

S. Hrg. 113–296

THE DEPARTMENT OF HOMELAND SECURITY AT 10 YEARS

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

A PROGRESS REPORT ON MANAGEMENT, MARCH 21, 2013

**HARNESSING SCIENCE AND TECHNOLOGY TO PROTECT NATIONAL
SECURITY AND ENHANCE GOVERNMENT EFFICIENCY, JULY 17, 2013**

**EXAMINING CHALLENGES AND ACHIEVEMENTS AND ADDRESSING
EMERGING THREATS, SEPTEMBER 11, 2013**

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



DHS AT 10 YEARS — 2013

THE DEPARTMENT OF HOMELAND SECURITY AT 10 YEARS

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

A PROGRESS REPORT ON MANAGEMENT, MARCH 21, 2013

**HARNESSING SCIENCE AND TECHNOLOGY TO PROTECT NATIONAL
SECURITY AND ENHANCE GOVERNMENT EFFICIENCY, JULY 17, 2013**

**EXAMINING CHALLENGES AND ACHIEVEMENTS AND ADDRESSING
EMERGING THREATS, SEPTEMBER 11, 2013**

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

80–224 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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan	TOM COBURN, Oklahoma
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE McCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	MICHAEL B. ENZI, Wyoming
TAMMY BALDWIN, Wisconsin	KELLY AYOTTE, New Hampshire
HEIDI HEITKAMP, North Dakota	JEFF CHIESA, New Jersey

RICHARD J. KESSLER, *Staff Director*

JOHN P. KILVINGTON, *Deputy Staff Director*

MARY BETH SCHULTZ, *Chief Counsel for Homeland Security*

TROY H. CRIBB, *Chief Counsel for Governmental Affairs*

SUSAN B. CORBIN, *DHS Detailee*

CARLY COVIEO, *Professional Staff Member*

KAYLEE M. MYHRE, *AAAS Fellow*

CARLA D. COTWIGHT-WILLIAMS, *AAAS Fellow*

JASON M. YANUSSI, *Senior Professional Staff Member*

HARLAN C. GEER, *Senior Professional Staff Member*

BLAS NUÑEZ-NETO, *Senior Professional Staff Member*

KEITH B. ASHDOWN, *Minority Staff Director*

CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*

DANIEL P. LIPS, *Minority Director for Homeland Security*

MONICA C. SANDERS, *Minority Senior Counsel*

KATHRYN M. EDELMAN, *Minority Senior Investigator*

WILLIAM H. W. MCKENNA, *Investigative Counsel*

MARK K. HARRIS, *Minority U.S. Coast Guard Detailee*

LAURA W. KILBRIDE, *Chief Clerk*

LAUREN M. CORCORAN, *Hearing Clerk*

CONTENTS

Opening statements:	Page
Senator Carper	1, 265, 437
Senator Coburn	4, 276, 440
Senator Johnson	5
Senator Heitkamp	20
Senator Ayotte	22
Senator Baldwin	25
Senator Chiesa	462
Prepared statements:	
Senator Carper	45, 307, 483
Senator Coburn	48, 486
Senator Chiesa	490
Closing statement:	
Senator Carper	485

WITNESSES

THURSDAY, MARCH 21, 2013

Hon. Eugene L. Dodaro, Comptroller General of the United States, U.S. Government Accountability Office; accompanied by Cathleen A. Berrick, Managing Director, Homeland Security and Justice	7
Hon. Jane Holl Lute, Deputy Secretary, U.S. Department of Homeland Security	10
Hon. Elaine C. Duke, Former Under Secretary for Management, U.S. Department of Homeland Security	34
Hon. Richard L. Skinner, Former Inspector General, U.S. Department of Homeland Security	35
Shawn Reese, Analyst in Emergency Management and Homeland Security Policy, Congressional Research Service, Library of Congress	38

ALPHABETICAL LIST OF WITNESSES

Dodaro, Hon. Eugene L.:	
Testimony	7
Prepared statement	50
Duke, Hon. Elaine C.:	
Testimony	34
Prepared statement	113
Lute, Hon. Jane Holl:	
Testimony	10
Prepared statement	99
Reese, Shawn:	
Testimony	38
Prepared statement	127
Skinner, Hon. Richard L.:	
Testimony	35
Prepared statement	119

APPENDIX

Responses for post-hearing questions for the Record from:	
Mr. Dodaro	136
Ms. Lute	142
Ms. Duke	260
Mr. Skinner	262

IV

WEDNESDAY, JULY 17, 2013

Page

Hon. Tara J. O'Toole, M.D., MPH, Under Secretary for Science and Technology, U.S. Department of Homeland Security	268
David C. Maurer, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office	273

ALPHABETICAL LIST OF WITNESSES

Maurer, David C.:	
Testimony	273
Prepared statement	326
O'Toole, Hon. Tara J.:	
Testimony	268
Prepared statement	309

APPENDIX

Responses for post-hearing questions for the Record from:	
Ms. O'Toole	337

WEDNESDAY, SEPTEMBER 11, 2013

Hon. Tom Ridge, President and Chief Executive Officer, Ridge Global, and Former Secretary, U.S. Department of Homeland Security	442
Hon. Jane Harman, A Former Representative in Congress from the State of California	445
Thad W. Allen, Admiral, U.S. Coast Guard (Retired), and Former Commandant, U.S. Coast Guard	448
Hon. Stewart A. Baker, Former Assistant Secretary for Policy, U.S. Department of Homeland Security	451

ALPHABETICAL LIST OF WITNESSES

Allen, Thad W.:	
Testimony	448
Prepared statement	505
Baker, Hon. Stewart A.:	
Testimony	451
Prepared statement	515
Harman, Hon. Jane:	
Testimony	445
Prepared statement	501
Ridge, Hon. Tom:	
Testimony	442
Prepared statement	492

APPENDIX

Additional information from Mr. Allen	523
Responses for post-hearing questions for the Record from:	
Mr. Ridge	553

THE DEPARTMENT OF HOMELAND SECURITY AT TEN YEARS: A PROGRESS REPORT ON MANAGEMENT

THURSDAY, MARCH 21, 2013

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Thomas R. Carper, presiding.

Present: Senators Carper, Baldwin, Heitkamp, Coburn, Johnson, and Ayotte.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. The hearing will come to order. To all of our guests and our witnesses, welcome. It is good to see you all.

At the beginning of each Congress, as we all know, the Government Accountability Office (GAO) issues something called a list of High-Risk Government Operations that leave our government and our taxpayers exposed to waste, fraud, or abuse, or which pose management challenges that threaten crucial government services. I have always considered this list as a to-do list for Congress, particularly for this Committee, and GAO's updated high-risk list will heavily influence our Committee's governmental affairs agenda for this Congress.

We also just marked, as you know, the 10th anniversary of the date on which the Department of Homeland Security (DHS) officially opened its doors. We plan to mark this milestone throughout the year by holding a series of hearings intended to take stock of how far the Department has come in maturing, how well it is doing in executing its core missions, and how we can help them do even better.

Our goal here, and this is one suggested by Senator Coburn, is we do a series of hearings from top to bottom, A to Z, after which we would work on reauthorization for the department. We have never done that in 10 years. It is time.

This hearing fits into both of those categories: One, our DHS oversight responsibilities; and second, the high-risk list.

From a government affairs perspective, the Department of Homeland Security's management challenges appear, again, on GAO's high-risk list, although GAO readily acknowledges that progress is being made. Like other agencies across the Federal Government,

the Department has grappled in recent years with a number of issues related to acquisition, to financial management, and to human capital, among others. Unlike some of those other agencies, though, DHS is moving the needle.

As we all know, sound and effective management practices are, of course, critical to the Department's ability to carry out all of its Homeland Security responsibilities, whether we are talking about cybersecurity, border protection, disaster response, or any of its other many missions. As we look back on the past decade, I think it is important to remember the circumstances in which the Department was stood up. The Homeland Security Act passed by Congress to create the Department was signed into law November 25, 2002. The Department opened its doors on March 1, 2003. So in just over 4 months, some 22 different agencies from across the government, with different cultures and different management practices and philosophies, were merged into a brand new department.

In those early days at the Department, the focus of both the Administration and Congress was on moving quickly to prevent another 9/11-type attack on our homeland. Management took a back seat to those efforts. Former Department of Homeland Security Inspector General Richard Skinner, who is here today again as a witness, confirmed this fact when he testified before our Committee last year. The management foundation of the Department really got shortchanged in those early days. It has taken years to dig out of the hole that the initial lack of a strong management foundation left.

That said, I want to give credit where credit is due. GAO's most recent report confirms that there has been considerable progress at the Department in integrating the components that were folded into it and in strengthening the Department-level management that overlays those components. The latest high-risk report includes a fair amount of good news because GAO acknowledges this progress and has narrowed the areas that remain on the high-risk list.

The Department also deserves credit for its detailed, aggressive plan to address all of GAO's concerns in its high-risk report, which I believe is unique among all the agencies on the high-risk list. I want to briefly review some of the major improvements to management at the Department of Homeland Security, and in doing so, I would agree with GAO that committed leadership at DHS has been critical to driving progress in these areas.

The Department is on the doorstep of having a clean financial audit for the first time. Last year, the Department was able to get its financial systems in good enough order to attempt a full financial audit. That was a major milestone. That leaves the important goal of now passing a financial audit. And I know that the Secretary, the Deputy Secretary, and their team are prepared to make the final push to earn a completely clean audit. If they are successful, it will be a major achievement.

Some of you heard me talk about a friend of mine. You would ask him how he is doing and he says, "Compared to what?" Well, compared to the Department of Defense (DOD)—we love them, but they were stood up, what, 65 years ago and they are not auditable. They have not passed a clean financial audit. And here we are, an

agency 10 years, also very complex, knocking on the door. So it will set a good example if you can get this done for our brothers and sisters over at DOD. Now, I know they are committed, especially the Secretary is committed to getting this done for them, too.

When the Department was stood up 10 years ago, there was no framework for accountability. There was also no guidance on which responsibilities lay with headquarters, and which responsibilities lay with the various components that make up the Department. Whenever that kind of Wild West environment exists in government, there is sure to be a lot of wasteful spending and inefficiency, and there was.

Now, the Department has made clear who is in charge of what. This new, more disciplined environment will better enable the Department to control costs at the various components and better ensure that all of them operate as a more cohesive, effective, and accountable agency.

The Department used to have an abysmal record when it came to awarding contracts without competition, but the Departmental leadership has been aggressive in turning that record around. Just last month, the report from the Office of Inspector General (OIG) showed that the spending on non-competitive contracts in fiscal year 2012 fell by almost 89 percent from fiscal year 2008 levels. That means about \$3 billion in contract dollars that were previously spent without competition are now being spent in a manner that gets better value for taxpayers' dollars. And the Department, as the governmentwide procurement data shows, actually has a better record on competing contracts now than most other major Federal agencies.

The Department has also revamped its process for identifying technological solutions at the border. The Department has moved away from the SBInet model, which was a mega-contract to a single company to build a virtual fence across the Southern border. It was an effort that went forward without the necessary work to identify what the Border Patrol really needed. As a result, it quickly became cost prohibitive and did not ever deliver the capabilities that were promised. The Department now is implementing a more rigorous process to identify needs, sector by sector across the border, and where possible, use commercially available technology off the shelf to drive down costs and enable our Border Patrol agents to become ever more effective.

In the area of information technology, the Department is now at the forefront of the Federal Government's efforts to consolidate data centers and move services to the cloud. These efforts save money and enable the Department and its employees to achieve better results.

Finally, there is no doubt that the response to Superstorm Sandy—we had a hearing here just yesterday on this—but that response to Superstorm Sandy shows how much the Federal Emergency Management Agency (FEMA) has improved since Hurricane Katrina struck the Gulf region in 2005. Simply put, this improvement would not have been possible without better management. For example, when Hurricane Katrina hit, FEMA did not have the necessary contracts in place to get needed assistance to victims in a timely manner. When Hurricane Sandy hit 7 years later, FEMA

was prepared, and as a result, there is a dramatic reduction in no-bid contracts compared to the Hurricane Katrina response.

These are all significant achievements and our witnesses will discuss for us today other examples. But I do not want to whitewash the serious remaining challenges with DHS management that remain on the high-risk list. The Department still has work to do—we know that—as both the Comptroller General and Deputy Secretary Lute will discuss. As I like to say, the road to improvement is always under construction, and my colleagues have heard me say a million times, everything I do, I know I could do better. The same is true for all of us. The same is true for this Department.

For example, this Department still does not have a comprehensive financial management system that gives the Secretary real-time visibility over the spending of 22 department components. Workforce morale at DHS remains the lowest of all major departments. I do not think that is going to be the case for much longer, though. Many major acquisitions have exceeded cost estimates or fall short of promised performance.

This hearing also provides a timely opportunity to discuss the possible impact of the fiscal year 2013 full-year Continuing Resolution (CR) on the Department. I am concerned about the \$20 million cut that DHS management and the Secretary's office would take under the bill and I want to hear from our witnesses today about the likely impact of those cuts. I am also concerned that the level of funding for consolidation of the Department at St. Elizabeths is insufficient to support the next phase, which could bring the leadership and operations center to one location and realize efficiency and effectiveness.

