) and Immigrations and Customs Enforcement (ICE) utilize many different types of technology to carry out their mission. One of the largest IT systems currently in use is TECS, which is the primary border enforcement system supporting the screening of travelers entering the United States.

The use of TECS goes well beyond CBP and ICE. TECS is currently accessed by over 20 Federal agencies; resulting in over 70,000 users conducting more than 2,000 transactions each and every day. According to CBP, which maintains TECS, it is the largest, most important law enforcement system currently in use by Federal, State, and local law enforcement agents.

It supports law enforcement "lookouts," border screening, reporting for CBP's primary and secondary inspection processes, money-laundering tracking and reporting, telephone and data analysis, and intelligence reporting and dissemination.

In sum, TECS is a vital asset to homeland security. However, TECS is a legacy system that has been plagued with problems based on the age of the system and its outdated technology.

As a result, the Department of Homeland Security is in the process of modernizing this 34-year-old border security tool, through a multi-billion dollar project known as TECS Mod.

Given the importance of TECS and its widespread use throughout the law enforcement community at every level, I support its modernization and look forward to the day when it can be used with speed, efficiency, and a reduced likelihood of false positives.

Unfortunately, 4 years after the beginning of TECS Mod, ICE is not much closer to developing a solution than it was on Day 1. Not only that, but CBP is still unable to determine its costs or schedule with sufficient detail.

Furthermore, DHS's management of this project and the lack of stated requirements have led to the waste of millions of scarce homeland security funds.

This concerns me because, as Ranking Member of this subcommittee, it is my responsibility to ensure that the Department is spending taxpayer dollars efficiently and that its programs are actually doing what they were intended to do and are keeping Southern Arizonans safe.

Ultimately, the Department of Homeland Security is at risk of spending an additional $45 to $60 million per year to maintain the aging system due to its outdated technology and exorbitant maintenance costs.

CBP, the Nation's largest law enforcement entity and its thousands of law enforcement agents across the United States rely on this system. They rely on it in order to do their jobs and keep us safe from harm.

Our Border Patrol agents and Customs officers and other border security officials in the field are doing their part to keep our country secure. We owe it to these frontline personnel to provide them the technological tools they need to carry out their mission.

At present, TECS Mod is being managed under the direction of two separate program offices—one at ICE and the other at CBP.

Although we have been advised that these offices coordinate and the initial decision may have made sense "on paper," I am concerned that this decision will result in duplication, unnecessary costs, and uneven results, which will ultimately affect the end-user.

When you put two separate components in charge of the same program, it is difficult to determine who should be held accountable for its results.

This could lead to jurisdiction conflict or worse, the inability to track accountability.

According to GAO, the schedule and cost for both programs are unclear, making it more difficult for those who rely on TECS to do their jobs. CBP states that the project will be complete in 2015, but GAO doubts that is possible.

ICE cannot determine a date because it has halted all work on TECS until an independent contractor can determine the life-cycle costs and the necessary requirements. As a result, the 2015 is in doubt.

In sum, the Department has work to do to turn this effort around and put it on the right track. I look forward to hearing from both CBP and ICE on how they plan to move TECS Mod forward, including how they will define key requirements, identify and manage risks, and accurately estimate a completion date for full modernization.

Mr. DUNCAN. I thank the Ranking Member.

We will go ahead and get back on track. I will recognize Mr. Armstrong for his testimony for 5 minutes.

STATEMENT OF CHARLES R. ARMSTRONG, ASSISTANT COMMISSIONER, OFFICE OF INFORMATION AND TECHNOLOGY, CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ARMSTRONG. Good morning, Chairman Duncan, Ranking Member Barber, and distinguished Members of the subcommittee. Thank you for the opportunity to appear before you to discuss U.S. Customs and Border Protection's efforts to modernize our aging information technology systems. I appreciate the subcommittee's leadership and your continued efforts to support the security of the American people.

Today I will discuss efforts we are making at CBP to continue effective delivery, within budget, of our TECS Modernization program.

TECS is a vital border security system supporting the vetting of travelers entering the United States who may be inadmissible or may pose a threat. TECS provides for the creation and query of lookout records and has more than 70,000 users from over 20 Federal agencies. Approximately 1 million travelers a day are vetted through TECS when entering the United States.

TECS is over 25 years old and uses data technology that is difficult to enhance and expensive to maintain. As part of an overarching strategy, TECS is migrating to a new enterprise architecture that will provide a solid foundation for the future, enhance capabilities, maintain high performance and availability, and align with other DHS modernization activities.

CBP began its TECS Mod effort in fiscal year 2008. TECS Mod functionality is concurrently and incrementally developed and deployed through five projects that focus on major functional areas.

CBP's TECS Mod effort is led by a program management office that has successfully delivered other high-profile border security systems. I chair the CBP TECS Modernization Executive Steering Committee, which provides program oversight and monitors cost, schedule, performance, and risk-management activities. The committee includes representation from CBP, ICE, and DHS offices.

I also hold monthly program management reviews and regular meetings with Mr. Michelli to provide additional oversight and coordination of the TECS Modernization activities. CBP and ICE program staffs meet frequently for detailed collaboration on the program.

CBP TECS Modernization has delivered functionality in four of the five projects. Secondary inspection has been fully deployed to all ports of entry. Officers have better information available to determine admissibility, spent less time navigating multiple screens and more time focusing their attention on the traveler.

CBP has also deployed a modernized query engine for Advance Passenger Information and for primary at air and sea ports. The modernized query provides a fast response to lookout record queries, informing officers if a traveler is of interest to CBP or other Federal agencies. TECS portal enhanced queries of lookout records, cross-data, and travel documents.

Because of the budget uncertainty during fiscal year 2013, the final TECS Modernization project primary inspection process, PIP, was paused. As a result, the TECS Modernization schedule was revised to restart the PIP in late second quarter of 2014 and move the program completion date from the end of fiscal year 2015 to mid-fiscal year 2016.

GAO's recent report contained four recommendations for CBP. CBP concurred with and has already implemented three of the recommendations concerning risk and requirements management. CBP did not concur with GAO's recommendation on our schedule process. I believe our established process has proven effective and aligns with our continuing effort to move to agile development.

The CBP TECS Modernization program has stayed within budget since it began in 2008 and has made significant progress, achieved

many milestones, and the program is in good overall health. Mr. Michelli and I are committed to the successful delivery of the program.

I thank you for the opportunity to testify today, and I look forward to answering your questions.

[The prepared statement of Mr. Armstrong follows:]

PREPARED STATEMENT OF CHARLES R. ARMSTRONG

FEBRUARY 6, 2014

Chairman Duncan, Ranking Member Barber, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you on behalf of the dedicated men and women of U.S. Customs and Border Protection (CBP) to discuss our efforts to modernize aging information technology systems in support of our border security mission. We appreciate the subcommittee's leadership and your continued efforts to ensure the security of the American people.

As the unified border security agency of the United States, CBP is responsible for securing our Nation's borders while facilitating the flow of legitimate international travel and trade that is so vital to our Nation's economy. Within this broad responsibility, our priority mission remains to prevent terrorists and terrorist weapons from entering the United States. Today, I will discuss efforts we are making at CBP to continue effective delivery, within budget, of TECS Modernization, one of our key border security systems to support the missions of CBP, DHS, and other Federal law enforcement agencies.

BACKGROUND

TECS (no longer an acronym) is a key border enforcement system supporting the vetting of travelers entering the United States and the requirements of other Federal agencies used for law enforcement and immigration benefit purposes. TECS supports the sharing of information about people who are inadmissible or may pose a threat to the security of the United States through the creation and query of "lookout records." TECS is used by more than 70,000 users, including users from more than 20 Federal agencies that use TECS in furtherance of their missions. TECS receives and processes traveler manifests from carriers and supports primary and secondary inspections for almost a million travelers and almost half a million vehicles at United States ports of entry (POEs) each day. TECS not only collects and creates border security information, but also shares that data with other systems and agencies. TECS also provides access to National Criminal Information Center (NCIC) and the International Justice and Public Safety Network (Nlets), as appropriate. TECS provides security and privacy controls to ensure users can only run transactions and access data to which they are authorized. TECS also includes extensive auditing of user actions for internal control purposes.

A typical "TECS Check" regarding a particular individual provides authorized users information on:

- Lookout records;
- Entries into and exits from the United States;
- Previous secondary inspections; and
- NCIC wants and warrants.

Because TECS is over 25 years old and uses dated architecture and technology that are difficult to enhance and expensive to maintain, TECS is migrating to a new enterprise architecture that will provide a solid foundation for the future, enable enhanced capabilities, maintain high performance and availability, and align with other DHS modernization activities. The program provides for highly-scalable functionality that meets constantly-emerging user requirements.

The modernization of the legacy TECS system is being accomplished through two separate but coordinated programs, one within CBP and the other within U.S. Immigration and Customs Enforcement (ICE). Each is funded and being executed separately in support of each agency's mission requirements. While both modernization programs remain focused on continued support of each agency's unique mission, both programs coordinate closely on common interests regarding planning, development, and data migration efforts.

CBP'S TECS MOD PROGRAM

CBP began its 8-year TECS Modernization or "TECS Mod" efforts in fiscal year 2008. A specific challenge to CBP's modernization effort is that modifications cannot

interrupt existing TECS functionality or availability. CBP's TECS system must be available to support border crossing operations 24 hours a day, 7 days a week. The need for high availability requires redundant hardware and failover processes to allow system maintenance with little or no interruption to end users of the system.

CBP's TECS Mod program is transitioning functionality incrementally with five projects, focusing on major functional areas to decrease risk and to continue providing existing capabilities to the end-user until modernization is complete. In addition to the five functional area projects, CBP TECS Mod also includes two overarching efforts to address infrastructure and security. The program includes migration of data from the legacy source system to the target databases, developing services for interfaces, and deploying a modernized web-based user interface (portal) to support TECS on-line users, ensuring compliance with security and privacy policies. The five functional area projects are:

- *Secondary Inspection (SI).*—This project supports processing of travelers referred from primary inspection and creates a modernized graphical user interface.
- *High Performance Primary Query and Manifest Processing (HPPQ).*—This project focuses on modernizing services and functionalities essential for primary inspection (person/vehicle) query functions. HPPQ also modernizes Advance Passenger Information System (APIS) receipt and processing of arriving and departing international traveler manifests.
- *Travel Document and Encounter Data (TDED).*—This project manages travel document data from the Department of State, U.S. Citizenship and Immigration Services, and State, Provincial, and Tribal governments. TDED also modernizes the way encounter data, which include person and vehicle crossing (entry/exit) data, I–94 arrival/departure data, and Currency and Monetary Instrument Report data, are made available for TECS on-line users and primary and secondary inspections.
- *Lookout Record Data and Screening Services (LRDS).*—This project will modernize the creation, maintenance, and query of lookout records for on-line users and interfaces with other systems. LRDS will also provide TECS data query capabilities and services to the law enforcement community via system-to-system interfaces or services. Additionally, the LRDS project will support current query capabilities for DHS component users with authorization to access NCIC, Nlets, and criminal history information.
- *Primary Inspection Processes (PIP).*—This project will modernize primary inspections (Air, Sea, and Land) user interfaces, services and processes. PIP will also modernize current Alternate Inspection (AI) processing which includes any inspection that is not conducted at an air, sea, vehicle, or pedestrian primary booth.

Program Governance and Oversight

The CBP TECS Modernization Executive Steering Committee (ESC) provides oversight of the TECS modernization effort. As CBP's chief information officer and Office of Information and Technology (OIT) assistant commissioner, I chair the ESC, which includes members from CBP offices; DHS's under secretary for science and technology, chief information officer, and chief financial officer; representatives from stakeholder groups; and ICE's TECS Mod program manager. The ESC, which meets every 2 months, monitors the program's cost, schedule, and performance, reviews risk management mitigation activities, and ensures corrective actions are identified.

Additional oversight and governance of CBP's TECS Mod program is provided by existing policies and guidance from DHS's Office of the Chief Information Officer (OCIO), Office of the Under Secretary for Management, and the director of operational test and evaluation. All three offices play key roles in overseeing DHS's major acquisition programs and are very involved with CBP TECS Mod. Further, DHS's Office of Program Accountability and Risk Management (PARM) works to ensure the effectiveness of the overall program execution governance process by providing independent assessments of major investment programs, and by identifying emerging risks and issues that DHS and its components need to address. I hold a monthly Program Management Review (PMR), attended by OCIO and PARM representatives, which covers schedule, cost, risks/issues, and other topics. In addition to these formal meetings, Mr. Thomas Michelli, ICE's chief information officer, and I hold regular meetings to coordinate TECS Mod activities, and our program staffs meet frequently for detailed collaboration.

Program Management

CBP's TECS Mod effort is led by the TECS Mod Program Management Office (PMO) within OIT's Passenger Systems Program Directorate (PSPD). PSPD man-

ages applications which support CBP's traveler vetting and processing systems at U.S. ports of entry. It has successfully delivered several high-profile border security systems, including Trusted Traveler, Electronic System for Travel Authorization (ESTA), and Western Hemisphere Travel Initiative (WHTI).

Vital aspects of CBP TECS Mod's strong program governance and program management are the risk and requirements management processes. CBP TECS Mod's risk management processes include a strategy outlining techniques and procedures for identifying sources of risks, and how to categorize, analyze, and prioritize identified risks. Additionally, each of CBP's five TECS Mod projects have a Government Project Manager whose responsibilities include identifying, verifying, analyzing, documenting, and tracking project risks, as well as communicating risk issues to the TECS Mod Program Risk Manager.

CBP's TECS Mod requirements management process was revised and improved in 2012, resulting in better organization, tracking, analysis, and communication of program requirements. These practices include a standardized plan to identify requirement types, such as operational, functional, or technical, and to attribute mandatory and optional traits for each requirement, such as source, date certified, and status. Requirements are elicited at user sessions, supported by key users identified by the CBP Office of Field Operations (OFO) and additional user communities within CBP, DHS, and/or partnering Government agencies (PGAs). Once functionality is developed, it undergoes rigorous developmental and user acceptance testing, followed by independent operational testing to ensure that the functionality is consistent with the approved requirements and satisfies user needs.

Program Schedule and Cost

The TECS Mod Acquisition Program Baseline (APB), the program's guiding document, provides the program milestones for key schedule events, including objective dates and threshold dates. The APB also specifies program cost objectives and thresholds to ensure the program stays within budget. The CBP TECS Mod program has stayed within budget since it began in fiscal year 2008. The PMO collaborated with the DHS Cost Center of Excellence in March 2012 to refine the Life Cycle Cost Estimate (LCCE) to ensure risk sensitivity was addressed and to validate the accuracy and approach of the LCCE. The LCCE has recently been updated to reflect actual costs for fiscal year 2012 and fiscal year 2013 as well as the impact of the pause of the PIP project. The current LCCE is $692.557 million (threshold level) covering planning, development, and maintenance costs from fiscal year 2008 through fiscal year 2021.

The TECS Mod master schedule provides visibility into program and project activities aligning with the APB. The schedule is reviewed and maintained by the TECS Mod Project Schedule Manager. CBP TECS Mod is continually improving and refining information in the schedule as a result of project and program maturity. The detailed schedule is reviewed biweekly and progress of major milestones is tracked. Despite challenges such as the size, detail, and complexity of a schedule with over 20,000 tasks, the current process allows the Program Manager to monitor the APB milestones, decision gates, and major deliverables and to ensure successful project management and delivery within planned dates.

The CBP TECS Mod scheduling process has helped the program deliver timely incremental functionality and stay on track for completion of the total program. Because of fiscal year 2013 budget uncertainty and sequestration, the CBP ESC decided to pause PIP, the last project under TECS Mod. As a result, the CBP TECS Mod schedule was recently revised to restart PIP late in the second quarter of fiscal year 2014 and to move the program completion date from the end of fiscal year 2015 to mid-fiscal year 2016. The APB has been updated with the revised schedule and is currently going through the approval process within CBP and DHS.

Program Performance

Some CBP TECS Mod functionalities have already been delivered, such as the modernized Secondary Inspection application, which is being used successfully at air, land, and sea ports of entry. The modernized High Performance Primary Query Service was made operational in 2012 and is now being used by the Advance Passenger Information System. In fiscal year 2013, TECS Mod delivered additional functionality such as implementing TECS portal, a web-based interface which will replace the current terminal-only access, for the TDED and LRDS projects. The first phase of this user-facing functionality includes lookout and travel document queries. In fiscal year 2014, TECS Mod will deliver new functionality such as enhancements to query and lookout applications.

CBP has made significant progress with our TECS Mod Program to date, and we anticipate completion of program development and Full Operational Capability

(FOC) in mid-fiscal year 2016. While 6 milestones were not met early in the program, by incorporating additional operational capabilities and adjusting to address technology implementation challenges, we have met all other major milestones and have been delivering modernized functionality incrementally as planned. Program planning and execution can always be improved; however, CBP TECS Mod has strong schedule, risk, and requirements management practices in place, which have facilitated delivery of required functionality on schedule and within budget. The PMO has grown in staff and matured its management processes since the program began in 2008.

The CBP TECS Mod program has made significant progress, reached many milestones, and the program is in good overall health. GAO report GAO–14–62, *DHS's Efforts to Modernize Key Enforcement Systems Could be Strengthened*, published December 5, 2013, contained four recommendations for CBP's TECS Mod program. DHS and CBP concurred with three of the recommendations and is in the process of resolving and implementing these recommendations. Although CBP did not concur with GAO's recommended changes to our schedule process based on the fact that our established process has proven to be effective and efficient, we will continue to refine and improve upon our current model.

CONCLUSION

CBP is working hard to continue incrementally delivering TECS Mod functionality and completing the program within budget by mid-fiscal year 2016. We are continuing to improve the management of all our programs by ensuring effective oversight, and by harnessing best practices in how we run those diverse programs. These efforts enhance CBP's multi-layered approach to vetting and identifying potential travelers to the United States who may pose a threat to the homeland.