Both the Administration and Congress need to work together to resolve these remaining high-risk areas, and we will. I welcome our witnesses today. We look forward to working with you and the dedicated people that you lead so that in 2 years, when GAO releases its high-risk list, and we are sitting here talking about GAO's high-risk list and the management challenges facing the Department of Homeland Security, we hope they are off that list, making our Nation more secure, and putting our finances in better shape, as well.

And now, Dr. Coburn, the floor is yours, and then I am going to call on Senator Johnson. He has to leave here. He is not going to be here to ask any questions, but I want him to just make a brief statement. He is so good about attending our hearings, so I am going to ask you to say something before you leave. Thank you.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. First of all, Mr. Chairman, I would like for my opening statement to be made part of the record, the written one.

Chairman CARPER. Without objection.

Senator COBURN. The Congressional Research Service (CRS) recently put out a memo by Shawn Reese about the definition of what homeland security is, and any organization that does not know what it is really all about is going to flounder in certain areas. The concern I have had is that we have taken what was intended to be Homeland Security and made it an all-hazards risk prevention agency, which is an impossibility. You cannot eliminate

all risk, nor even if we could, we could not afford to. So I look forward to all of your comments today and a frank discussion.

Senator Carper and I, over the next 4 years, will oversee every nook and corner of Homeland Security for the transparency that needs to be there and also to see the improvement, and I appreciate his cooperation and his leadership in doing so. I think it is healthy for you all. It is certainly healthy for the Congress. We make a lot of decisions a lot of times without the input that we need to have from the agencies, and getting to know what you do and how you do it and to understand that better can help us as we direct funds.

So I am thankful for your work and I am thankful for your dedicated service and look forward to hearing your comments.

Chairman CARPER. Thank you, sir. Senator Johnson.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Mr. Chairman, I was not prepared, but I will take the opportunity, first of all, to certainly voice my gratitude for both the Chairman and Senator Coburn in terms of the way you are going to be conducting this Committee in the future.

I think it is a really good sign that we are going to try and reauthorize this Department. The Department of Homeland Security should be playing a pretty vital role in the security of this Nation. We are facing incredibly serious threats.

I have always been concerned since I came here a couple years ago, was it really the right move? I mean, you take, what is it, 22 different agencies and try and combine them into one with the added layer of bureaucracy. I am not sure that is really the most efficient business model.

If I had time to ask questions, the one question I have always had is, it is about a \$50 billion a year agency. The Defense Department is about a \$600 billion a year agency. Wal-Mart and ExxonMobil are about \$450 billion a year companies. They get audited every year. A \$50 billion company, it starts up, it gets audited every year. It does not seem to have much of a problem doing so. So I have always been scratching my head wondering why cannot the Department of Defense, why cannot the Department of Homeland Security pass an audit?

So I guess I would look to private business practices and take a look at what is different in government that prevents that type of accountability, because the only way that the Department of Homeland Security is going to be able to fulfill its very important mission is through a very accountable, a very efficient, a very effective management style. And I do not know how you can obtain that accountability if you cannot pass a basic audit that private industry businesses that size do all the time.

And, by the way, if the management of those companies do not pass an audit now under Sarbanes-Oxley, I mean, they go to jail or they certainly face criminal charges. So I think we need to bring that type of dedication, those types of private sector disciplines to government to make sure that we are auditable, that we are efficient, and that we are effective.

Thank you, Mr. Chairman.

Chairman CARPER. That is a great point. When you jammed together 22 different agencies 10 years ago, different cultures, different financial systems, different accounting systems, it is not easy. And 65 years later, the Department of Defense is still struggling with it.

I think there are really two keys, and one of those we will talk about here today, is leadership. It is leadership from the Department of Defense and Leon Panetta, now Chuck Hagel, saying, we have to get this done. We are going to make this a priority. And in this case, Secretary Napolitano and Deputy Secretary Lute.

And the other thing is our responsibility. We are working with GAO, saying, this is a priority. And we are going to keep holding these hearings. We are going to do our job on oversight until we finally achieve this.

And to their credit in this Department, they are coming along and it is good. It is like turning an aircraft carrier, but they are coming. That aircraft carrier is a big one over at DOD. They are turning that one, too, and in a couple of years, hopefully we will be singing their praises, as well.

Senator JOHNSON. Again, my point was not to be critical—

Chairman CARPER. I understand.

Senator JOHNSON [continuing]. But, again, just really being encouraging in the direction we have to go. Again, I am highly encouraged with what this Committee has set out to do here and I think this is the right path that we are on. So, again, I just want to be encouraging.

Chairman CARPER. Senator Johnson here comes out of the private sector, as Tom does, who has done any number of things in his life, but he understands full well the value of being able to measure things. What we cannot measure, we cannot manage. And thank you for the role that you play on this Committee. You are just a very good addition to this Committee.

All right. Having said that, let me just briefly introduce our witnesses. The first panel includes not two but three very impressive public servants: Jane Holl Lute, who is Deputy Secretary of the Department of Homeland Security, and Gene Dodaro, Comptroller General. Accompanying Mr. Dodaro is Cathleen Berrick of GAO. She is not here to testify, but she is here to field the really tough questions so that when he is stymied and does not know what to say—which has never happened before in my time here—she can jump in and help out. We appreciate both of you taking the time to be with us to talk about GAO's high-risk update and the progress made by the Department, and we look forward to continuing to work with both of you and your folks.

I think, Deputy Secretary Lute, ordinarily, as a matter of protocol, the Committee would ask you to be our lead-off hitter, but if you are willing to do this, I think it might make sense for Mr. Dodaro to set the stage for us by providing us with a little bit of a broad overview and some context of the high-risk series and the summary of how the High-Risk List relates to the specific subject of our hearing, the management of the Department of Homeland Security.

If you are comfortable with that, we will just ask him to lead off and you can try to move him around the bases, all right. Mr. Dodaro, you are recognized. Thank you. Thank you all.

TESTIMONY OF HON. EUGENE L. DODARO,¹ COMPTROLLER GENERAL, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY CATHLEEN A. BERRICK, MANAGING DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. DODARO. Thank you very much, Mr. Chairman, Ranking Member Dr. Coburn, Senator Johnson. It is a pleasure to be here today to talk about GAO's high-risk update.

As you point out, we have been doing this the beginning of each new Congress since 1990. This past year, we provided the update just recently. I am very pleased that this Committee has already held hearings on two areas under the high-risk list, on the Postal Service financial condition and on the cybersecurity area, and is considering legislation which is necessary to get those items off the list. In many cases, it is the agency's actions that are required, but in a number of areas that are high risk, it is really also up to the Congress to pass legislation.

Now, we have reported this year notable progress in most of the areas—there are 30 of them—on the high-risk list, and this is a very good 2-year interim report by historical standards. So there is a lot of effort going into these areas.

And I would credit this because the Congress has passed several pieces of legislation that are important to getting areas off that list. The agencies have worked hard. And the Office of Management and Budget (OMB) has worked with GAO and the agencies to convene meetings to focus on the high-risk areas.

In two of the areas, we noted enough progress that we removed them from the list. One is interagency contracting. We put it on in 2005, and this is a good practice for agencies if implemented properly. But we found they were doing it, not within scope. The roles and responsibilities were not clear. Probably the most notable example is when interrogators were hired for Iraq off of a General Services Administration (GSA) information technology (IT) contract. And so there clearly needed to be some changes.

Now, at congressional direction, the Federal Acquisition Regulation (FAR) was changed and improved to require a best procurement approach, which required documentation of the decision, and written agreements on spelling out roles and responsibilities. Also at Congress' urging and direction, there was a requirement added for a business case to be developed and approved at senior levels within the Department before new interagency contracts could be put in place. And then Congress also asked for a series of audits by the Department of Defense IG, and that Inspector General found less problems over time.

So we are satisfied that the mechanisms are in place. There is demonstrated progress. And we have removed them from the list.

The other area is the Internal Revenue Service (IRS) Business Systems Modernization (BSM). We put that on the list in 1995. IRS

¹ The prepared statement of Mr. Dodaro appears in the Appendix on page 50.

was mired in technical and management weaknesses with that system. Over the years, they have made steady improvement. Congress has required an annual expenditure plan from IRS, which GAO was required to review.

And IRS finally has made measurable progress. They have installed the first module of their new system, which allows for daily updating of taxpayer accounts. This is a huge change. It enables refunds to get out faster. It enables them to send notices faster and to field questions and helps in enforcement areas.

They also have instituted about 80 percent of all the best practices for IT investment management and 100 percent of those best practices for project management, which is a notable achievement. They have also been rated, their Software Acquisition Department, at a Computer Maturity Model 3 Level by the Software Engineering Institute Standards, which by industry standards is a very good mark.

Now, for both of these areas, a point that you made, Mr. Chairman, in your opening statements, Senator Coburn, Senator Johnson, all of you touched upon the importance of congressional oversight. These two areas have had sustained congressional oversight over that period of time and good leadership by the agencies, which are the two key ingredients. Virtually every area we have taken off the list, and we have taken a third of them off over the years, have been attributable to those two key ingredients being in place.

Now, while they are off the list, they are not out of sight. We continue to monitor what is going on to make sure that the progress is sustained.

We also evolved one of the areas this year, which is modernizing the financial regulatory system for the United States to include the financial management problems at the Federal Housing Administration. They are below the capital requirement needed. They took on a lot more risky loans during the recessionary period where the private sector backed out of the mortgage market. So we wanted to highlight those changes.

But also, as Congress resolves the conservatorships of Fannie Mae and Freddie Mac, you need to take into account the implications for the Federal Housing Administration and it really needs to be an integrated decision as those efforts are resolved as to what the proper Federal role should be in the Federal housing mortgage market.

Now, we added two new areas to the list this year, as well. The first was limiting the Federal Government's fiscal exposure by better managing climate change risk. I am very concerned about this area and the financial risk. The Federal Government owns hundreds of thousands of properties, many Defense installations along the coastal areas. The Federal Government owns 29 percent of the land in the United States in terms of managing it and dealing with erosion and other issues.

The Federal Government runs two of the largest insurance programs. One is the Flood Insurance Program, and the Flood Insurance Program already owes the Treasury Department over \$20 billion, and has not made a principal payment back on that debt since 2010. The levels have just been raised to allow them to borrow additional money to help out in Hurricane Sandy. Congress has

passed some legislation recently, but it needs to be implemented effectively.

And also the disaster aid that is provided. The criteria for providing disaster aid really has not been changed since it was established in 1980. Right now, it is \$1.35 per person per State. It was not adjusted for inflation for a 13-year period of time. We estimated if it had been adjusted for inflation, the Federal Government would not have been involved in 25 percent of the disaster declarations put in place over time.

We also do not budget for major disasters, which is a real problem, particularly given our precarious financial situation right now. The only thing that is budgeted for are 5-year historical averages of disasters under \$500 million. So virtually, of the tens of billions of dollars that have been appropriated over the years, in the last decade over about \$140 billion, well over 80 percent of that, almost 89 percent of it, has come through supplemental appropriations which were not budgeted for.

So we have many ideas for improvements in these areas. It is very important.

It is also related to the last area that we added to the high-risk list, which is a gap in environmental satellites. The polar orbiting satellites, in particular, provide global coverage of the surface of the earth twice a day, morning, afternoon and evening orbits, and this data feeds the weather prediction models for 3-, 4-, and 7-day forecasts. Because of procurement and management problems over the years, there is a gap that could be anywhere from 17 to 53 months where we may not have this information. It is critical. If we had not had the satellite data in Superstorm Sandy, one credible organization predicted that storm to go out to sea and not hit New Jersey. So there would not have been adequate warnings for the residents.

So we have encouraged National Oceanic and Atmospheric Administration (NOAA) and DOD to put contingency plans in place, but they need to be properly executed and this is an area for congressional oversight, to make sure that these gaps do not create real problems that could lead to loss of life, property, and other economic damages over time.

Now, we also narrowed the areas for three of the high-risk areas, including the Department of Homeland Security. We found that, over the years, the department has made good progress in its initial implementation. For example, they have created the National Response Framework for addressing disaster assistance. They have hired, produced, and have in place workforces. They have stood up new agencies, like the National Cybersecurity Communications Integration Center. So we felt comfortable narrowing them to the management challenges that they have.

And for most of the management challenges—you have highlighted some of the major progress that has been made, so there has been some progress, but there really needs to be additional progress. DHS needs to get a clean audit opinion for 2 years to get off the high-risk list. They need to have financial systems in place. Major acquisitions are still overrunning costs and are not being delivered on time with the expected type of product that is needed to execute the mission. And there are many other areas.

Now, we identified 31 specific actions that needed to be addressed to come off the list. The Department has fully addressed six; two, mostly addressed; 16, partially; and seven, they have initiated action. So that provides a scorecard. They have an excellent roadmap now. They just need to execute it.

And we are committed—I think we have had a very good, constructive dialogue and partnership with DHS to provide clarity. They have stepped up, have plans in place, know how to do it, and if they execute those plans, I think they will continue to make excellent progress.

So I thank you for the opportunity to be here today. I will be happy to answer questions once the Deputy Secretary provides her statement.

Chairman CARPER. Thanks very much for that overview and for some of the specifics on the Department and for being, really, a good partner with us as we try to help DHS do the work that they already do even better.

All right. Secretary Lute, you are on. Welcome. Glad to see you.

**TESTIMONY OF HON. JANE HOLL LUTE,¹ DEPUTY SECRETARY,
U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. LUTE. Thank you very much, Chairman Carper, Ranking Member Coburn—good to see you again—distinguished Members of the Committee. I am grateful for the opportunity to appear before you today to discuss the Department of Homeland Security and our progress over the past 10 years.

Our 10-year anniversary provides an important opportunity to consider how DHS has evolved to fulfill its original purposes and reflect on further work that has to be done to realize full potential.

Now, I do not know, Dr. Coburn, Shawn Reese, but if he were sitting here, I would tell him he is behind in his reading. I am not a politician. I am not a diplomat. I spent a long time as a soldier and I am an operator. I run things. And I describe the mission of Homeland Security in simple terms. Our job is—as part of the Federal Government—to help create a safe, secure, resilient place where the American way of life can thrive.

And in order to meet that job, in order to fulfill that mission, we focus on five main things: Preventing terrorism and enhancing security; securing and managing our borders; administering and enforcing our immigration laws; ensuring the Nation's cybersecurity; and building national resilience.

We do not do any of this alone. While DHS plays an important role, we view homeland security as a whole community effort and, therefore, rely heavily on many partners throughout the homeland security enterprise, at the State, local, Tribal, Territorial level, across the rest of the Federal Government, in the private sector, and among the American people.

In turn, our partners, and including Congress and this Committee, which we have appreciated over the course of our lifetime. It is the reason the Department is 10 years old and not 1 year old for the tenth time. There is a big difference. We have made

¹The prepared statement of Ms. Lute appears in the Appendix on page 99.

progress over the course of these past 10 years and we intend to continue making progress.

But this Committee, in fact, the American people, have a right to expect that we can do three things. They have a right to expect that we can execute the missions that I just outlined for you. They have a right to expect that we can run ourselves. And they have a right to expect that we can account for the resources that have been entrusted to us, and we expect no less of ourselves.

DHS is, in its nature, composition, and purpose, an operational department. Yes, we have policymaking responsibilities. Yes, we have regulatory responsibilities. But we have operational responsibilities, as well. Every single day, tens of thousands of Homeland Security professionals provide essential services to the American public, from securing our borders, to processing immigration benefits, responding to disasters, patrolling the Nation's waters, safeguarding our air travel, and in countless other ways.

To carry out this mission, we must be able to recruit, hire, and retain qualified staff; budget, account, and oversee billions in financial resources; procure complex systems and services; collect, sort, and share data; maintain 24-hour communications and situational awareness; ensure appropriate security and safety for these operations; and effectively manage the hundreds of facilities and locations where our personnel are deployed.

We do these things in Homeland Security every day and we do it for the American public. To do these things, we know we have to be well staffed, well trained, and well led.

And to meet these requirements, we have worked constantly to improve our hiring processes, our acquisition and procurement processes, data management and financial systems. As a result, for example, of the effort we have made to improve our management operations across the board, for the first time since the creation of the Department in 2003, DHS has earned a qualified audit opinion on all five of its balance sheets. And I project this year, Mr. Chairman, that we will have a clean audit opinion. Perhaps we will be able to achieve a clean audit opinion for 2 years, for 2012 and for 2013. That is our aim.

I do not need to tell this Committee what an——

Chairman CARPER. I want to repeat myself. From your lips to God's ears. That would be great.

Ms. LUTE. Thank you. I do not need to tell you what an extraordinary achievement this has been, but I would like to acknowledge my colleagues from across the Department who have worked tirelessly to make this a reality under the leadership of Rafael Borrás, our Under Secretary for Management, and Peggy Sherry, our Chief Financial Officer (CFO).

The lights are on in many buildings around Washington, DC, and across the country very late into the night so that this can be achieved, and we are proud of our people who have done this. We will continue our fierce commitment to sound management practices and expect that DHS will receive that unqualified audit opinion.

We know that Congress and GAO understand the importance of effective management. When GAO placed the implementation and transformation of DHS on its high-risk list in 2003, it cited three

principal reasons for doing so. First, the sheer size of the task with respect to numbers and the complexity of transforming 22 agencies into one coherent Department. Second, the fact that many of these agencies were coming to DHS with preexisting conditions, preexisting GAO findings and other challenges to overcome. And third, because of the potential for catastrophic consequences should this effort to strengthen the security and safety of this country fail.

The undertaking has been massive and there have been many challenges, but there have also been many advantages, beginning with the men and women of the Department and their unwavering professionalism and commitment to the mission of homeland security. Similarly, in the early years, the leadership of DHS worked to build a sensible foundation from which to grow, and Congress has been indispensable to our progress, as has our important partnership with GAO, with whom we tend on nearly all matters to find overwhelming agreement.

With this help, we have made considerable progress in all key areas of management and take some measurement of satisfaction in the significant narrowing of the high-risk area in GAO's recent report. The close working relationship we have built with GAO is founded on principles of engagement, responsiveness, and mutual respect, and we are grateful for the level of coordination and professionalism that GAO displays to us in our work together. We know that their partnership has been important to the achievements we have made.

Today, we are more integrated and unified as a Department and we are able to leverage both expertise and experience to achieve our mission. There are things that are done today that were not possible before the Department was created. Two examples will illustrate this point and are indicative of the kind of Department we have become with your help.

First, the Homeland Security Surge Capacity Force was created legislatively in 2006, requiring the creation of a volunteer force made up of DHS employees who could deploy in the event of a catastrophic disaster to support survivors. On November 1, 2012, in the immediate aftermath of Hurricane Sandy, we activated the Surge Capacity Force for the first time. Within just a few days, nearly 1,200 employees from Homeland Security from across the Department—the Transportation Security Administration (TSA), Citizenship and Immigration Services (CIS), Customs and Border Protection (CBP), Coast Guard, U.S. Immigration and Customs Enforcement (ICE), Secret Service, and DHS headquarters—deployed to New York and New Jersey in support of FEMA's response and recovery effort.

These individuals communicated directly with disaster survivors regarding power restoration, emergency services, food and shelter options, and how to register for disaster assistance. They slept on ships docked offshore so that they would be close to the people they serve and not take up limited hotel space. They empowered those who had been disempowered by the storm. They were at their best for people who had been through the worst.

The second example of the things that we can do today in the Department that we could not do 10 years ago is cybersecurity. People did not even talk about it in the terms they talk about it

now. But by bringing the components and offices of Homeland Security together, we have been able to formulate a coherent strategy to defend the Federal networks in dot-gov, engage a broad community of expertise, from law enforcement to the private sector, the intelligence community, as well, to strengthen the protection and resilience of the Nation's critical infrastructure, both cyber and physical.

The point of these two anecdotes is not just that we have helped communities bounce back from disaster or that we have architected from the ground up a responsible approach to cybersecurity. The point is that the very best of what this Department is about comes from the work that we do together and from the individuals who have transformed the Department from 22 separate agencies into one cohesive and mission-driven unit whose purpose is to help create a safe, secure, resilient place where our way of life can thrive.

From a management perspective, as well, we continue to streamline and strengthen ourselves. The Secretary's efficiency reviews, begun 4 years ago, have led to DHS employees identifying 45 specific projects and initiatives that have yielded more than \$4 billion in savings and cost avoidances, savings that have been reinvested into our critical missions.

Elsewhere, as you have noted, Mr. Chairman, we have consolidated data centers, overhauled our procurement and acquisition systems, written the Federal Government's first ever guidelines on financial assistance, created clear and measurable performance objectives, have built a statistical compendium of all of our operations in Homeland Security to give us visibility into the kinds of indicators and metrics that indicate successful performance, and we have become auditable.

We know our work is not done. We know that nothing stands still. Threats continue to evolve. Technology will continue to advance. And operational demands will continue to grow. We are deeply connected to this dynamic world and we are committed to doing our very best to ensure that this country remains a safe, secure, resilient place where the American way of life can thrive. We count on our continued partnership with Congress to help us hit the mark the American people expect and deserve.

And I thank you again, Mr. Chairman, for the opportunity to appear before you today and I look forward to your questions.

Chairman CARPER. We have all heard the old saying, that is my story and I am sticking with it. That is a good story to tell and it is a great story to build on.

We have been joined by Senator Ayotte and Senator Heitkamp and Senator Baldwin, all new to this Committee, Senator Ayotte not new to the Senate. But we are delighted that you are here today to hear this testimony and to join us in asking questions.

I have prevailed on Senator Johnson just to wait for a couple minutes. He needs to go someplace else. But he asked a very good question sort of earlier. I do not know if you want to ask the same question or something else before you head out, that would be great.

Senator JOHNSON. Maybe two quick questions. This one is pretty broad.

Deputy Secretary Lute, how long have you been with the agency?

Ms. LUTE. Four years.

Senator JOHNSON. Four years. Having been there now and understanding the complexity of having 22 different agencies—again, this is all hindsight, Monday morning quarterbacking—are there any of those agencies that you think might have been restructured better someplace else and maybe should not be part of the Department? Is there any restructuring that you would, again, just in hindsight, or do you think things are pretty well comprised here?

Ms. LUTE. Thank you, Senator. I have been running organizations for a long time. I do not have too many organizational theories. You can always do things differently and make improvements. But I think if you ask any of the 22 agencies, the legacies and the offices that have come together, can they find themselves in that mission statement of creating a safe, secure, resilient place, yes, they can. Can they find themselves in any of the five missions—preventing terrorism, borders, immigration, cybersecurity, and building national resilience? Yes, they can. So, largely, for the most part, they are in the right place.

Senator JOHNSON. OK. Then just getting back to the audit, can you just describe the major reason why that has not been achievable in the last 10 years? I mean, is it the incompatibility of accounting systems between 22 different agencies? I mean, what has prevented just a complete audit?

Ms. LUTE. Well, we have made progress over every year. I mean, I would tell you at the moment, we are focused on property. I think we will be able to resolve it for 2012 and certainly going forward.

Senator JOHNSON. So it is really just the complexity of individual issues as opposed—and being able to account for that 29 percent of all land that the Federal Government operates and that is now under your jurisdiction?

Ms. LUTE. It is a tremendous challenge. It is not that we do not know what to do. It is not that we do not have the tools to do it. It is a tremendous challenge. And it is not that we lack the commitment or the help and support of our partners. We have all of those things. We will get this done.

Senator JOHNSON. So it is just the number of things you have to account for and trying to get it all—

Ms. LUTE. It is a big job.

Senator JOHNSON. OK. Thank you very much. Thank you, Mr. Chairman.

Chairman CARPER. Senator Johnson, thanks for sticking with us to ask those questions. Good questions.

Let me just start off with a question, if I could, for the Deputy Secretary. Let me focus for a couple of minutes on the next steps the Department is going to be taking to improve the management of the Department. GAO recommends that the Department track and independently validate the effectiveness and sustainability of the management improvements that have already been made. Let me just ask, how will you do that, and also, what type of reports will be available to this Committee so that we can monitor the progress that is occurring and meet our responsibilities for providing good oversight?

Ms. LUTE. Thank you, Chairman. So, we have done several things. One is to launch the Management Health Initiative, which

is really designed to create a dashboard for that at-a-glance look at critical systems and performances.

In addition, as I mentioned, we have for the first time begun to compile a statistical compendium to give us visibility into all of the resources that we have in the Department and how they are applied against those mission sets. So building this kind of business intelligence and understanding of our operation is fundamental to be able to report in a cogent and authoritative way on the accomplishments and the achievements that we have made. So we look forward to working with this Committee to get that right and to establish regularized reporting to give you the visibility we have.

Chairman CARPER. All right. Good.

We all know that management matters and good management is the platform on which agencies, frankly, businesses, execute their missions. I hope that is one of the missions that comes out of this hearing, that good management matters, and I am convinced that we have good management.

I also am encouraged we have some continuity in that management, and with, I think, Secretary Napolitano—nobody is perfect. She is not. God knows, I am not. But I think she is a very good administrator and very committed. I think you are, too. I think the fact that she is going to be staying around for, hopefully, four more years, my hope is you are going to be staying around for at least that long, and that leaves in place a very good management team.

I think over your right shoulder is Rafael Borrás. Is that the man? Rafael is the Under Secretary of Management, and a lot of what we are talking about here is actually an effort that he has led. You mentioned that and we want to acknowledge him and the team that he works with, so thanks so much.

But, Deputy Secretary Lute, would you provide us with just a couple of maybe concrete examples of in the past where weak management has really undermined the performance of the Department, and conversely, where good management has enabled the Department to better carry out its mission. So a couple of good examples of where bad management undermined the Department and its mission and maybe one or two where it is just the opposite has been true.

Ms. LUTE. Thank you, Mr. Chairman. First, if you will allow me, you will not hear me say the Secretary is not perfect. [Laughter.]