Thank you for allowing me the opportunity to testify before you today. I look forward to answering your questions.

Mr. DUNCAN. Thank you for your testimony.

Mr. Michelli, you are recognized for 5 minutes.

STATEMENT OF THOMAS P. MICHELLI, CHIEF INFORMATION OFFICER, IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MICHELLI. Chairman Duncan, Ranking Member Barber, Congressman O'Rourke, I thank you for the opportunity to discuss ICE's efforts to improve TECS and the findings of GAO's recently-released report.

We appreciate GAO's work conducting the review of TECS Modernization, and we look forward to working with Mr. Powner and GAO on this important program.

Today I would like to provide some background on ICE TECS Mod and to outline the actions we have taken to manage our program, as well as respond to GAO's findings and recommendations.

As you have mentioned, TECS supports ICE's investigative case management, including documenting subjects of criminal investigation in the form of records and reports, which is the basis for criminal prosecution. TECS Mod is a coordinated initiative by ICE and CBP to replace the portions of legacy TECS that align with our respective core missions.

ICE's goal is to relocate the system from an expensive mainframe by the end of September 2015 by developing a modernized and comprehensive investigative case management system that will support the investigative mission of ICE's Homeland Security investigations.

Subsequent to a full and open competition in 2011, ICE awarded a best-value, cost-plus contract for a custom-developed investigative case management system. Much work progressed well, including programmatic management improvements, requirements refine-

ment, development and delivery of data synchronization with the legacy system, interfaces to required systems, and robust development in test environments.

What did not progress well was core case management design and development. Many of the issues we identified causing this lack of progress were subsequently included within the findings in the GAO report. Our Government and contractor team worked diligently to remedy these issues before, during, and following the GAO study.

As we work to improve program performance, we apprise and receive direction from the appropriate executive steering committees, which included DHS, ICE, and CBP senior leadership. We made program decisions based on business analysis of trade-offs of cost, schedule, and performance consistent with our overall goal to be off the legacy TECS mainframe by September 2015.

In June 2013, after a diligent effort to bring the core case management development back on track, ICE concluded, in collaboration with the vendor, that the core technical architecture was insufficient. In an effort to independently validate our concerns, ICE commissioned a brief independent verification and validation analysis of the system's status and viability, which confirmed that the existing technical architecture was not viable.

Once ICE confirmed nonviability of the technical solution, we acted immediately to change the direction of the program. Based on the recommendation from the IV&V, a subsequent market research assessment, as well as the conclusions reached in conjunction with our governing bodies, ICE is pursuing procurement of a commercial off-the-shelf, or COTS, -based solution for investigative case management.

All indications based on recent market research are that we will be able to procure, deploy, and successfully be off the mainframe by September 2015, while also achieving lower life-cycle costs.

GAO's findings related to ICE focused on two key deficiencies: Risk management and requirements management. We concur with all three recommendations offered by GAO to aid in overcoming these deficiencies and have completed the appropriate documentation and implemented processes and procedures to fulfill these recommendations.

ICE initiated new status reporting methods based on leading practices, providing management with a more immediate picture of program progress. The program has overhauled its reporting structure and established integrated project teams that report status and coordinate dependencies weekly. We now track all known risks, not just those considered significant. We have revised our risk threshold to ensure risks are identified and are properly raised to leadership in a timelier manner.

The program has also implemented a method to mitigate each elevated risk over a period of time. Both the revised risk threshold escalation and the method to mitigate risk have been incorporated into Government oversight process and will be in the scope of work for the new contracts for a future ICE TECS Mod solution.

The ICE TECS Mod program has completed a detailed evaluation and comprehensive analysis of our system requirements. The program identified and eliminated overly prescriptive, technically out-

dated, and redundant requirements. This refinement resulted in a reduction in excess of 75 percent of system requirements without compromising capability.

We have validated our new requirements baseline and confirmed that they are in line with other Federal law enforcement investigative case management programs. ICE has established new guidelines related to requirement management and established strict change control processes, which is consistent with GAO's recommendation.

ICE remains committed to working in a coordinated effort with DHS and CBP to remedy any issues that have arisen during our modernization effort. We will continue to coordinate with stakeholders as we move forward to rebaseline the program and restart development work.

In closing, both Mr. Armstrong and I are committed to the success of this program. Thank you again for the opportunity to appear before you today, and I would be pleased to answer any questions.

[The prepared statement of Mr. Michelli follows:]

PREPARED STATEMENT OF THOMAS P. MICHELLI

FEBRUARY 6, 2014

INTRODUCTION

Chairman Duncan, Ranking Member Barber, and distinguished Members of the subcommittee: On behalf of Secretary Johnson and Acting Director Sandweg, thank you for inviting me to appear before you today to discuss efforts of U.S. Immigration and Customs Enforcement (ICE) to improve TECS and the findings of a report released in December 2013 by the Government Accountability Office (GAO) entitled "DHS's Efforts to Modernize Key Enforcement Systems Could Be Strengthened."

The U.S. Department of Homeland Security (DHS) and ICE appreciate GAO's work conducting the review of TECS Modernization and issuing this report, and I am grateful for the opportunity to provide background on ICE TECS Modernization (ICE TECS MOD) and outline the actions we have taken relating to GAO's findings and our continued collaboration with U.S. Customs and Border Protection (CBP) to address the recommendations offered by GAO.

HISTORY OF TECS AND MODERNIZATION EFFORTS

TECS is a mainframe system that is the primary system of both ICE and CBP, initially developed in the 1980s. TECS was previously known as the Treasury Enforcement Communications System when it was managed by the former U.S. Customs Service (which previously encompassed portions of both CBP and ICE functions). The system, which is currently managed by CBP, supports primary and secondary inspection processes for CBP and Federal agencies vetting for law enforcement and immigration benefits purposes. TECS also supports ICE's investigative case management including documenting subjects of criminal investigation in the form of records and reports, forming the basis for criminal prosecutions. The TECS modernization effort (TECS MOD) is a coordinated initiative by ICE and CBP to replace our respective portions of legacy TECS.

Currently, our agencies are engaged in efforts to modernize the system into products that fit both specific and mutual needs and to migrate the legacy TECS system from the outdated CBP mainframe computer system (ICE TECS MOD and CBP TECS MOD programs, respectively). ICE's initial goal was to relocate the system from the prohibitively expensive mainframe by September 30, 2015 by developing a comprehensive law enforcement investigative case management system that will support the investigative mission of ICE's Homeland Security Investigations (HSI) and its shared mission with CBP to protect the homeland.

Subsequent to the award of a best-value, cost-plus contract, ICE concluded, in collaboration with the vendor, that the core technical architecture was technically insufficient in June 2013. In an effort to independently validate our concerns, ICE commissioned a brief Independent Verification and Validation (IV&V) analysis. ICE

used the IV&V to conduct an assessment of the system's status and viability. Following an abbreviated examination, the IV&V confirmed that the utilization of existing architecture would not be technically viable to support system needs. The IV&V also indicated that there were significant technical and management process deficiencies that would make meeting the September 30, 2015 deadline highly improbable.

In consideration of the collective conclusions of ICE, the vendor, and the IV&V, it was determined that the ICE TECS MOD program required restructuring in order to ensure accountability and the ability to address deficiencies in technical oversight and requirements management. Accordingly, ICE restructured the program by increasing executive oversight, establishing integrated project teams and Government personnel accountability, identifying alternative technical options, and began the process of identifying a new prime contractor.

PRIOR AND FUTURE FUNDING

The ICE TECS Modernization Life Cycle Cost Estimate (LCCE) was finalized on September 6, 2011, at $818 million for all acquisition and sustainment costs, assuming a life cycle for the program extending to 2024. Prior to the award of the Design/Development contract in September 2011, the program received $55.4 million in automation modernization funding and expended $22 million in support of requirements analysis, data migration, and acquisition activities. Between fiscal year 2012 and fiscal year 2013, the program received $36.9 million in automation modernization funding, expending $21.2 million on the Design/Development effort that was curtailed in July 2013, and expending $17.8 million on ancillary contracts including data migration, training, and communications and program support. In fiscal year 2014, the program's automation modernization budget is $23 million. In total, ICE TECS Modernization has received $115.3 million in funding, and we have expended $63.9 million to date.

The program is in the process of revising its LCCE to be in line with its future plans for the program, and anticipates the full LCCE to be less than the original $818 million due in large part to an increased use of commercial, off-the-shelf products (COTS) that will require less custom development and on-going support. Once the revised LCCE is complete, the program will be able to adjust future automation modernization funding requests, and account for both funds received but not expended, as well as lower anticipated costs.

GAO'S FINDINGS AND ICE'S RESPONSE AND ACTIONS

According to GAO, its objective during its review was to determine the scope and status of CBP's and ICE's TECS MOD programs, assess selected program management practices for TECS MOD, and assess the extent to which DHS is executing effective executive oversight and governance of the two TECS MOD programs. In order to accomplish these objectives, GAO reviewed requirement documents, as well as cost and schedule estimates to determine the current scope, completion dates, and life-cycle expenditures. In addition, GAO reviewed risk management and requirement management plans, as well as the meeting minutes of the governance bodies.