She is a terrific boss and a terrific leader for the—

Chairman CARPER. Well, I will say the Chairman here is not perfect, though.

Ms. LUTE. But I will—

Chairman CARPER. And I have known the Secretary for a long time.

Ms. LUTE. I know.

Chairman CARPER. As good as she is, she is not perfect, either. You can always do better. Tell her I said that.

Ms. LUTE. And I will accept her imperfections.

Leadership and management are things that I have paid a lot of attention to over the course of nearly 35 years of working in the public sector, in the military, in the international civil service, and in the not-for-profit sector, as well. What management needs to do very clearly is provide people purpose and pride. You do not run

organizations through derogation and putting people down. You have to say very clearly, what is our job here.

And what we have tried to do in the Department of Homeland Security—four years ago, I stood in a door jamb of one of my colleagues and said, we need to narrate the purpose of this Department in very clear terms. We need to conduct a bottom-up review of what we are doing and balance that examination against what we said is important to do. We need to get off the GAO high-risk list and we need to become auditable. So those are the kinds of examples, I think, and we have made progress in every single one of those, in every single one of those areas, if I can be allowed.

When you are creating a new department and a new enterprise—I have done this several times now in the public sector—this narration of purpose is really essential so people understand how what they have been doing now contributes to the purpose that they are being asked to perform. It is easy sometimes, particularly at the operational level, to be absorbed in the day to day. It takes a great deal of effort to sit back, develop perspective and a strategic understanding of how those discrete individual operational efforts add up to an overarching purpose.

So narrating that purpose of Homeland Security, clarifying the five mission areas, as we have done, orienting people in the direction of, are you performing these missions? Are you contributing to running ourselves? Are you contributing to our public accountability? If whatever you are doing is not in one of those three buckets, stop doing it.

So it is a particular leadership challenge when you are doing startups, one that I think that we have met, together with those who have gone before us, in establishing this Department.

Chairman CARPER. One more for you, if I could. Secretary Lute, we are in a tough fiscal environment. We are working on it. We passed a Continuing Resolution to fund the government for the rest of the fiscal year, not perfect, but it is better than stop and go, the fiscal cliff, lurching from emergency to emergency. But it is still a tough environment that we are going to be operating in for the foreseeable future.

Let me just ask, do you think you will be able to sustain and improve upon the vital management progress that has been made in the past 5 years? The Senate version of the Fiscal Year Continuing Resolution that we passed yesterday in the Senate cuts about \$17 million from the Department's management functions. Tell us, what could be the practical impact of a reduction of that nature? For example, does this put in jeopardy the Department's ability to do rigorous reviews of the component's acquisitions that GAO recommends?

Ms. LUTE. Thank you, Chairman. You do not run an operational department without the ability to hire, retain, and manage people, without the ability to acquire and procure goods and services, without the ability to run your financial systems from an accountability point of view. All of those will be affected by cuts. Things may take longer. There may be aspects of things that we do not get to as thoroughly as we would like under other circumstances. Our job is to limit any negative effects and prioritize. That is part of the leadership job.

Chairman CARPER. All right. Dr. Coburn, please proceed.

Senator COBURN. Secretary Lute, I know I appreciate your work. I hope you will have somebody stay around here to hear Mr. Reese's paper, and I think it is unfortunate you have not read it. It was published January 8. The fact is, there are some significant criticisms that you need to be aware of rather than to dismiss them, especially since it sounds like you or your staff have not read his scholarship. So I hope you will leave somebody here after you testify to hear his testimony about what his research shows and his fair criticisms and then give us an answer to it.

Ms. LUTE. I did read his paper.

Senator COBURN. You did? And so you think it is totally off base?

Ms. LUTE. I disagree with what he finds. I do think we know what our purpose is. I do think we know how to orient our missions to that purpose.

Senator COBURN. OK. That is fair.

A number of recommendations were made by the 9/11 Commission. That is a fairly remote Commission now. One is the status of TSA's effort on explosives. I would just like an update of where we are and where you are going to be on that requirement.

The other requirement that they had is on the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program. GAO found that there were 825,000 pieces of data that are not matched to the correct fingerprints. They might be fraudulent, and right now, there is no way to determine whether or not they are fraudulent. So if you could—and you do not have to answer these now. I do not expect you to know that detail and understand that.

But, to me, those represent two of the areas where we have had substantive recommendations by the 9/11 Commission that we have not achieved the goal, and both of them are significantly important to the missions of your organization. So I would hope that you would respond to me on that.

Since 2004, your agency has disbursed \$35 billion in grants. What do you know about the effectiveness and the accomplishments of those grants?

Ms. LUTE. Thank you, Dr. Coburn. We do not have the kind of granular visibility into the accomplishments that we want to have. We do know that we have created a great deal of capability across the country in those grants, and we do know that there is a need for a comprehensive approach to a financial assistance that the Federal Government, in our case DHS, provides.

We have written that approach to financial assistance. We have taken a look at everything, from understanding requirements in the grant-making area, how to build and work with the communities at the State level and local level in constructing well-written grant proposals. We have looked at the accountability and our ratio of personnel to oversight. We have a lot to do, but we have begun to make progress through that financial assistance work under the direction of our CFO, Peggy Sherry.

Senator COBURN. Do you think FEMA, at the very least, should track what grants are spent on?

Ms. LUTE. Yes, sir, I do.

Senator COBURN. OK. And are you?

Ms. LUTE. Not as well as we would like, but we are improving.

Senator COBURN. OK. GAO found that fewer than 10 percent of DHS's acquisition programs fully comply with the new acquisition policy. And I know this is a work in process, so I am not actually being critical when I make that note. I know that your intent and goal is to accomplish that. They also found that only one-third of the programs that should have had approved acquisition baselines actually do. The baselines actually are probably the most important tool for managing individual programs and conducting congressional oversight.

Having said that, what steps are you taking to hold components accountable for complying with the DHS acquisition policy? I know you have made the policy. Now, where is the management accountability to make sure the agencies are holding within that acquisition policy?

Ms. LUTE. Well, as you noted, we have drawn all of our programs under Management Directive 102. Each of the programs submit to a regular review by the Acquisition Review Board (ARB). Decisions are taken. We will not progress if we are not satisfied the questions and accountability are in line. We have instituted a lifecycle management cost model, as well, which we are imposing. And we have shut programs down that were not performing.

So we have begun to change the culture. I think we have gone a very long way. It is unthinkable that we would undertake a major acquisition without a careful review under our directives procedures of what our requirements are and exposing those requirements to regular oversight through the ARB process.

Senator COBURN. How about the acquisitions that were started before you started?

Ms. LUTE. Some of them——

Senator COBURN. What are you doing with those?

Ms. LUTE. Some of them have proven problematic, and all of them, we are incorporating into the new process.

Senator COBURN. Would you submit to the Committee the ones that you have terminated and the ones that are problems?

Ms. LUTE. Yes.

Senator COBURN. Thank you. My first training was as an accountant and as an auditor, and I can tell you, the experience when I talk to Marine captains and colonels today, they are so thankful that the Marine Corps is just about to pass an audit, because what it has actually done is made their job easier and their decision-making easier because they now have visibility on the key parameters which would judge the outcome of a decision or direct them to make a new decision.

Are your people ready to use accounting information to make management decisions and all the way through all 22 agencies?

Ms. LUTE. That is a great question, Dr. Coburn. The answer is, absolutely. And if I can just call out the men and women of the Coast Guard as the first——

Senator COBURN. Yes, I know.

Ms. LUTE [continuing]. As the first uniformed service——

Senator COBURN. You bet, the first one to do it.

Ms. LUTE [continuing]. The first to achieve auditable status. This is something that we have and the Commandant has and the leadership across the Coast Guard has pushed down, you are exactly

right, down to the lowest level possible. The American people have a right to expect that we can account for the resources that have been given to us, and when you can do it, it is very powerful from a leadership point of view.

Senator COBURN. OK. Let me ask you one other question. You have accomplished and actually performed on about 60 percent of the GAO recommendations. I do not expect you to say they are right in every indication. I understand that sometimes they miss it. But there are 40 percent of their recommendations that you really have not acted on. What is the plan? Are some of those recommendations that you actually disagree with, or are they just ones that are harder to implement, and is there a push from senior management at DHS to actually accomplish and meet those recommended accomplishments?

Ms. LUTE. There absolutely is a push, I think as Mr. Dodaro mentioned. This is not the first time he and I and Cathy are sitting together at a table. We have known each other for 4 years because we made a commitment early on to get this right.

There are a few things we do not agree with, but we have an overwhelming bandwidth of agreement between us, what needs to be done. And also—

Senator COBURN. Let me just interrupt. Will you send me and the Committee—what you do not agree with?

Ms. LUTE. Whatever material we have that we can share with—

Senator COBURN. Yes, where you say, here are their recommendations. Here is where we think they are wrong. Send that to us, because we actually read GAO reports in my office, and—

Ms. LUTE. Mine, too.

Senator COBURN [continuing]. And we would love to have the other side of the issue—

Ms. LUTE. OK.

Senator COBURN [continuing]. Of where you think they disagree, since the final arbiter is the U.S. Congress in terms of making the judgment on some of these things and whether some mandate is going to be put in an appropriation bill to make you do something that you actually disagree with and have a good reason for saying, “We think GAO got it wrong.” So if you would send those to us, I would appreciate it. And I am sorry for interrupting you.

Ms. LUTE. No, sir. And as I was just going to conclude, he also mentioned that he has seen from us detailed plans for working through the findings that they have given us. And it is the only way I know as an operator. What do we need to do to know that we are done, and we will do it.

Senator COBURN. Yes. OK. Thank you.

I am over my time. Are we having a second round?

Chairman CARPER. I hope so. It may be abbreviated, but we will have one.

What you just said about agreeing with most of the recommendations but not all, and Mike Enzi, a Member of this Committee, has shared with us any number of times something he calls the 80/20 rule, which describes how he and Ted Kennedy were able to get so much done when they were leading the Committee on Health, Education, Labor, and Pensions. The 80/20 rule means this. He says,

“Ted and I agreed on 80 percent of the stuff. We disagreed on 20 percent of the issues. We decided to focus on the 80 percent that we agreed on, set the other 20 percent aside to look at another day,” and that is how they were able to get a lot done. And I think that maybe kind of describes what you are doing here, and whatever you are doing is, I think, working, and let us just keep it up.

Senator Ayotte is next, and she stepped out for a moment. We are going to go to Senator Heitkamp, and if Senator Ayotte does not return immediately, then Senator Baldwin. Thank you. Senator Heitkamp, you are recognized.

OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you so much, Mr. Chairman, and thank you for appearing today.

I actually do know Janet pretty well and she is not perfect. Tell her I said that. [Laughter.]

We were Attorney Generals (AGs) together.

During my time in public life, I have been a tax auditor, tax commissioner. I have been an Attorney General. So this is an area that I think I have kind of two perspectives on, how difficult it is to do security, how difficult it is to wake up every day and realize primarily your mission is to protect this country and protect people. But the only way we can do it is when we are held accountable for how we do it.

And we are in a time of pretty tough budget questions, and when we have 10 years where we are not able to pass audits, it gets increasingly difficult to justify to the American public that we are doing the right thing here. Now, I am new to this and I can tell you—maybe if I sat through 10 hearings like this on a GAO audit—I would be a little tougher. But I want to give you an example of why the American public gets frustrated.

Recently in North Dakota, TSA removed three scanners, full-body scanners, to move to other locations to replace scanners that you had to replace because they did not pass privacy measures. Now, Minot, North Dakota, is a place of great economic growth. In fact, their airport is experiencing a 49 percent increase in passengers. We have more airlines flying in there. The airport is understaffed. But yet you removed their scanner, causing the people of Minot to think, OK, here we go again. They cannot seem to get it right in Washington. They cannot seem to get procurement right. We see it every day.

Obviously, we are extraordinarily grateful in North Dakota for all the help that we have received from FEMA. Minot is grateful for all the help, and, I think, all the true compassion and caring that the people experienced. But at the end of the day, yes, people can like the Federal employees who show up, and yes, you guys can sleep on ships and demonstrate your willingness to be accountable, but people want their dollars spent in an accountable and efficient manner, their tax dollars.

And when we see repeated problems and a lack of what we have been hearing today. Sixty percent, you can agree with. You are moving on 60 percent. But, yet, there have been a lot of years to make this happen. And I can tell you as an agency head, if I had come back year after year with an audit and not having responded

to concerns and questions, I probably would not have gotten an appropriation the next time and the legislature would have probably taken away my responsibility.

And so I just have a couple questions about my scanners, and I know that it is, in the grand scheme of things, this is not the big issue, but it illustrates concerns that we have about defending and representing the Federal Government when we go home.

And so I have been told by John Sanders that the agency is developing an acquisition program for the next generation of scanners that are going to replace the systems that were transferred out of our airports. This is a critical acquisition program which will impact the safety and the security of my constituents. What steps are DHS and TSA management taking to ensure that the acquisition problems identified by GAO, such as a lack of a plan to manage the risk and measure performance, are not repeated? And that we are not going to see—I have to tell you, I was pretty tough when I talked with John because I said, look, if the next thing is that you move those same scanners back into North Dakota, I will have 400 constituent letters about the waste of time. I said, you have to figure out how you can do this in a way that does not disrupt. And the notice was way too short, so there was not an ability to adapt.

And so I use this as an illustration of the frustration, and want to be supportive and want to learn more about what the challenges are of meeting these acquisition policies. But I also want you to know that I am concerned deeply about irregularities. I am concerned deeply about inefficiencies and about a 10-year audit where the response is, “We are working on it. We are hoping we will get there.”

Ms. LUTE. So, Senator, when I was in the Army, one of the Chief of Staffs of the Army, Gordon Sullivan—I am a great admirer of his—used to have a saying, “Hope is not a method.”

Senator HEITKAMP. Yes.

Ms. LUTE. We are not hoping to get to a clean audit opinion. We were not hoping to get to a qualified audit opinion. We were going to get there, and we are there. We are at a qualified audit opinion. We are auditable in less than 10 years of existence of a \$60 billion agency with half-a-million people.

So I share your determination that the accountability and the auditability and the answerability continues and has to improve. We will do that.

Senator HEITKAMP. But if I can just make a point, and it is not to be belligerent, but it illustrates, if a bank consistently told the bank regulator after 10 years, “We are working on it. We have a strategy, we think,” they would not have been given 10 years to hit the mark. They would not have been given 10 years.

Ms. LUTE. I worked in a bank when I was younger. I will not pretend to answer for it now. But what I can tell you is that we take a backseat to no one in our determination to achieve what we said we were going to do, which was a clean audit opinion, and sustain that, and I believe we will hit that mark. I know we will, because I know the effort that is going into this.

In terms of the acquisition, I would be happy to share with you our detailed Management Directive covering the acquisition process

to which now all programs must adhere, and it is a rigorous process that examines from requirements to ultimate disposition.

Senator HEITKAMP. And if I can just—not to belabor it—every organization has a policy. The question is whether they have the will to implement the policy, and so we will wait and we will see. But these numbers at this point are not numbers that I can defend in North Dakota.

Ms. LUTE. What I could say, we also have a proven track record over the past 4 years of actually holding the meetings, canceling programs, improving the accountability and the understanding and the oversight within the Department of our acquisition programs, and we would be happy to lay all of this out for you in as much detail as you would find useful.

Senator HEITKAMP. Thank you.

Chairman CARPER. Senator Heitkamp, if you have not taken advantage of this, or any other Members of our Committee, I know Senator Coburn has, but Deputy Secretary Lute was good enough to spend a couple of hours with me and members of my team and it was just enormously helpful in understanding where they were when she started and where the Secretary started and how far they have come and what more they need to do. Hearings are good. Roundtables are good. But that is even better, and I would just urge you to take advantage of that. If we can be helpful in maybe pulling together a small group of Senators to have that kind of conversation with their staffs, I think everybody would be better for it, all right.

OPENING STATEMENT OF SENATOR AYOTTE

Senator Ayotte, thanks for being with us yesterday. Thanks for being back again today. You are recognized.

Senator AYOTTE. Thank you, Mr. Chairman.

I want to thank the witnesses for being here today and wanted to followup on, I think, some questions that you were already asked by Senator Coburn and may have been touched on by Senator Heitkamp, as well, and that is the grant programs and acquisition programs.

The December 2012 GAO report found that, in fact, there were—unfortunately, the major acquisition programs are continuing to cost more, take longer, deliver less capacity, and GAO identified 42 particular programs with cost growth or schedule problems, 16 of which saw increased costs, from \$19.7 billion in 2008 to \$52 billion in 2011. And according to that December GAO report, this was due to the Department's lack of adherence to knowledge-based program management practices, and I know that Dr. Coburn touched on that, but where are we on this and how do we—basically, as Senator Coburn said, if we cannot measure effectiveness for these and we are continuing to see cost overgrowth in a challenging fiscal climate, how do we justify to our constituents that we should be spending money on these programs?

So can you explain, where we are on that, and also, I would love to get some comment from you, Ms. Berrick, on that issue.

Ms. LUTE. Thank you, Senator. We agree that we can do better, and as Dr. Coburn and I discussed, this is something we are very seized with.

One of the things that we did was put in place the National Preparedness Goals. What do communities need to do? How much of X, Y, or Z do they need to have? How do they know that from a set of judgments regarding what constitutes community preparedness that they are getting close to that? So articulating those preparedness goals was an important first step.

Evaluating the capacity that has been created over the past 10 years, with a sizable investment by the Federal Government in that capacity, is something that we are intending to do, as well.

And then measuring performance objectives. And we have begun the performance objective process with ourselves. In 2009, we had over 182 performance objectives, some of which, quite frankly, were impenetrable. They were really difficult to understand and they were not at all straightforward. We looked at every single one of them. We have broken them down. We have cut them by more than half. And we have put them in plain language so that we know if we do these things, these are recognizable steps in the direction of preparedness, safety, and security.

Senator AYOTTE. Can I share an experience I had when I was Attorney General? When the Homeland money first came in, to the State level, at least, the experience I had in our State, good intentioned people, but a lot of specific requirements on the Homeland money that maybe allowed a local agency to buy an All Terrain Vehicle (ATV) or a particular piece of equipment, but as I saw it, no connection to the overall plan to homeland security. Where are we on that with the State dollars that have flowed down and what I have seen sort of from a State perspective is a lot of piecemeal equipment here and there, but I could not connect it to the overall protection of either the State or the country.

Ms. LUTE. Again, that was part of the purpose of laying out these National Preparedness Goals, so that we could see not just what the States were doing, but that the States could, further on down, see what was going on at the local level.

Senator AYOTTE. And that it was all coordinated to some greater plan to protect the homeland?

Ms. LUTE. So that it would be better coordinated to address the risks in a prioritized way.

Senator AYOTTE. OK. Well, I appreciate that, and this is something that I—obviously, I am new to this Committee, but want to hear more about, and I would certainly like to hear your perspective, Ms. Berrick.

Ms. BERRICK. Sure. I think Senator Heitkamp really captured the State of DHS's acquisitions well, which is they have a good policy in place. The key is really execution moving forward.

In addition to some of the statistics you mentioned, our review that we issued late in 2012 identified that most of DHS's major acquisition programs lack key documentation. That is really fundamental to managing those acquisition programs. And, in fact, half of the programs did not have any of that documentation, and that includes new programs and also older programs, as well, that predated the new Acquisition Directive.

DHS has a number of really promising initiatives that they are pursuing right now that will strengthen their acquisition function.

The status is they are in the very early stages, and I can give you a couple of examples.

One is they have recently developed a requirements validation function which basically looks at the requirements for new systems and looks across the Department and coordinates that and makes sure that they are developing one DHS solution to meet all of their needs. We think that is very positive, but it is still in the very early stages. They are just starting to meet as they move forward. So we are going to be watching that moving forward.

Another promising development is they developed a dashboard to oversee cost, schedule, and performance for their acquisitions, again, very promising. But that also is in the early stages. And, in fact, due to data issues, managers cannot really rely upon that system right now to make decisions.

Regarding DHS's progress related to acquisitions, they are absolutely moving in the right direction. The key will be executing on their policy, which is a good policy, and then assessing the results as they move forward.

Senator AYOTTE. Thank you. I also wanted to ask about just looking at the 2013 high-risk list, where are the issues that fall under, really, primarily DHS that GAO issued? And, of course, I think the one that jumps out at me, as I am aware we have had a pretty lengthy hearing on the cyber challenges, but the establishing effective mechanisms for sharing and managing terrorism-related information to protect homeland security. I mean, this is the key issue post-9/11. Where are we? If it is still on the high-risk list, what have we done that is well that you can talk about here, and where are the major challenges that remain?

Ms. BERRICK. The first—

Senator AYOTTE. Obviously, if there are things you cannot share here, I understand that.

Ms. BERRICK. There has been significant progress in standing up the information sharing environment, which is really the government's structure to manage this issue because it goes beyond DHS. It affects a lot of Federal agencies that have key leadership roles in this area. So there have been good oversight structures. The White House has established a Policy Committee that oversees efforts in this area. They also established a strategy with pretty good metrics.

The key, really, right now is for the five major departments that have key responsibilities in this area, including DHS, to execute their information sharing initiatives and to coordinate with one another. DHS has made very good progress in this area. They have prioritized their information sharing initiatives. A key challenge that they are facing is—as other departments are, as well—is really resourcing those initiatives. We think they still have work to do in leveraging efforts of other departments and also identifying what their resource needs are for all of the various initiatives which are still underway.

Another big challenge in the information sharing area is really the IT issue of connecting systems to enable departments to share information. There have been some frameworks put in place, but the agencies are really in the early stages of that. So very good progress in standing up a governance structure. The key right now

will be for the departments that have key responsibilities to move forward and coordinate their initiatives, such as the IT initiatives, and work together to address these challenges.

Senator AYOTTE. Secretary.

Ms. LUTE. I would just add one thing to what Cathy has said, in addition to all of that. Maybe two things.

One is, sorting through the rules of information sharing is an important aspect of this, as well—U.S. persons, non-U.S. persons, law enforcement sensitive information, et cetera. We have been working through that with all of our counterpart agencies and we think we are making progress, but it is something that we have to and do pay attention to.

The other thing that we have begun to come to grips with, and I would say that this is a tremendous challenge, is the so-called big data challenge. We have an initiative—we have several initiatives sort of, again, that are across the Department of Homeland Security. I call them the DHS Commons—common vetting, common aviation, common redress and traveler assistance and customer service.

In the common vetting, what we know is we interact daily with the global movement of people and goods. TSA moves two million people a day. A million people cross our borders. We have a tremendous amount of data. How can we minimize the collection of that data so as to not pose an undue burden on the traveling public, for example, and how do we share it in an expedited way, subject to rules, with appropriate limits of use, protections for privacy, civil rights, and civil liberties that people have a right to expect? We are making progress on all of those fronts, in addition to what Cathy said.

Senator AYOTTE. Thank you all. I know my time is over-expired, so thank you for that latitude, Mr. Chairman.

Chairman CARPER. It was worth stretching it out. All right. Thank you very much. Thanks for being here again.

OPENING STATEMENT OF SENATOR BALDWIN

Senator Baldwin, welcome. Great to see you. Please proceed.

Senator BALDWIN. I want to also thank the Chairman and Ranking Member for holding this up and down review of the Department of Homeland Security. Clearly, what was accomplished back in 2003 was no easy task, and I certainly recognize the incredible progress made in the 10-years since the Department's creation. But since we are here today, I want to focus in on a couple of the areas in which the Department can improve or have been pointed out.

Fortunately for me, Senator Ayotte's last question was the first question I was going to ask about in terms of the recommendations in the GAO High-Risk Report on information sharing across agencies, so I feel like you have tackled that.

But I want to also look at another area. Mr. Dodaro, in your testimony, you discuss the inclusion of a new high-risk area in 2013, limiting the Federal Government's fiscal exposure by better managing climate change risks. And our country has certainly seen an increase in weather-related events that have contributed to significant loss of life and property, and it seems to me that each year, the weather-related events become more and more damaging and

the level of involvement of the Federal Government has only increased.

One of the recommendations in your testimony is for DHS to improve the criteria for assessing a jurisdiction's capability to respond to and recover from a disaster without Federal assistance and to better apply lessons from past experiences when developing disaster cost estimates.

A few weeks ago, I was meeting with a county executive from one of the larger counties in the State of Wisconsin and we briefly discussed the need for FEMA and other Federal agencies to be more involved in ensuring that our local communities are prepared for the worst. And so I am wondering if both of you could comment on what DHS action items have occurred and will occur in the near future to assist local communities in preparing for the worst.

Mr. DODARO. First, the criteria issue is a very important one. The criteria was established, and it is qualitative criteria, but they use some quantitative measures. One is the per capita cost, per person in each State, and it started out as a dollar in the 1980s per person per State as sort of a threshold of whether or not the total costs of responding to the disaster would go over that. Then the Federal Government would get involved. That was not indexed for inflation for a 13-year period of time, from 1986 to 1999. Our calculations show that if it had been indexed for inflation, the Federal Government would not have been involved in about 25 percent of the disasters that occurred during the time period we reviewed.

And FEMA did agree with our recommendation to reassess the criteria and said that they were going to do that. It is a complicated task to be able to do it, but it is very important because of the incentives that it provides at the State and local level to make their own plans for preparedness and to identify where accountability lies. Particularly with State and local governments having zoning responsibilities, they have a lot to say in terms of where there infrastructure is located.

Now, the other responsibility that FEMA has is to come up, ultimately, with criteria to determine readiness at the State and local level, and this goes to the grants question, as well, that was raised earlier. With all the grants that have been provided, at what point, even with what Jane mentioned regarding their goals that will be established, at what point are States capable of responding to these situations? FEMA is still working on that issue and has not really resolved that issue, as well.

So there are two issues. One is the criteria for whether the Federal Government intervenes or not, and I think it needs to be reassessed. FEMA has agreed. But it will be a while before they come up with the criteria. But Congress should ask. And second is when FEMA comes up with a criteria for determining readiness of the capabilities at the State and local level. Both are needed to have good benchmarks in that area.