The report highlights that ICE's initial efforts were determined to be ineffective, resulting in the need for the program to restart. It is pivotal to note that ICE made the determination itself based on identified risks, schedule slips, and poor quality of interim deliverables, which ultimately led to the final determination that the current technical solution would not be able to support the mission needs of ICE. Based on this determination, ICE took steps to verify this conclusion through an independent third party, as well as improve management oversight. Once ICE confirmed non-viability of the technical solution, we acted immediately to change the direction of the program. Our action included an external evaluation, which predated the GAO report. Upon receipt of this independent evaluation, ICE undertook major course corrections that are in line with those ultimately recommended by GAO.

GAO's findings highlighted the status of ICE's efforts to modernize our portion of legacy TECS, focusing on two key deficiencies: Risk management and requirements management. We concur with the three recommendations offered by GAO for executive action directly linked to ICE.

The following are highlights of ICE's responses and actions taken:

RISK MANAGEMENT

GAO recommended that the Secretary of Homeland Security direct the acting ICE director to ensure that all significant risks associated with the TECS MOD acquisi-

tion are documented in the program's risk and issue inventory—including acquisition risks—and briefed to senior management, as appropriate.

ICE initiated new status reporting methods based on leading practices, providing management with a more immediate picture of program progress. The program has overhauled its reporting structure and established Integrated Project Teams that report status and coordinate dependencies weekly.

In addition to the other programmatic risk changes, we also concur and have adopted the GAO's recommendation to add and track all known risks. For example, the ICE TECS MOD program has documented in the risk inventory a new acquisition risk that accounts for the aggressive time lines associated with the revised program strategy. This risk, as with all identified risks, has been reviewed by the program's Risk Advisory Board and elevated to ICE and DHS senior leadership.

GAO also recommended that the Secretary of Homeland Security direct the acting ICE director to ensure that the appropriate individuals revise and implement the TECS MOD program's risk management strategy and guidance to include clear thresholds for when to escalate risks to senior management.

The ICE TECS MOD program currently has a set of conditions that must be met for a risk to be elevated. We are revising our risk threshold to ensure risks are identified and appropriately raised to leadership in a timelier manner. The program is also identifying detailed activities that will help to mitigate each elevated risk over a period of time. Both the revised risk threshold escalation and the method to mitigate risk are being incorporated into the Government oversight process and will be in the scope of work for new contracts for the future ICE TECS MOD solution.

REQUIREMENTS MANAGEMENT

In addition, GAO recommended that the Secretary of Homeland Security direct the acting ICE director to ensure that the newly-developed requirements management guidance and recently revised guidance for controlling changes to requirements are fully implemented.

The ICE TECS MOD program has completed a detailed evaluation and a comprehensive analysis of our functional requirements. The program identified and eliminated overly prescriptive, technically outdated, and redundant requirements. This refinement resulted in a reduction in excess of 75 percent of functional requirements without compromising capability. Additionally, the program has validated its new requirements baseline against other Federal law enforcement investigative case management programs. ICE has established new guidelines related to requirement management and strict change control processes, which is consistent with GAO's recommendation.

COORDINATION WITH KEY STAKEHOLDERS

Throughout this effort, we have been committed to open and consistent communication with the DHS Office of the Under Secretary for Management. As it became apparent that the technical solution under development would not support the objectives of the program, ICE increased the frequency of its meetings with DHS to provide more regular and timely reporting of program issues and proposed resolutions. Additionally, ICE notified DHS after learning the program would not meet the revised baseline date of December 2013. The program is currently working with DHS's Office of Program Accountability and Risk Management to establish a new revised program baseline. This baseline will be formally reviewed and approved by DHS per the Acquisition Decision–102 guidance, before the program can restart development.

In a similar manner, we have maintained on-going collaboration and coordination with CBP, our key mission partner. CBP serves as a voting member on the ICE Executive Steering Committee (ESC), which is responsible for oversight of the ICE TECS Modernization effort, and ICE serves as a voting member on the corresponding CBP ESC. In addition, both ICE and CBP participate as partners through the coordination of delivery schedules, technical solutions, and risk/issue resolution. We recognize that close coordination is vital to the joint success of both programs, and will continue to take the steps necessary to maintain that coordination going forward.

CONCLUSION

ICE remains committed to working in a coordinated effort with DHS and CBP to remedy any issues that have arisen during our modernization efforts. The ICE TECS MOD effort has taken a variety of steps to ensure that the program not only stays on track, but that there is careful oversight of the acquisition and development process while utilizing independent authorities to assist with validation of our

collective efforts. ICE will continue to coordinate with stakeholders as we move forward with efforts to re-baseline the program and restart development work to become independent of the costly legacy system as soon as a viable modernized system can be deployed.

Thank you again for the opportunity to appear before you today and for your continued support of ICE and its law enforcement mission. I would be pleased to answer any questions.

Mr. DUNCAN. Thank you, gentlemen, for your opening statements.

I will now recognize myself for 5 minutes for questions.

Let me just say, I will reiterate what I said earlier. I understand the immense challenge of the number of vehicles and persons entering the country every day. I probably don't understand it as much as the gentlemen from El Paso or Arizona do, but I do comprehend that we need to facilitate the flow of commerce and activity across the border in these border communities like El Paso. I will leave those comments for my friend from Texas.

But when I think about it from a private-sector standpoint and I look at the fact that we just spent $60 million in taxpayer funds—taxpayer dollars, taken from hardworking Americans that work hard to earn that money, taken from them through taxation—and we spent that over a 4-year period of time, and I don't know that we are far enough down the road to where we need to be.

I am not going to say that 100 percent of that $60 million was wasted, because you learned from those efforts, you actually built a platform that you can take the next step from, so I am not saying that at all. But I am concerned, because I know in the private sector there are not many firms, if any, that could invest that kind of money for very little result. I don't know many private-sector firms that actually would. They would hold someone accountable in year 1, year 2, and probably a lot quicker.

So it seems that the requirements process broke down within both CBP and ICE regarding the TECS program. Given the requirements process has been a problem in past DHS failures, and I point specifically to SBInet, explain to me why CBP and ICE weren't able to get this right this time. You know, what were some of the obstacles that, after spending $6 million, you say, you know, we are going to have to start over?

I will address that first off to Mr. Armstrong, and then I will come back to the GAO. I want to hear your take on it.

Mr. Armstrong.

Mr. ARMSTRONG. Well, first off, I mean——

Mr. DUNCAN. Microphone. There you go.

Mr. ARMSTRONG. First off, you know, I don't believe we had any complete failures in our requirements process. Our requirements process did have some challenges that could have been better, but I will say that one of the lessons learned, you know, since you asked, I mean, one of the lessons learned we have picked up from other programs is we are trying to move to more of an iterative process where we are prototyping functionality and not doing a big, monolithic build of functionality before we deploy something.

So our officers and agents actually get to see the functionality early on before we spend a lot of money to go then build it. Then, after we build it, then we go out to some test ports, and then we

prototype that in the actual live environment. That gives the officers and agents an opportunity to work with the system and gives our program office an opportunity to make sure that we have the requirements right before we fully deploy the system.

So we iterate back through that; we roll that back into sub-releases. Then, once that is in a, kind-of, final stage, it goes through a control gate, where then the user signs off on it and we start to deploy that out to more locations.

So I think that those are the big lessons learned that we got out of other programs. I feel like we are on track.

Mr. DUNCAN. Thank you for that.

Before I come to the GAO, it just hit me that, you know, in the private sector, there is a finite amount of money that a company has to spend. Sometimes that is money that they have saved over the course of business practices for a number of years, anticipating the need for further investment, regardless of whether it is IT or capital improvements or whatnot, or they borrow money, or they raise money through stock initiatives, but it is still a finite amount.

But it seems to me, when we see where we are with this kind of money being spent, that elements within the Government don't believe there is a finite amount, they believe that there is an unlimited supply. You know, we are $17.5 trillion in debt because we have had that mentality in this Nation that we can just continue spending without the kind of accountability that you would see in the private sector.

So, Mr. Powner, the GAO has looked at this. That is your responsibility. How can we be better stewards of taxpayer dollars, and how can we ensure that these agencies actually don't wait till 4 years out, that they actually have more checks and balances going forward?

Mr. Barber mentioned the two different groups' almost duplicative efforts and how you have accountability with that. So I would love for you to speak to that, if you will.

Mr. POWNER. So, a couple points, starting with requirements.

I think from a requirements perspective, both programs, I would say they have fairly solid requirements management processes in place now. Those were put in place late. I think it was most evident in the ICE program. I mean, Mr. Michelli's comments about the requirements resulting in a 75 percent reduction in requirements, that is a big change. I am glad that we are getting it together now, but a lot of this is coming too late.

The other thing that I would like to mention in addition to the program management on requirements and the risk that we need to do a better job at, not just here at DHS but in a the lot of pockets of the Federal Government, is executive leadership. These executive steering committees that were put in place, chaired by both these individuals, are now in place, and I think they are working more effectively now. But it sure would have been nice to have those in place sooner.

Mr. DUNCAN. Okay.