Senator COBURN. Would the Senator yield for just a moment? Let me make a comment about Oklahoma. I think Oklahoma received 11 disaster declarations based on the per capita damage ratio, and it is supposed to be a combination of overwhelming local resources and the per capita damage ratio. If you just looked at when we were overwhelmed, it was one of those.

Now, we are happy to take the money. I know our Governor is and our State Legislature. But I will put us back into perspective. We are going to spend a trillion dollars more this year than we have and there comes a point in time where local responsibility has to take over and be responsible for their legitimate functions for a couple of reasons.

One is, we can never solve all, have them totally prepared, even if we were the great benevolent figure that we are.

And No. 2 is, financially, we cannot afford to do what we have said we are going to do now. And so we have to change this indicator, at least change it for inflation, because it is a tremendous advantage to a small State. We have less than four million people. It is not hard to get \$4 million worth of damage from a tornado in Oklahoma. How much responsibility should Oklahomans bear for that? I would say the vast majority of it, not the Federal Government.

So I think your point is well made, and I am sorry I interrupted you and we will add more time to you. But we have to start putting this into perspective.

Mr. DODARO. I agree with you, Senator. I think a good interim measure would be to index it for inflation for the entire period of time, because FEMA has indicated it is going to take time to come up with new criteria and go through a vetting process. But there could be some interim changes that they could consider.

Chairman CARPER. Senator Baldwin, would you just hold your thought for just a moment. None of this counts against your time. In fact, we will give you more time.

My understanding, just correct me if I am wrong, is about the last dozen or so years, I think this number has been indexed to the rate of inflation, I think. But for the first 12 or so years that it was in existence, it was not. And so I think that is the issue here, and the question is, what kind of catch-up do we do for those first dozen or so years.

OK. Senator Baldwin, you are on. Thank you for bearing with us.

Senator BALDWIN. No problem.

Deputy Secretary Lute, I do not know if you have any comments on this question also.

Ms. LUTE. So, I would only say two things. It is not 60/40. Gene and I agreed it is probably 95/5. We agree on most things that need to be done and improved, and it is really on that basis of common perspective that we proceed.

And I guess the only thing I would add reflects a little bit on the point Dr. Coburn was making, which is in the tragic tornado that went through Joplin, Missouri, not long ago, it was an extraordinary demonstration of local capacity and mutual aid from the local community. No Federal search and rescue resources were deployed to that area. It is a small, teeny example, but exactly the kind of point, I think, that you are raising and making, and that is where we are headed.

Senator BALDWIN. The other question I had, my home State of Wisconsin has a number of ports of entry throughout the State that Customs and Border Protection oversees. And I am curious as to whether there are any major recommendations that directly involve Customs and Border Protection and whether such recommenda-

tions focus on security at ports of entry, if you could both comment on that and provide context to whether there are current issues with security at our ports of entry.

Mr. DODARO. Yes, Senator. I will ask Cathy to elaborate on it, but regarding maritime ports, the one I know of is the Transportation Worker Identification Card (TWIC) issue, which we have written about in a couple of reports, and the status of that card. Part of the problem was not having the card readers available yet. So that has been one problem. But I will ask Cathy to elaborate on others.

Ms. BERRICK. In addition, I would mention, as was already discussed, the US-VISIT exit system, which is a mandate that DHS has to develop a biometric exit capability to track foreign nationals leaving the United States. They have a biometric entry system. But that is a key area outstanding that they are working on.

Also, another area is determining the appropriate mix of technology and infrastructure to secure different sectors along the Southwest border. As was mentioned, SBInet was canceled and DHS's new approach is to determine the appropriate mix across the sectors rather than have a one-size-fits-all solution, and that work is still in progress and GAO has ongoing work looking at it.

We have also made recommendations related to training for CBP agents and the need to have recurring training and refresher training after agents have been hired.

Those are some key ones, and we have a number of others that we would be happy to discuss with you.

Ms. LUTE. I think what I would just say in response, all of these are known to us and things that we are working on. As Cathy said, there is no one-size-fits-all for the ports of entry at the border and there is no single-point solution, just technology, or just more personnel, or just better process. You need to integrate all of these things in a sensible approach at the border, as we have been demonstrating.

With respect to training, I could not agree more, and I am fond of saying sometimes that in the Federal Government, people talk about investment. Really, the only place you invest is in people. That is where you get the return. We spend a lot of money. We place some bets. Is this going to work or not? But the real investment is when you invest in people and that is in training.

And we have taken steps, particularly on leadership training. We have created—it did not exist before—a comprehensive leadership training program for the Department of Homeland Security so young, entry-level professionals coming in as a Homeland Security person can see themselves all the way through and understand that as they progress in their career, there is a progression in expectations of the responsibilities they will assume. Certainly, this applies here, as well.

Senator BALDWIN. Thank you.

Chairman CARPER. One of the recurring themes of our hearing yesterday—on the oversight of the Hurricane Sandy response—one of the recurring themes was shared responsibility. We are not in this by ourselves. It is not just the Federal Government. It is not just State or local government. It is just government. We are all in this together, so that is good.

Mr. Dodaro, if you could, a question for you. I am going to try to keep this under 4 minutes. If you could help me with that, that would be good. But if you had to provide us with maybe the top two or three areas that you think would yield the greatest results in further improving the management of the Department of Homeland Security, what might those two or three areas be?

Mr. DODARO. I think the first area, the one area that I would focus on, is the acquisition management area, because—

Chairman CARPER. Is your microphone on? Just start over.

Mr. DODARO. I am sorry.

Chairman CARPER. We want to hear every word.

Mr. DODARO. OK. I will ask Cathy to provide input too. I will give the first one, and that is acquisition management. I think the acquisition management area is so critical to procuring the types of systems, whether it is scanners, IT solutions, or other solutions, that are critical to implement the Department's missions. And I think that is very important, whether you are talking about immigration, Customs and Border Patrol, or other areas. That is where I would focus. That is an area where we have seen well-established departments, long-established departments—Defense, National Aeronautics and Space Administration (NASA), Department of Energy—with acquisition management still on the high-risk list. So that is a tough issue to resolve and it is all about implementation and having the proper discipline in place.

Chairman CARPER. Thank you.

Ms. BERRICK. And just to provide some context, GAO has issued over 1,300 products looking at different aspects of DHS's programs and operations and made over 1,800 recommendations. A key theme we identified, looking across all those products that has impacted the Department's efforts trace back to the management of the Department, just to put this in context. So we have identified this as a cross-cutting issue.

And while all the management areas are important, I agree that acquisition along with IT are the two areas that have the most direct effect on the Department's ability to implement their missions—secure the border, secure air travel. IT is very similar to acquisition.

DHS's focus really needs to be on moving forward on the initiatives that they are pursuing, and ensure that they are following their existing policy, not just in acquisition and IT but across all the management functions. DHS has good policies in place. The key is really execution, moving forward on these initiatives that they are starting, and monitoring their progress moving forward.

Chairman CARPER. OK. Thanks.

My last question. On our second panel today, Elaine Duke, who is here today already, served as the Under Secretary of Management at the Department, and former Inspector General Richard Skinner, are both going to caution us on this Committee that it is important not to be short-sighted with the budget for management. The Fiscal Year 2013 Continuing Resolution passed by the Senate yesterday would cut \$17 billion from management at the Department of Homeland Security. What area or areas of progress in addressing management are the most at risk if there are funding reductions, and what will be the impact in the next 5 to 10 years?

Mr. DODARO. We have already received a request from the Congress to look at the impact of sequesters on Federal departments and agencies, so we will be looking at that issue, including in terms of how they have prepared for this issue, because a lot depends on what kind of decisions that they have made in terms of what impact it is going to have, and once we complete that work, we would be happy to provide it to this Committee.

Chairman CARPER. OK. Fair enough. Dr. Coburn.

Senator COBURN. You said \$17 billion?

Senator CARPER. I said \$17 billion. I think I misspoke. It is \$17 million.

Senator COBURN. General Dodaro, the DHS employee morale survey this year went down. Why do you think it did?

Mr. DODARO. Well, I think there are two reasons. If you look at all the Federal departments and agencies, it went down, I mean, overall, with few exceptions.

Senator COBURN. OK.

Mr. DODARO. So I think it is part of the environment and the uncertainty associated with the environment.

Beyond that, I am really not sure, and one of the things that we have recommended to the Department is that they do a root cause analysis to try to figure out what is driving the decrease in scores.

Senator COBURN. It is a pretty depressing place up here, is it not? [Laughter.]

Mr. DODARO. Well, this is a tough issue. I know from running the GAO, we have employee feedback surveys, too. Fortunately, we are one of the top-ranked ones, but we did not get there by accident. We worked on this over the years. It is very difficult to figure out what motivates people and what you really need to do to address their concerns. But you have to keep trying really hard to find out what some of the root causes are to be able to do that. We have made that recommendation to DHS. They have agreed to do that. And I think that will provide some insights as to the reasoning. You really have to study this.

Senator COBURN. Yes.

Mr. DODARO. If you leap to conclusions about things, you can actually make things worse.

Senator COBURN. Yes, right.

Secretary Lute, do you think it is any worse in DHS than it is anywhere else in the government?

Ms. LUTE. I will not speak for anywhere else in the government, Dr. Coburn, but it is unacceptably low to me, certainly to the Secretary. I have been around a lot of workforces for a long time, and as Gene said, across the Federal Government, it is down. Across the country, the public mood ebbs and flows. There have been pay freezes. There have been other things going on.

Senator COBURN. Tough times.

Ms. LUTE. But there also have—I think—and this Committee has been very helpful in this regard and helping the American public understand that their red, white, and blue-collar workforce shows up to work for them every single day. And you do not run an organization with denigration and derogation and dismissiveness. You run it with purposefulness and pride. And you run it most effec-

tively when you put that purpose and that pride in the hands of your workforce and you lift them up. Our job is to lift them up.

So one of the things that I also know is that your front-line supervisor matters a lot to you. Do our front-line supervisors have the tools they need to do their job? We are trying to give them that with this emphasis on a leadership training program, and other things, as well.

People want to show up. They want to connect to the meaning that brought them to public service. They want the tools they need to do their job. They want to add value and they want to feel valued. That is what we are going to do.

Senator COBURN. Secretary Lute, let me ask you one last question. We will submit a lot of questions for the record, which we routinely do, and I appreciate you all being timely on the response.

Homeland Security Permanent Subcommittee on Investigations (PSI) and my office did a study on urban area security initiatives this last year and published it, and we got a lot of blow-back, but it is \$8 billion out of the \$35 billion that you spent in the last few years on grants. And Senator Ayotte was here. New Hampshire spent hundreds of thousands of dollars on a BearCat for a pumpkin festival. What Senator Heitkamp said, it is pretty hard to explain to people why we are releasing people from detention who are undocumented aliens when we are spending two or three-hundred-thousand on a piece of equipment that is going to rarely, if ever, be used for its original intended purpose.

What level of specificity are you putting into the grant requirements? We are spending American taxpayers' money to help them get prepared, and then they see all these areas where we are spending, whether it is snow cone machines or underwater robots for a city that does not have a lake or whatever it is? How are we changing that?

Ms. LUTE. And I agree with you, Dr. Coburn. That has to change. In part, we are changing that through the identification from FEMA of the National Preparedness Goals. What do you need to be able to do? What capabilities are required for that, and how do you measure your performance going forward?

Senator COBURN. And how much of it is the State and local responsibility?

Ms. LUTE. It is. As you know, a great deal of it is. But also, this serves as guidelines for them as it further cascades down.

In addition to that, we have written this financial assistance policy which now is comprehensive. It looks at requirements. It looks at grant writing. It looks at accountability. It looks at grant oversight over the course of time, disposition and ultimate reporting. We know we can do better on this and we are committed to doing it. And, again, the proof is in, not just writing the policy, but following through.

Senator COBURN. All right. Thank you very much. Thank you all for being here. I appreciate your dedicated service.

Chairman CARPER. As do I.

Before we release you, I just want to mention a couple of things. One—I think Tom has heard me say this before—people say to me from time to time in Delaware and across the country, I do not mind paying taxes. Some people say, I do not even mind paying

more taxes. I just do not want you to waste my money. I just do not want you to waste our money.

This Committee is dedicated, committed to—not just the two of us, but I think everybody on this Committee is determined to be a good partner, provide oversight, but be a good partner with you, both of you, the three of you, to making sure that we waste a whole lot less. Our goal is to be perfect, but the road to improvement is always under construction. I am encouraged that this road to improvement is under construction, for sure. We are making some progress.

The other thing, on morale, it troubles me. I want people who work here with us on this Committee and our staffs, our colleagues, I want morale to be good. And one of the most interesting things I have heard lately about morale, what people like about their work, it is people like different things about their jobs. They like getting paid. They like having vacations. They like having benefits, pensions, so forth, health care. But what people most like about their work is that they feel that it is important and they feel like they are making progress. That is the most important thing. They feel the work, that their work is important, and they feel like they are making progress.

Clearly, the work that you and the team that you and Secretary Napolitano do, the work you do is hugely important for our country. And not everybody knows this, but pretty soon it will be a secret no more. You are making progress. GAO, who we look to for enormous help on this, has verified that. Can more progress be made? Sure, it can. And I think with the attitude that you bring to it and the oversight we will provide and the help that hopefully we can provide, we will provide even more.

We did not get into the issue in terms of management success and morale, as to whether or not it makes sense to try to put more resources behind consolidating your operations in one location. We did not talk at all about St. Elizabeths. We are going to have some follow-up questions. But I think that is an important issue and we are not doing a very good job. At this time of scarce resources, it is hard to come up with the money, but what we do come up with, it is important that you use it in a cost-effective way and help us in working with the appropriators to make sure that the dollars that are available for this are being put in the right place to help to better manage the Department, better do your work, and, really, in a sense, enhance morale.

All right. Anything else, Tom?

Senator COBURN. I do not think so. Thank you.

Chairman CARPER. OK. Thank you all very much.

And I want to say, I do not know, Ms. Berrick, if you could stay with us and sit through—just remain at the table and we will add another nameplate if you could remain with us, just to be—I do not know that we will call on you, but we may, and it would just be helpful if you could be here.

Ms. BERRICK. Sure.

Chairman CARPER. Secretary Lute—

Ms. LUTE. Yes, sir.

Chairman CARPER. Good job.

Mr. Dodaro, as always, thank you.

Mr. DODARO. Thank you. [Pause.]

Chairman CARPER. All right. Welcome. It is great to see all of you and have you join us at this witness table. You are not strangers to us and we are mindful of your years of service to our country, and your continued service. I am going to provide brief introductions and then we will turn you loose to testify and then respond to our questions.

Our first witness on this panel is Elaine Duke. Ms. Duke had a 28-year career with the Federal Government culminating in 2008 with her nomination by President Bush and Senate confirmation to be the Department of Homeland Security's Under Secretary for Management. She is the principal of Elaine Duke and Associates and provides acquisition and business consulting services. Welcome. In addition, I understand that you are an Adjunct Professor of Acquisition for American University and a Distinguished Visiting Fellow at Homeland Security Studies and Analysis Institute. Again, we are grateful for all your service and very grateful that you can be here today.

Our second witness is Richard Skinner. After 42 years of Federal service, having started at the age of 12, Mr. Skinner retired in early 2011. He was the first Senate-confirmed Inspector General of the Department of Homeland Security. Prior to his July 28, 2005, confirmation, he held the position of Deputy Inspector General starting on March 1, 2003, the date the Department was created. Prior to his arrival at DHS, Mr. Skinner was with the Federal Emergency Management Agency, where he served as the Acting Inspector General and Deputy Inspector General. In 1998, he received the President's Meritorious Executive Rank Award for sustained superior accomplishment in the management of programs of the U.S. Government and for noteworthy achievement of quality and efficiency in the public service. That is a high honor.

Our third witness is Shawn Reese, Analyst of Homeland Security Policy at the Congressional Research Service. Mr. Reese has written numerous reports to Congress on Federal, State, and local homeland security policy issues. He has testified numerous times on homeland security and counterterrorism issues before House Committees. Mr. Reese is a 2011 graduate of the Department of Defense's National War College and a former U.S. Army officer. We are happy to welcome you. Thanks for joining us.

And, Cathleen, thank you for sticking around.

Ms. Duke, you are recognized. Your full statement will be made part of the record. You are welcome to summarize it. I will ask you to try to stick close to 5 minutes, if you could. If you go a little bit over, that is OK. If you go way over, I will have to rein you in. All right. Thanks. Please proceed.

TESTIMONY OF HON. ELAINE C. DUKE,¹ FORMER UNDER SECRETARY FOR MANAGEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. DUKE. Thank you, Chairman Carper, Ranking Member Coburn, and Members of the Committee. I am very pleased to be here today. Management integration at DHS and the GAO high-risk list was important to me when I was at the Department and it continues to be of importance to me even after I have retired from Federal service.

I would like to talk about three phases of DHS management integration briefly, the past, present, and future.

In the past, first, we went through what I will call a building block stage. Some have the misperception that DHS was actually kind of formed as a blank slate, but really, it came together as 22 different agencies with many disparate and different systems, cultures, missions, all united by legislation. And each of the agencies brought with it both the good and the challenges of the legacy agencies. And so in bringing them together and achieving management integration, we had to start first by undoing to bring together in a more effective manner.

For example, when DHS was formed, about 90 percent of the major programs, and those are over a billion dollars in acquisition costs, were not run by a program manager with the skills and experience to run it. Now—and one of the building blocks we put in place was to develop a certification program for program managers and other acquisition professionals to appropriately run this program. And as a result of that initial building block, now, over 75 percent of the major programs are currently run by a program manager.

Now, I will briefly address some of the present initiatives to further enhance management integration, and these focus a lot on integrating some of the building blocks that were put together in the first 3 to 5 years of the Department. It has expanded and it is preparing to expand the Acquisition Certification Program to the other career fields that are critical for success, most notably cost estimating, logistics, test and evaluation.

It has put in place Component Acquisition Executives (CAE). It is a position, but it is key to continued accountability and authority of driving good acquisition throughout the operating components. And it has also raised the level of acquisition oversight to direct report to the Under Secretary for Management, Mr. Rafael Borrás, in the Program Accountability and Risk Management Office (PARM).

DHS has made significant accomplishments toward management integration. It has strengthened the authorities of the six business chiefs, which was critical in driving integration through DHS. And it has strengthened the functional integration between those chiefs and the operating components. It has chartered two federally funded research and development centers to assist in driving these objectives through DHS, the Homeland Security Studies and Analysis Institute and MITRE.

¹ The prepared statement of Ms. Duke appears in the Appendix on page 113.

As a result of the continued efforts of DHS leadership and management personnel, we are beginning in the Department to show sustained and demonstrated improvements. It first started at the U.S. Coast Guard (USCG) as the Blueprint for Acquisition Reform. DHS has applied the best acquisition practices throughout the Department. It has taken back systems integration responsibilities in key programs such as Coast Guard Deepwater and CBP SBInet. It has used the acquisition review process to redirect programs that are breaching cost, schedule and performance measurements. It has made significant improvements on its financial audits, as was discussed in the first panel. Another example is the consolidation of data centers, closing 18 already with six more slotted for closure this fiscal year.

Finally, I will give my recommendations for the future. DHS has developed an Integrated Investment Life Cycle Model (IILCM), and this model is critical and ideal for the next phase of management integration. It does two important things. First, it develops much needed management structure around policy and joint requirements. Second, it seeks to integrate and flow the decisionmaking of the various building blocks that were put in place in the first 10 years of the Department of Homeland Security. The integration of policy, joint capabilities and requirements, resources and acquisition under the Integrated Investment Life Cycle Model is critical for the continued maturation and integration of DHS management.

I believe there are several key things that DHS, GAO, supported by this Committee and other Committees of Congress, must do to support DHS in its continued seek for management integration: focusing on effectiveness and efficiency, continuing to form the capital and resources necessary for the integration, supporting the IILCM, and appropriately recognizing the employees that have continued to make the results that have been accomplished to date, as Deputy Secretary Lute talked about a little earlier. We must not underestimate the recognition of these outside parties.

I am looking forward to answering your questions this morning as we proceed with this panel. Thank you.

Chairman CARPER. Thank you, Ms. Duke.

Mr. Skinner, please proceed.

TESTIMONY OF HON. RICHARD L. SKINNER,¹ FORMER INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. SKINNER. Good morning. I believe it is still morning. [Laughter.]

Chairman Carper, Ranking Member Coburn, it is truly an honor to be here today and I appreciate this opportunity.

The Department's management support function was, when I was the IG, and you said earlier, one of the major problems when the Department first came together. It had to dig itself out of a hole. It inherited billions and billions of dollars' worth of programs, all with material weaknesses and inherent weaknesses. Yet, the management support staff that was transferred to the Department was not sufficient to support those programs. They have been digging themselves out of a hole for years.

¹ The prepared statement of Mr. Skinner appears in the Appendix on page 119.

Management support, and it has been repeated all morning, is in fact, the platform on which all of the DHS programs and operations are built, and they are critical to the success of the Homeland Security mission. And if the Homeland Security programs are in fact weak, so in turn, will be the programs which they are supporting.

Elaine and others have already hit on this, but I think it is really important to understand that when the Department was stood up, that this was one of the largest reorganizations in the past 50, 60 years, since DOD. That, in and of itself, created problems. And the fact that the environment in which we were living in those days, right after 9/11, also I think, contributed to this oversight. Everyone was mission focused, not management support focused. And as a result, I think that has delayed the building of the management support operations that we are still grappling with today.

The Department, and this goes back to all three Secretaries, Ridge, Chertoff, and now Napolitano, all recognized this as important. But I think the real progress that we are starting to see has occurred in the past 5 to 6 years, and it is moving at a snail's pace, but it is moving. The barometer is going up, and I think that is a very healthy indication of where the Department is headed.

Financial management, everyone has talked about that and everyone is very proud of the fact that DHS has received a qualified opinion on the balance sheet for fiscal year 2011 and reduced its material weaknesses. I would like to emphasize that obtaining an auditable financial statement is not the end goal. That is just one of the benefits that you receive from having a good, sound financial management system.

The Department right now is operating—their systems are being operated with band-aids. In order to get that clean opinion, it takes a Herculean effort by staff burning midnight oil, and it is going to do that year-in and year-out until it modernizes its financial management systems. Yes, it can tell you where it is at a point in time, September 30, but can it tell you where it is at on a daily basis? That is what a good financial management system should be doing. We still need to invest in modernizing DHS' financial management system.

The other area is information technology. That continues to be one of the Department's biggest challenges, in my opinion. We have to keep in mind, DHS inherited over 2,000 IT systems back in 2003. I think they have reduced that down to well below 700. It took almost 2 years just to inventory the IT systems. When we did that, when the Department accomplished that, finished their inventory, we found that the systems were archaic, stovepiped, unreliable, and many simply had no real value. Things are starting to change now. Things are starting to meld. But DHS is still in a very delicate stage, early stage of creating a good integrated IT system.

Acquisition management, this is the one area, and it is the one area everyone has been harping on for a long time and everyone has been highly critical of it, but during my tenure there and my observations over the last 2 years, it is the one area, in my opinion, that has improved the most, thanks in large part to my co-panelist right here, Elaine Duke, and the leadership that they have given to acquisition management. If you could understand how bad things were in 2003, I think we would appreciate how good things

are today. As bad as they are, it is improving. We must stay on that task.

And finally, grants management. That is something else that concerns me and continues to concern me as a citizen because of the waste that we are experiencing. I looked at the IG's semi-annual report, or the past two semi-annual reports. The OIG conducted about 50 audits and identified well over \$300 million in questioned costs. That is just unacceptable. There is something inherently wrong. We need to correct that.

The other thing that bothers me, always, when I was the IG and when I was with FEMA, is our inability to measure the impact those grant funds are having on our Nation's security. It is something, I think, that needs to be addressed. We need to do a better job of monitoring. We need to do a better job of measuring our performance.

In conclusion, I would just like to say that 10 years after its creation, the Department has in place the strongest management team imaginable. The Under Secretary for Management, the Chief Information Officer (CIO), the CFO, the Chief Procurement Officer (CPO), all have proven they possess the knowledge and skills to get the job done. Moreover, they have the support of the Secretary and Deputy Secretary. However, if DHS is going to progress, it is very important, I believe, that the Congress continue to support these initiatives. They are fragile—not only because they are in the early developmental stages, but because in today's budget environment. I understand that the first place you want to cut is the management support, not your operational or your mission objectives. We will be penny wise and pound foolish if we do not continue to invest in DHS' management support functions. We will be talking about this 5 years from now, 10 years from now, if we turn our back on the progress that has already been made.

I realize my time is up. I am sorry. I will be happy to answer any questions, Mr. Chairman, that you or Senator Coburn may have.

Chairman CARPER. He will be right back.

A lot of wisdom in what both of our first two witnesses have said, especially what you said there at the end. We have passed in the Senate and we expect the House to adopt today a budget resolution that carries through the end of September, for the next 6 months. It reduces for the balance of this year, I think, the management function at DHS by about \$16 million. And that is not good. We know that. We know that is not good. As you said earlier, there are some choices that need to be made.

We have the opportunity to take up today, tomorrow, maybe over the weekend, a budget resolution for the next 10 years and we will have an opportunity to revisit this particular issue, the kind of resources that we are putting toward the management function of DHS. My hope is that we will do a better job and maybe have some more resources and maybe be able to make some smarter decisions than we did in this instance.

But having said that, let me just yield to our third witness, Shawn Reese. Mr. Reese, we welcome you. Thank you.

**TESTIMONY OF SHAWN REESE,¹ ANALYST IN EMERGENCY
MANAGEMENT AND HOMELAND SECURITY POLICY, CON-
GRESSIONAL RESEARCH SERVICE, LIBRARY OF CONGRESS**

Mr. REESE. Chairman Carper, Ranking Member Coburn, Members of the Committee, on behalf of the Congressional Research Service, I would like to thank you for the opportunity to appear before you today.