My staff just reminded me, you know, I am talking about $60 million, but CBP has spent a quarter of a billion dollars since 2008, and the only project fully completed is secondary inspection. You

have a long ways to go. That is a heck of a lot of taxpayer dollars that were spent—a quarter of a billion dollars.

I am going to stop because I need to let my blood pressure calm down a little bit as we move forward, and I am going to recognize the Ranking Member.

Mr. BARBER. The Chairman is passing his blood pressure problem along to me. Very good. I appreciate it.

I, too, am worried and concerned, as the Chairman is.

Let me start, Mr. Armstrong, by asking you this question. Last month, on January 10 to be precise, the Chairman and I wrote a letter to the under secretary for management, Mr. Borras, expressing our concern over CBP's decision to take corrective action on the procurement efforts for the TECS Mod and asking for an update on when the final request for proposals will be complete.

The contract, as you may know, is currently operating on a series of 3-month extensions. Such short-term contracting, I think without question, has created uncertainty among those individuals who are responsible for the TECS Mod update.

To my knowledge, my office—and perhaps the Chairman has, but I don't know that he has, because I think we would both receive the response at the same time—we have not yet received a response from the Department. It has been almost 30 days.

So, two questions: No. 1, when can we expect the office to respond to our inquiry? How is DHS providing direction and clarity to stakeholders throughout the TECS Mod process, including any decision to recompete the TECS Mod contract?

Mr. Armstrong.

Mr. ARMSTRONG. First of all, I don't control the Departmental clearance process. So, I mean, we are prepared to give them—I mean, we have the information that they would need to respond to you. That would need to be cleared by the Department.

We would be more than happy to come up and do a, kind-of, closed-door briefing on the acquisition. But since a lot of that is procurement-sensitive, I really don't feel comfortable, kind-of, commenting on all that here today. But more than happy to come back with our contracting officers and go through, kind-of, where we are on the acquisition for you.

Mr. BARBER. Certainly. Contact my office as soon as you can, and we will arrange for that meeting.

Could you, within the Department, ask of the people you have to deal with on the clearance process when we might expect an answer to the questions that we phrased?

Let me next move to some questions for Mr. Powner.

You know, I have only been on this committee for a year-and-a-half, and one of the things that I think troubles me a lot is how many GAO reports we get regarding DHS. Perhaps other agencies get as many, but I have a feeling we are a little bit on the high end here.

So, as you know, Mr. Powner, TECS is used by CBP and ICE, of course, and it is also used by over 20 other Federal agencies, as I have mentioned in my opening remarks, including FBI; Alcohol, Tobacco, and Firearms; and the Terrorist Screening Center; as well as Departments of State and Treasury. These are accessing TECS on a daily basis.

When you looked at the TECS Mod process, Mr. Powner, did it reveal to you the level of consultation that DHS had or the interactions it had with other users of the TECS from other Federal agencies to get their feedback on suggested requirements?

I mean, critical, I think, in any development of any system, new system or revised system, that the end-user have some input on the process and what they expect to get out of the end product. Could you tell us what you found in your inquiries, if you looked at this?

Mr. POWNER. Well, when you look at the requirements-setting process, I mean, clearly, you know, when they put a system in place, the primary user is DHS, but that process does touch with the other stakeholders in the program and the other departments and agencies. I mentioned in my opening statement 10 departments use this system.

So that is part of the process. It is important as part of the process going forward that when we validate these new requirements, as these programs are being rebaselined, that we continue to get feedback from those stakeholders. I assume—like Mr. Michelli talked about, discover the requirements—I assume there was a process to vet that with some external stakeholders.

Mr. BARBER. Well, perhaps, Mr. Michelli, you could comment on that in terms of consultation with other departments. Can you tell us to what extent that was done as you are moving forward?

Mr. MICHELLI. Congressman, I don't know for sure what the extent was, and I can get back to you on that. I do know that we have an entity within ICE that conducts information-sharing requirements generation with other entities, and I will find out what they have done.

Mr. BARBER. I am running out of time, but, Mr. Chairman, if you can indulge me a few more seconds here. Just two quick questions for Mr. Armstrong.

Basically the same question that I just asked of Mr. Michelli and Mr. Powner, but in a different context. Again, when the end-user is consulted in any IT project, you get a better outcome. Unfortunately, all too often, they are not considered.

So can you tell us, were CBP officers and agents involved in the development and setting of requirements for TECS Mod?

Mr. ARMSTRONG. Sir, they were absolutely involved. We have a requirements board that worked with our officers and agents and worked with other stakeholders throughout the Federal Government. I can tell you that even in our first deliveries of secondary processing, we got feedback from other agencies complimenting us on the efficiency by which the system worked.

So, absolutely. We have been doing this for a long time with other agencies. We have a lot of experience in doing requirements management with other agencies. So we believe that it is working efficiently.

Mr. BARBER. My last question to you, Mr. Armstrong, has to do with something I mentioned earlier, and that is the delays that people have coming into our country for legal commerce, tourism, produce, products from Mexico and all the rest. The lines that are waiting at the ports of entry, particularly in my district and the adjoining district, sometimes can be 2, 2½ hours. This directly speaks

to the economic issue that my State and the country faces; when we could expedite trade, we get economic development and growth.

I want to ask you if you can comment on to what extent you think the TECS system, which is cumbersome and obsolete, has impacted on these delays. I know we have a problem with the number of agents we need, but is TECS a part of the problem, do you think?

Mr. ARMSTRONG. Well, I would say the biggest issue in terms of TECS and wait times at the border has been the stability of the old system. So the new system is going to allow for a lot more redundancy within the system, and it will reduce the amount of outages we have to take for maintenance.

So I think, coupled together, the availability is going to go up. That is certainly the platform that we put together. It will also reduce those outages, those planned outages that we normally take at least once a month. So I believe it will improve things.

Then, also, kind-of parallel to this, you know that we have been moving to other technologies at the ports that will help expedite especially the pedestrian traffic, so things like ready lanes and allowing more self-service in those areas. The new system, I believe, will allow us to avail ourselves of some of these technologies as they become available much quicker than the old mainframe system.

So, as our officers continue to work on process improvement, looking at throughput in the ports not just from the physical standpoint but also from the time it takes to get people through primary and/or through secondary, I believe the new system will definitely expedite that processing downstream.

Mr. BARBER. Well, thank you, Mr. Armstrong.

Mr. Chairman, before I yield, I would like to ask unanimous consent that Congresswoman Sheila Jackson Lee, who is a Member of the full committee and Ranking Member of the Border Subcommittee, be allowed to join the panel and ask questions when time is allowed.

Mr. DUNCAN. Without objection, so ordered.

The Chairman will now recognize Mr. O'Rourke for 5 minutes.

Mr. O'ROURKE. Thank you, Mr. Chairman.

I want to commend you for your focus on issues of accountability, especially when it comes to purchasing and contracting within DHS. I feel that, when it comes to technology solutions, we can become enamored of quick fixes, blinded by the difficulty of understanding the specifics involved. When we have the kind of blunders that it seems that the GAO has uncovered here, the boondoggles like SBInet that you pointed to, as a whole, as a body, Congress, I think, oftentimes turns a blind eye. So I really appreciate the focus, the attention, and the drive for accountability.

I also want to refer to the numbers that you gave us: A quarter of a billion dollars for CBP's five-step program, only one of which, one of those steps, has been achieved. You mentioned $60 million earlier; $20 million on the Raytheon mistake with the TECS Mod where we are cutting 75 percent—or 70 percent of the requirements, had delays of nearly a year, and are having to redesign from the beginning the whole process.

You compare those numbers to $140,000, which is what it costs to fully train, hire, and move a CBP officer to where he will be em-

ployed. That officer will contribute nearly $2 million to the economy, will help create 22 additional jobs in the U.S. economy throughout every State in the Union.

So, while I certainly understand, as Mr. Armstrong said, the time savings that we might be able to see if we can successfully implement some of these technology initiatives, and I certainly want us to do that, I also think that we have some much lower-hanging fruit, including spending and deploying those assets much more wisely.

I would start with our human assets, those CBP officers, who have some of the most dangerous, difficult, and most critically important jobs when it comes to our economy, the safety and security of our country. I would urge CBP and DHS to focus more attention on that.

To Mr. Powner, you mentioned SBInet, which really seemed like a contractors-gone-wild episode, where Boeing is designing the scope of the project, they are responsible for defining the milestones and the measurements, and we saw, you know, hundreds of millions of dollars later, that we had a system that we could not use, that was a waste of taxpayer money, and that we had to scrap completely.

We looked at the Raytheon TECS Mod project, begun in September 2011: A delay of 7 months, 70 percent of the requirements were removed from the project, and $20 million later, it sounds like we are starting over again.

Do we have—and you mentioned a deficiency in your opening statement of core case management and development. Is there some kind of brain drain within the Federal Government that does not allow us to properly manage these projects? Should we be doing more of this in-house and not allowing the Boeings and the Raytheons of the world to design these projects, and should we be doing more of that work in-house? Then, when it comes to actually implementing, programming, testing, holding to account those who are working on this, should we be doing more of that in-house, as well?

Mr. POWNER. Well, there are very few pockets in the Federal Government that can do a lot of this, in terms of the development. There are limited pockets. I will give you IRS as one example; they have pockets where they do their own development. But we contract this out.

I think the key is, there are responsibilities that the Government has and responsibilities that the contractors have. In the requirements-setting process, let's start with that, that is the responsibility of the Federal Government to define what we want. Too often with a lot of these programs, you are absolutely right, Representative O'Rourke, that we have contractors get involved in defining how we are going to do things, so that we need a real clear line of delineation there. I think these two gentlemen are getting—that is actually improving with both these programs. That is very important.

Then, once we get those contracts in place, the contractor oversight that needs to occur needs to be rigorous. We need to know what is being delivered in terms of productivity and quality. A lot of these programs, when you go in and you ask, is the contractor

delivering, how is the quality and productivity, we don't get the right answers from the Government when we look at it. That is why I would say these executive steering committees are very important in ensuring that we have the appropriate contractor oversight and we are holding contractors' feet to the fire.

I would say, on both these programs, in addition to our recommendations, one very important thing is we are in the process of putting contractors in place on both programs. I believe the ICE program has an award date for this summer, and I believe that is the same with CBP. It is very important that we get those contractors in place, the right contractors, as soon as we possibly can so that we can make progress.

Mr. O'ROURKE. Mr. Armstrong and Mr. Michelli have done a good job of walking us and taking us through process improvements, oversight committees, means by which we are sharing information across silos. But given SBInet, given what we have just described from the Members of the committee and what we read in the GAO report, what is going to give me confidence in terms of the human resources that we have within DHS, that we are not going to have a repeat of these problems going forward?

In other words, do we have the right structure, the right line of accountability within DHS to ensure that we don't have this again, either within ICE or CBP or some other aspect of DHS?

I am out of time, so I will ask Mr. Armstrong and Mr. Michelli to just very quickly address that question.

Mr. ARMSTRONG. Well, you know, I would say, at the current staffing level, I feel confident that we can provide the correct oversight on the program.

I think what concerns me and part of why I am still here in the Government is, you know, the budget issues that are going on today across the Government and the desire to, kind-of, start to downsize some of these mission support areas in order to save money. So what I can't speak to is what is going to happen in the following years, in terms of staffing and our ability to replace people as they retire and go on to other things in their life.

I will tell you that a large part of my staff, more than I would like, is retirement-eligible. They stick around because they enjoy the work that they do and they feel like the value they deliver to those front-line officers is very important to them. But that is going to soon come to an end because they can't stay around forever.

So our ability to attract and bring new talent into the Government to be able to pick up with the new technologies greatly concerns me.

Mr. O'ROURKE. You know, Mr. Chairman, with your indulgence, point well-taken that, when we have the sequester, when we have Government shutdowns, we are not allocating resources wisely. It affects you and your ability to retain the best and brightest within your organizations.

But I will also note that, since 1986, we have seen a 1,400 percent increase in spending on border security solutions. So when we look at SBInet, when we look at TECS Mod, when we look at a potential biometric exit system, I understand that we need to resource appropriately from the Congressional level, but, at the same

time, you have unparalleled, unprecedented resources at your disposal today.

Maybe what we are both saying is that more of that could be spent on our human resources, on the talent that we have there, recruiting and retaining, and less on flashy new ideas like SBInet, like a biometric exit system, when our greatest single asset is the people who protect our borders, serve the trade and the crossers coming across, and potentially design and oversee these systems that we are talking about.

Mr. Michelli, any thoughts on that?

Mr. MICHELLI. Yes. In ICE, after day-to-day mission, cybersecurity, and public officer safety, ICE TECS Mod is the No. 1 priority. We are putting our best and brightest on TECS Mod.

When we did the requirements refinement in our ESC, which has an HSI, Homeland Security Investigator chair, realized that we could use additional help, he has put his best and brightest on the project, as well.

I do have concerns as we progress into a commercial off-the-shelf program that we have the right technical skills for oversight for that. So, as part of the contract action, we have gone out with an FFRDC to get that expertise in-house so we will have that technical oversight.

So I believe we are staged to have the right human skills, both on the technical side and on the mission side, to have success.

Mr. O'ROURKE. I hope so. We need to make sure that that is the case.

Thank you, Mr. Chairman.

Mr. DUNCAN. Thank you. Great questioning.

Before I recognize the gentlelady from Texas, I had looked up some comparison numbers of a system known as Iron Dome deployed by Israel, very effectively I may add, a system that was developed from drawing board to combat-readiness in less than 4 years, a system that is effective at shooting down an airborne rocket traveling at a very high rate of speed, for the cost of $210 million. Rafael corporation did that.

So, you know, the reason I say that is, we have put this in context, with the amount of money we are spending and what we are spending the money on—it is not hardware; to some degree, it is a software and hardware blend, I understand that—but what one group of people were able to do in less than 4 years for a lot less money than the numbers we are talking about today.

So, with that, I will recognize the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Let me thank the Chairman, Mr. Duncan, and Mr. Barber, the Ranking Member, for their courtesies for allowing me, as a Member of the full committee, to sit on this committee.

Let me thank the witnesses very much for their service.

Allow me just to make two points before I offer some questions that I think we all are concerned about—the operations of a very, very, very important agency.

I first want to say that I am very grateful for the breakthrough that we have heard over the last couple of weeks, or last week, regarding our Republican friends in the United States Congress on

the idea of comprehensive immigration reform and their own principles that have been enunciated, and to thank them for that.

One of the key elements, which I want to put on record, where there is not a divide is the idea of border security. This hearing obviously plays a very large role, I believe, in the moving forward of comprehensive immigration reform.

We truly believe here on the Homeland Security that we have crafted a thoughtful legislative framework in H.R. 1417 that may avoid prospectively some of the defaults of this TECS Mod program. H.R. 1417 thoughtfully lays out a roadmap, seeks the input of the Department of Homeland Security ahead of the strategies being articulated, and soundly commits to the security of the Northern Border, which I always want to mention, and the Southern Border.

Mr. Chairman and Mr. Ranking Member, I think the oversight work that you are doing complements where we need to be if we move forward as Republicans and Democrats on what I hope will be not listening to the naysayers who are countering my optimism that we will reach a point where we have an effective construct. With that in mind, we will need the kind of technological forceful structure that works because that is part of the compliment of H.R. 1417.

The last statement I want to make is that I hope that we can work out CBP—this is on the record—the issues with how CBP officers are dealing with overtime. We recognize that there are some unfortunate incidences that have occurred, but I support them. I would like to see their overtime reinstated or a process reinstated for them to be fairly compensated for both their work and their sacrifice, along with ICE and others.

I want to quickly move to Mr. Powner and indicate if I could what can you give us, give the committee an effective, efficient, and modernized tech system, what if you could just concisely throw out what it would be? I know you gave us a number of suggestions, and unfortunately, it looks as if they were not followed. Then would you also suggest how it would be managed? Can it effectively be managed with multiple partners or multiple leaders? I will just pose that question to you. I will quickly go to Mr. Armstrong and Mr. Michelli, if you can be prepared to tell me what you actually got out of the $60 million in 4 years program that was halted.

Mr. Powner, can you answer what would be an efficient tech system?

Mr. POWNER. So, first, when you look at the process for delivering the tech system, I think the requirements are getting laid out in increments. I will reiterate the importance of having strong program management, risk and requirements and having the executive-level governance. I will add this. When we look at successful IT acquisitions, they go small increments. When we try to go big, we have failures time and time again. We always have these failures, and what happens to fix it? We go with smaller increments, so I think the more we can go with small increments and even smaller increments going forward, that is what will be very successful going forward.

Ms. JACKSON LEE. When you say "executive," what do you mean by that?

Mr. POWNER. Having the right executive-level oversight. What I mean by that is when something fails, we typically point at the poor program manager and blame the program manager when, in fact, it needs to be executives who own the project.

Ms. JACKSON LEE. How far up do you go when you say executive? Secretary of Homeland Security?

Mr. POWNER. Well, clearly, these guys run the executive steering committee, so they're key players. But then it ought to go up the CIO of the Department, and it ought to go up to the under secretary for management, clearly, if this is an important project for the Department.

Ms. JACKSON LEE. I think these are important instructions. Can I quickly ask you to ask us, just you, did we gain anything from the present system that we had?

Mr. POWNER. We sure did. I mean, if you look at what CBP, with the secondary inspections, clearly there was value in—delivered with that. We had $225 million spent on that piece, so there was some value derived there.

To Chairman Duncan's comment about $64 million spent, you are right; we did learn a little bit, but there was some money wasted there, Mr. Chairman.

Ms. JACKSON LEE. To the two gentlemen who, agents or groups who were the co-managers, I guess, of this, what did your boots on the ground, what did you think your particular entity, CBP and ICE, gain from the present program that was halted, and how can you learn going forward?

Mr. ARMSTRONG. Well, certainly, as Mr. Powner said, our officers have gained greatly from the secondary inspection consolidation because that allowed us to reduce the number of lookups and screens they had to go to and gave them more opportunity to focus on the person in front of them and less time toggling through screens.

It also, and certainly in an airport environment, where there may be different parts of secondary located physically separate, it allowed for kind-of a consolidated view from the different officers within secondary so they would all know exactly what the status was of that particular traveler and anything that they may be bringing in with them.

Also, I do want to point out that we have delivery in our high-performance primary query that was not completed at the time of this report, but that is now up and running. That brings together a lot of our queries, and we're running that in parallel with our old system. The big advantage there is once we get that fully deployed, that gets what we call rapid response out to all of our officers. Rapid response does a lot more criminal history checks than what the old tech system did. So just to highlight, we have gotten significant value so far.

Ms. JACKSON LEE. Mr. Chairman, if you would indulge me, I would ask Mr. Michelli to give me the same answer. If he might just respond, what is the name of that the system, Mr. Armstrong, that you just spoke of, what is that operating under right now?

Mr. ARMSTRONG. It is one of the five projects that was delivered as part of TECS Modernization, and it is our high-performance primary query.

Ms. JACKSON LEE. That one is operating?

Mr. ARMSTRONG. Yes.

Ms. JACKSON LEE. And is still under funding; is that what you are telling me? It is still being funded?

Mr. ARMSTRONG. Yes. It is part of the $240 million.

Ms. JACKSON LEE. All right.

Mr. Michelli.

Mr. MICHELLI. Congresswoman, we have programmatic management improvements, requirements refinement, development and delivery of data synchronization with the legacy system, in other words a new database, interfaces to required systems. We have our development and test environments. This may not seem like a lot, but it actually is. This is equivalent to if you are building a skyscraper, the foundation. It is something that most people don't see, but it is very fundamental for any new system. We have that in hand. What we don't have is the first floor.

So, of the $60 million that we spent, about $20 million was for co-development. We made the decision, after receiving at least one, that it was not a sustainable solution, and we had to look at other alternatives.

So what we did learn from that is when we went out to do the market research, that the market has changed and that there are commercial off-the-shelf programs that we can now use. Our HSI agents are excited at what they see. In fact, by using from the custom code development to a commercial off-the-shelf solution, early estimates, very early estimates in the market research is we could save money over the life-cycle cost estimate of the system.

Ms. JACKSON LEE. Let me, Mr. Chairman, thank you.

If I might just say to the committee, it is very obvious that hardware of the 1970s or 1980s is so different from what we have now. Technology changes so rapidly, and as this committee does its very able work, I think some of the questions that we need to hear answered is a whole new construct as to how acquisition is done, what kind of thoughtfulness is put into it. I think what Mr. Powner said strikes me so strongly is, be measured and small. When you try to get into the ocean and just grab everything, you may have serious issues of those elements working together. I am hoping the whole committee can look at your work and maybe work, looking at a whole, I would say a whole new approach.

We have been doing acquisition issues and issues dealing with purchases by this Department for as long as I have been on this committee.

Mr. DUNCAN. I want to thank I the gentlelady for that. We are working on an acquisition bill, and it is a bipartisan with Ranking Member Thompson and Ranking Member Barber and others on your side of the aisle. Hopefully, we will be bringing that forward soon. I would love to have you look at it, Ms. Jackson Lee, and love to have your support because it does a lot of the things that we are talking about today and the great comment about the ocean and thinking, you know, small steps and small parameters so we scan have measurable activities, and we can actually measure it on a very timely basis. So I look forward to that.

Ms. JACKSON LEE. Well, let me then thank you and Mr. Barber for allowing me to be on and to listen to the proposal. I look forward to looking at the legislation. Let me thank the witnesses.

I yield back.

Mr. DUNCAN. Thank you for your interest.

In the essence of time, because they are going to call votes in 15 minutes, and much to the chagrin of my staff, I am going to yield some time to the gentleman from the Southwest for the remaining time we have here because this is an issue that is closer to home to you guys. I have got all kinds of questions I could ask, but I want to make sure that we ask the right questions if you all bring some personal local experience to the table.

So, with that, I yield to the Ranking Member, Mr. Barber, for a question.

Mr. BARBER. Thank you, Mr. Chairman.

Again, I want to thank the witnesses. I know that we have asked some tough questions of you today, and I just wanted to express that it is frustration on a broader level. As I said, I have been on this committee now for, on the subcommittee, for a year and a month and on the full committee for a little longer. But it is really frustrating for me to go home to the people I represent and to tell them once again we have another issue with expenditures with apparent waste of taxpayer dollars. We are not making much progress.

I absolutely recognize and appreciate that bringing together 22 legacy agencies is no small task. In fact, I have said before that I think actually, given the scope of this job and the importance of this job to the safety of our country, this Department is probably one of the, if not the top in priority department in the Federal Government, and certainly the job of Secretary is enormous.

I met recently—he came to my district with the new Secretary, and I am hopeful that he can bring some greater efficiency and effectiveness to some of these matters.

Let me just pose a question, a similar question, to both Mr. Armstrong and Mr. Michelli.

Mr. Armstrong, as you know, the GAO states that CBP's Office of Information Technology lacks a sufficiently-detailed master program schedule to complete major portions of the TECS Mod project and that 65 percent of its work activities apparently remain unconnected. This has led to delays and cost overruns. This obviously creates uncertainty for users of the system in the Department and for those involved in modifications of the program itself. To date, only the secondary inspection, as you mentioned, project to process travelers has actually been deployed to all air, sea, and land ports of entry.

So I would like to ask you, Mr. Armstrong, if you could outline for the committee how and when the Department plans to complete a sufficiently-detailed master program schedule for the modernization.

A similar question if I might to Mr. Michelli. You know, there apparently is no clear designed framework estimate of how much the project is going to cost, why it costs the amount it does and why it is in the interest of the Government to pay the amount requested. Then also, of course, with ICE TECS Mod's component, these are vital determinations that cannot be made because ICE cannot state with any specificity what it will deliver and how much what it will deliver will cost.

So, to both gentlemen, could you please respond to these questions? When are we going to see this level of detail which we can use as a road map to see where we are going and when we are going to get there and what it is going to cost?

Mr. ARMSTRONG. Sir, I think that, from our perspective, there is kind of a misunderstanding in terms of what actually lays out a master schedule. We have a 20,000-line master schedule in place today. The issue that GAO brought up is that we don't have all of our predecessor tasks tied together at a low level. You know, in concert with an agile development process, we wouldn't have this tied together. We would deal with those more from the iterative process that we go through. This program meets weekly to go through essentially immigration and risk issues within the program. As we move more and more to an agile environment, that process will become almost daily.

So the idea is that we are not going to be building out schedules for 3 years from now when we don't know exactly what all those tasks are going to be. We are going to build them out to that degree and scope when we are actually getting ready to do the work.

I think to the point earlier about some of these big programs that have failed, they have spent a lot of time and money building out schedules for years and then found that when they get to that point, the schedules aren't valid, and they have to go back and rework all those schedules.

So we did have some schedule issues early on in the program. Some of those were the result of some technical problems that we had, not within the scheduling, but getting technology to work. So, therefore, it took us a little bit longer to get some of our technology that allows us to keep both the old system and the new system in sync because we are building a plane and flying it at the same time. So the commercial off-the-shelf software that was out there at the point in time we started the program could not keep up with the rapid pace of which we needed to be able to process people through the border. So we had to work very closely with the vendors to get that software tuned and get it working right. So that did cause us a little bit of schedule issues.

We have now learned some lessons from that. That is part of our iterative development process to talk about those much more rapidly and get those escalated quicker. So I feel like we have got a schedule and a schedule process that works, and I think that, from my perspective and from the direction from the Department, we need to focus more on this iteration through the requirements and getting stuff deployed in smaller chunks quicker.

Mr. DUNCAN. Mr. Michelli.

Mr. MICHELLI. Congressman, yes.

We have a very broad schedule now because at week-end we are going out to a new procurement. We met our first goal yesterday when we went out with a solicitation or an RFI for a commercial off-the-shelf solution. Our next target date is June, when we hope to make an award at that time because we don't want to tell the winning vendor how to do their business. We want to work with them collaboratively to ensure that we are off the mainframe by September 2015. We will work with them to get the more refined schedule out.

As far as to cost, preliminary market research shows that with a commercial off-the-shelf solution, we anticipate a 10 to 20 percent lower cost in the total life-cycle of the solution.

Mr. BARBER. I want to thank the Chairman again for convening the hearing, the witnesses for coming. I just hope that we can get these processes moving faster, more efficiently, and be better stewards—I think we all need to be—of the taxpayers' money.

I know you are working hard at this, but we need to succeed, and we need to do it soon and in a very cost-effective way. I wish you the best of luck, and thank you for coming here today.

Mr. DUNCAN. Thank the Ranking Member, and I will recognize for the last questions, because they are calling votes as we speak, for 5 minutes, and then we will wrap it up.

The gentleman from Texas.

Mr. O'ROURKE. Thank you. I want to get to the issue of accountability and, again, always view issues through the perspective of being a resident of the border and through the eyes of my constituents, one of the poorest communities in this country, a community that has 22 million crossings across our border every year. Those crossings are fundamental to economic opportunity and job creation that have in El Paso and paramount to a quality of life that we want to maintain there. So I appreciate the efforts to improve that through faster crossing times, implementing technologies that will allow for that. But it is also hard to go back to those folks in El Paso who are really struggling to get by, who are waiting in these long border lines, and tell them that we have spent $240 million so far to achieve it now turns out two of the five steps that we need to achieve, that we have wasted money without much accountability to it.

So a couple of questions. First, to Mr. Armstrong, $240 million has bought us secondary inspection and high-performance primary query. When it comes to these modifications to the TECS system, how much will it cost us to deliver the three remaining parts of that 5-step process?

Mr. ARMSTRONG. So we have spent $240 million to date, and let me point out that it is not just on those two pieces of functionality. I talk about those in terms of the results that we have achieved. We have actually done work in all five areas. Even in the PIP process, we have done requirements development, but we did not go on to start building things because there was budget uncertainty. So each one of the five projects, there has been work going on concurrently.

Mr. O'ROURKE. Understood, but just in the essence of time, how much will it cost us when we are done?

Mr. ARMSTRONG. So the current life-cycle cost estimate, which was just completed, is $693 million.

Mr. O'ROURKE. Thank you. What are the—to Mr. Armstrong, to Mr. Michelli, if we have time, I would love to hear from the representative from the GAO—what are the consequences when we miss our budget targets, when we spend more than we committed to spending? What are the consequences to the contractors? What are the consequences to you and the people who work for you? What is the accountability that we have in DHS for these mistakes

that have been made so far? I will ask Mr. Armstrong first and then turn to Mr. Michelli.

Mr. ARMSTRONG. Well, you know, all of these objectives are laid out in the performance plans for my program managers. So both my program manager over this program, my executive director that oversees all of our passenger processing, myself, my deputy, we all have performance milestones within our performance plans with respect to the delivery of this program.

Part of the re-compete of the contract is the old contract didn't have a whole lot of avenues for accountability in it. I am hopeful that the new one will and that we can hold the vendor more accountable for delivery. To the point that you asked me earlier, we have a lot more Government staff on-board now than we did, say, 10 years ago; so the mix of Government-to-contract employees overseeing this program is much greater than it was in the past. So I am confident that we are going to deliver within our budget and there hasn't been more than a $7 million swing in any of our lifecycle cost estimates by the middle of fiscal year 2016.

Mr. O'ROURKE. For Mr. Michelli, and I believe I am quoting from the GAO report. In September 2011, ICE entered into a contract with Raytheon to serve as a prime contractor for TECS Mod. In 2012, the program began to experience technical issues, which resulted in a delay of approximately 7 months and the decision to defer or remove approximately 70 percent of the requirements Raytheon was hired to complete. What are the consequences to Raytheon?

Mr. MICHELLI. So, for any vendor, we provide a CPARS, which is a rating on the performance, so we would rate them appropriately. They also in their contract have an award fee, and we would adjust that award fee appropriately based on the requirements of the——

Mr. O'ROURKE. Can you tell us how we have adjusted downward the award fee to Raytheon due to their performance?

Mr. MICHELLI. I would be happy to get back to you once I consult with the contracting office. I am not sure what the sensitivity of that is.

Mr. O'ROURKE. Okay. For the last word, I have got 10 seconds, Mr. Powner. Anything on that theme that you would like to comment on?

Mr. POWNER. Yeah, I think you are spot-on. I think there needs to be more accountability, not only within the Department of Homeland Security, but with those contractors. I think a best practice up-front is you sit down with the contractor and demand a meeting at a very high level and talk about what a priority this is for the Department of Homeland Security with folks probably even above these two individuals' levels, because you get the A team men if you are the squeaky wheel.

They are going to be competing with a lot of programs in the Federal Government. Those contractors have a lot of other Federal contracts. The program that is the squeaky wheel, that you get a very high-level individual saying that I am on top of this, and I am going to watch the performance of this contract and how things are going, that would help.

Mr. O'ROURKE. Thank you. I appreciate that.

Mr. Chairman, thank you.

Mr. DUNCAN. I want to thank the witnesses, Mr. Powner, Mr. Armstrong, Mr. Michelli, for your valuable testimony today. I apologize that the hearing is going to be cut short due to votes.

There are a lot of other questions that we have as we pursue how we proceed from here and make sure that we are good stewards.

You know, these hearings aren't the grooviest topics. They are not the Benghazis or the IRS targeting or all of that, but I think it is important, as you have seen today, on both sides of the aisle, we are very concerned about how taxpayer dollars are being spent, to make sure that we are getting the most bang for the buck and that we don't go so far down the road, have to stop, retrace our steps and start over.

So I want to thank the Members of the subcommittee for their questions and participation. The Members of the subcommittee may have additional questions for you guys, and we will ask those witnesses if they will respond to those questions in writing.

So, without objection, the subcommittee will stand adjourned.

[Whereupon, at 11:23 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR DAVID A. POWNER

Question 1. The DHS chief information officer rated the TECS Mod program for ICE as medium-risk and CBP as moderately low-risk. In addition, the Program Accountability and Risk Management Office rated the program as high-value, low-risk.

Do you believe the Department needs to reevaluate the criteria by which it considers these large-scale IT projects high-risk and in need of a TechStat review or health assessment?

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

Question 2. One of the subcommittee's biggest concerns with the review process for an IT project of the size of TECS is that the appropriate risks were never identified, whether it is with identifying the appropriate requirements needed or that smaller problems snowballed and were never identified until the whole program was put on hold.

How would you recommend these risks be corrected so that we don't end up in this situation again in the future?

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

Question 3. What grade (A,B,C,D,F) would you give CBP and ICE 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.

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR CHARLES R. ARMSTRONG

Question 1. If DHS had conducted a TechStat review of the TECS modernization effort, could that have helped to identify performance lapses and recommend corrective actions to get the modernization effort back on track? What steps have you taken to ensure that high-risk, high-value IT programs like TECS Mod will be identified as such in the future?

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

Question 2a. According to a copy of the Acquisition Program Baseline CBP recently submitted to DHS that was provided to the subcommittee, TECS Mod's costs have decreased by about $30 million, while the end-date for the program has been pushed out to the middle of 2016.

Can you explain how the program will cost less but take longer to complete? Do CBP's revised plans for TECS Mod envision a reduction in functionality—and if so, what does the reduction consist of?

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

Question 2b. In that same revised APB, CBP altered, or in some cases removed key TECS Mod performance parameters. In practical terms, please explain what these changes will mean for the overall performance of the system, especially for the CBP officer at a port of entry.

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

Question 3. The current request for proposal has been protested by three of the four competitors and, it is my understanding, that the CBP withdrew the award before the GAO could rule. After more than a year, it is my understanding that the CBP is going to simply recomplete the contract based on the same RFP.

To what extent has CBP considered extending the current contract?

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

Question 4a. According to the GAO report, the TECS modernization effort should result in the ability to better match names from foreign alphabets and improve the flow and integration of data between CBP and its partner agencies.

Looking back at the tragic Boston marathon bombings, are there capabilities that may help prevent similar events from occurring in the future?

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

Question 4b. If TECS had been modernized fully last year, could TECS have increased the alert and awareness on Tamerlan Tsarnaev?

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

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR THOMAS P. MICHELLI

Question 1a. Did anyone within your office at ICE reach out to the DHS CIO to initiate a TechStat review of your TECS Mod efforts in order to identify performance lapses and recommend corrective actions to get the modernization effort back on track?

Question 1b. What steps have you taken to ensure that high-risk, high-value IT programs like TECS Mod will be identified as such in the future?

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

Question 2. The cost of the ICE TECS Mod program before the rebaseline was $800 million. What will the new life-cycle cost be?

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

Question 3. ICE recently commissioned a technical assessment by MITRE to identify potential commercial-off-the-shelf solutions for its TECS Mod program. Please describe the results of this study and how ICE intends to incorporate those results in its planning moving forward? Will you please provide the results of this assessment to the subcommittee?

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

Question 4. Do you believe you are using the DHS OCIO's risk management processes effectively? Do you think problems with your portion of TECS Mod could have been escalated earlier on to address them?

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

Question 5a. According to your statement, ICE "anticipates the full life-cycle cost to be less than the original $818 million due in large part to an increased use of commercial off-the-shelf products that will require less custom development and ongoing support."

Whether it is SBINet or high-cost IT programs, the committee has heard that COTS products alone will reduce costs but this seems rarely the case because there's usually more work needed to adapt the technologies to operational needs. What assurance does the taxpayer have that use of COTS in this case will reduce costs? What concrete evidence do you have to show that COTS in this type of IT environment will result in cost savings?

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

Question 5b. Will a single COTS product satisfy all of ICE's requirements? If not, what additional functionality will be required and how will that functionality be delivered?

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

Question 6. You mentioned during the hearing that ICE's "preliminary market research shows that with a commercial off-the-shelf solution, [ICE] anticipate[s] a 10 to 20 percent lower cost in the total life cycle of the solution." Can you explain where these savings are coming from and why these savings were not identified in the original APB?

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

○