When I wrote my report, the first edition, a year ago, I had no idea that it would be getting as much attention as it has in the past year, so I am glad to see that my work for Congress is paying off.

I will discuss the absence of a national comprehensive homeland security concept and the lack of homeland security mission priorities, not just within the Department, but nationally as a whole, and how these issues may affect DHS's integration and management of its missions.

Arguably, a comprehensive homeland security concept that prioritizes national homeland security missions is needed. This is more than an issue of what words describe homeland security. It is instead an issue of how policymakers understand or comprehend what homeland security is and how it is accomplished.

My written statement addresses this in detail and discusses the absence of both a standard homeland security concept and a single national homeland security strategy. I will now briefly discuss these issues.

In the past 10 years, Congress has appropriated approximately \$710 billion for the Nation's homeland security. That includes entities, not just the Department of Homeland Security, and that is based on OMB's estimate. However, homeland security missions are not funded across the board using clearly defined national risk-based priorities. Funding allocations are most effective when priorities are set, clearly defined, and well understood.

In August 2007, Congress required the DHS Secretary to conduct a Quadrennial Review of Homeland Security with the enactment of implementing the 9/11 Commission's Recommendations Act. This review was to be a comprehensive examination of the Nation's homeland security strategy, including recommendations regarding long-term strategy and the Nation's priorities and guidance on the programs, assets, capabilities, budgets, policies, and authorities of the Department. The 2010 Quadrennial Homeland Security Review (QHRSR) was criticized for not meeting these requirements. Given that DHS is in the midst of developing their 2014 Quadrennial Review, now might be an ideal time to review the concept of homeland security, its definition, and how that concept and definition affect DHS appropriations and the identification of priorities.

Obviously, the concept of homeland security is evolving and national DHS-specific homeland security missions are being funded. However, the manner in which future Homeland Security appropriations will be allocated is still a point of potential contention if there continues to be no comprehensive concept or list of national homeland security priorities.

¹ The prepared statement of Mr. Reese appears in the Appendix on page 127.

Policy makers continue to debate and consider the evolving concept of homeland security. Today, DHS has issued several mission-specific strategies, such as the National Response Framework. There has not been a distinct National Homeland Security Strategy since 2007. It may even be argued that the concept of homeland security as a separate policy area from national security is waning. Evidence for this may be found in the current Administration's combining of the national and Homeland Security staffs and the inclusion of Homeland Security guidance in the 2010 National Security Strategy.

Finally, OMB has questioned the value of requiring Federal departments and agencies to identify homeland security funding with their 2014 budget requests.

To specifically address the issues of funding national and DHS homeland security missions in DHS management, Congress may wish to consider three options. First, Congress could require either DHS or the combined national and Homeland Security staff to develop and issue a distinct homeland security strategy. That would prioritize missions.

Second, Congress could require refinement of national security strategy that would include not only national guidance on homeland security policy, but also include a prioritization of national homeland security missions.

Finally, Congress may focus strictly on DHS's forthcoming Quadrennial Review and ensure that DHS prioritizes its homeland security responsibilities.

In closing, it is important to note that Congress does appropriate funding for DHS missions. However, there is no single, comprehensive concept of homeland security and no single national homeland security strategy at this time. This may hamper the effectiveness of congressional authorizations, appropriation, and oversight functions. It may also hamper or restrict DHS and other Federal entities' ability to successfully execute homeland security missions.

I will conclude my testimony here. Once again, thank you for the privilege to appear before you.

Chairman CARPER. Thank you. Thanks for the time and energy you have put into this and for being with us today.

I want us to start off by asking each of you here for the—I think each of you were here for the testimony of the first panel, is that correct?

Ms. DUKE. Yes.

Chairman CARPER. All right. And you heard what they had to say, and questions and answers and back and forth. Just reflect on what you heard. Maybe you think you should underline or emphasize something for us or you might want to question something, but just react to the first panel, what was said.

Mr. SKINNER. First, I think the first panel was on target and I agree, particularly with the Comptroller General Gene Dodaro, with regards to what is important. Acquisition management is very important. Over 40 percent of DHS's budget is being spent on contracts every year. I believe that will probably continue because it has to rely on the private sector and the technology that they can bring to the table in supporting DHS.

DHS is going to continue to be wasteful if it does not have a strong acquisition management strategy in place that not only uses knowledge-based programs and theories, but also that holds people accountable, and that is, I think, the two things that were missing in the first panel, is accountability and transparency. We need to be able to show people on a real-time basis where our money is going. We cannot do that now with the financial management systems that we have in place. We can do it once a year, but we cannot do it on a continuing basis.

The other thing that I heard today, especially from Deputy Secretary Lute, was the commitment and dedication to improving the department's management support functions. And I truly believe there is a dedication and a commitment there to move forward, to move that meter forward. To stop pedaling right now, we are just going to fall over. They need support. They need oversight. And that can come from Congress. And I think it is very important that Congress stay on top of not just the mission-related functions, but also DHS' management support functions and to support them.

Now, I understand the budget situation, we all do, that we are facing today. It is going to take longer. We cannot do it all. Everyone expects it to be done tomorrow. It is not going to be done tomorrow. DHS needs to develop a strategic plan that clearly sets forth where it is going to be this time next year, where it is going to be 3 years from now.

One of the things that distressed me this morning was the focus on having an auditable financial statement 3 years from now. That is fine, but that does not mean it will have a good financial management system, and that is what concerns me. The focus on obtaining a clean opinion now is the end game. Victory will be declared if it can get auditable financial statements. DHS should not stop there. IT should be focusing on improving its financial management capabilities, and as a result, it will get auditable financial statements.

Chairman CARPER. Good. I think they understand that. I think Secretary Lute understands that. It is an excellent point. It is actually just some good advice for us as well as for the folks who are sitting at the table today. Thanks.

Ms. Duke, please.

Ms. DUKE. I would like to first of all, reiterate what Deputy Secretary Lute said at the end of her statement about the value of the employees. It seems to be a little in vogue right now to really criticize Federal employees—

Chairman CARPER. Not just right now. It has happened too often. Few things make me less happy than when I hear people describing Federal employees, or State employees, or local employees, as nameless, faceless bureaucrats. It demeans them. It demeans the importance of them as human beings and the work that they are doing. I find it very troubling.

Ms. DUKE. Thank you, Mr. Chairman. You made my point better than I would, so I will go on to No. 2.

Sometimes we talk about management and mission as if they are two separate things, and mission is nothing more than the foundation enabler of mission, and we cannot deal with the two of them separately. And so I think it is important as we move forward, es-

pecially as we are in this fiscally constrained environment, to not talk about them separately, because management delivers the people, the resources, the budget to deliver a mission and you cannot separate the two.

And the last thing I would like to point out is we really are driving toward a strategy. DHS is looking at management integration in a very strategic way. But it is important, I think, as we go along the way to not just measure the utopic State, the end State, but to measure tactical measures as we move along. What specifically are we doing to bring us toward that end goal? And I think that it is going to be important now to make sure we do take some of those tactical steps and not stop. And some of the innovations do require investments in capital investments to go forward, and I think we should be thinking collectively of how we can innovate to keep those going.

One of the ideas that we might want to consider is a share-in-savings type approach, which is where industry provides an infusion of capital and the Federal Government does not have to fund investment so that we can continue to move some of these management initiatives forward, like data center consolidation, like information sharing, like DHS headquarters.

Chairman CARPER. Thank you.

Mr. Reese, just very briefly respond, if you would. Any, just, quick reactions to what you heard from the first panel?

Mr. REESE. Sir, just I think that DHS has very much identified what its missions operationally are and it has identified the goals within each of those missions, and that is the word "operation" used so much this morning, I think that is—

Chairman CARPER. Excellent. Thank you for saying that.

A quick point, if I could, for Mr. Skinner. I believe you are the first Senate-confirmed Inspector General at the Department of Homeland Security, if I am not mistaken. That is right, is it not?

Mr. SKINNER. That is correct.

Chairman CARPER. OK. Senator Coburn and I have been joined by every Member of this Committee in sending a letter to the President last month saying, Mr. President, there are about six or so departments that do not have a permanent, confirmed Inspector General. We have an obligation, I think. The President has an obligation to nominate, to vet, ensure that they vet good people, whether it is for IGs or cabinet secretaries or under cabinet secretaries. The Senate has an obligation to, in a timely way, make sure that those folks are well qualified and move those nominations. We are not doing our job. In fact, we have not done our job well there for a number of years.

Talk to us just very briefly, and I will yield to Dr. Coburn, why is it important to have, in those half-dozen or so Federal agencies, why is it important to have Inspector Generals that are confirmed by the Senate? Nominated by the President, confirmed by the Senate? Why is it important?

Mr. SKINNER. I think it is extremely important, and I think we are seeing the results of not having the Senate-confirmed Inspector Generals in place right now across the board, not only at DHS but in other agencies.

One, I think it has an impact on staff morale.

Two, I think that serving in an acting capacity, you are not going to move the agency forward. I think oversight is extremely important, particularly in an organization such as DHS, but across the government, and it provides accountability. It helps provide transparency. It helps put funds to better use. And it helps identify where funds are being wasted or fraudulently spent.

By having acting people in place, what you are doing is running in place. You are not moving the organization forward, and you are not taking those steps necessary, as a confirmed IG would, to provide the independent oversight, I think, that is absolutely critical to the success of any organization.

Chairman CARPER. Good. Thank you for those comments. Dr. Coburn.

Senator COBURN. Sitting and thinking about our hearing today, the one word I had not heard, which should have been in everybody's testimony, is "risk-based." I mean, Homeland Security has to be about where the risks are. Now, we did not hear it from the GAO and we did not hear it from Secretary Lute. And what we have seen, and Tom will disagree with this to a certain extent, but most of the grant programs come out of here as a honey pot based on parochial preference rather than risk. Some of them, we divide. Fifty percent of it goes to risk-based. But everybody else gets their cut and share.

How important is it, that Homeland Security ought to be about risk? Everything ought to be about risk. Where are the risks? Where do we impact the risks? Where do we intercede in the risk? And how do we put resources where the greatest risk is? What are your thoughts about that?

Ms. DUKE. I agree with you, Dr. Coburn. I think DHS's recent move to move their Risk Office into the Office of Policy was critical, and I think that, in theory, that is to drive risk into the policy-making, and I think that is critical to going forward.

I also think that some of the moves on, for instance, securing the border and transportation security and doing a risk-based multi-layer threat look is critical in moving forward, from both a mission effectiveness and an efficiency standpoint. And I think the Department is starting to take looks at that and needs to move quite a bit forward. And, hopefully, the second QHSR is another opportunity, a point in time, where that can be emphasized even more.

Mr. SKINNER. Maybe the term "risk" was not used in explicit terms, but I think it was implied, particularly with Deputy Secretary Lute and the way they are approaching their strategic plans. Yes. It is risk-based. And you see this in all of their programs. In our grant programs, instead of just sending out money across the board, we should be establishing standards for the recipients and the applicants for these funds. Identify your risk, identify your vulnerabilities, and identify your capabilities to address those risks? We are unable to do that right now, and I think we could do a much better job in guiding billions of dollars that we will probably continue to spend to support State and local governments' preparedness capabilities. Where are our risks?

Mr. REESE. I would just take a quick look, and I would think also the gap exists between how the Federal Government as a whole looks at risk-based in homeland security and the nexus of where

that mix is with national security, because the Department understands its missions, but those are missions that have either been inherent because of the organization or how the Department has developed since then, and risk-based evaluation, I am sure, goes into that. But I think we still have an imbalance, or there is a missing component between how we look at national homeland security risk and how we address it and what the Department does.

Senator COBURN. Ms. Berrick.

Ms. BERRICK. If I could just add, Senator, risk-based decision-making and incorporating risk into planning, programming, and budgeting has been a key theme of GAO's work. In fact, the 1,300 reports I talked about that GAO has issued on DHS's programs and operations, the need for DHS to better incorporate risk into its decisionmaking, both at a strategic and a tactical level, really was a key theme throughout all of our work, right.

And at the tactical level, for example, talking about the QHSR, DHS did not apply risk in prioritizing what its QHSR priorities were. At a more tactical level, just to give you an example, for a program, the Chemical Facility Anti-Terrorism Standards (CFATS) program, which I know you are very interested in, we recently testified that in identifying which facilities should be in the higher-risk tier, DHS did not consider all elements of risk in making that decision. They were not considering all elements of threat, consequence, or vulnerability.

So it is extremely important, securing the border, aviation security, across DHS's range of missions, I think, overall, they have made the most progress in assessing risk. I think where they need to go is to build in—

Senator COBURN. The application of that assessment.

Ms. BERRICK [continuing]. The application of the risk.

Senator COBURN. Yes. Do not get me started on CFATS. So far, we have not accomplished much.

I am going to have questions for each of you. I would appreciate very much if you would be prompt in the response.

I would also note—my Chairman is not in here—that we have had key Homeland Security people and hearings in this Committee already at a level far faster than what we have seen in the past and we intend on continuing to do that. Learning from people who testify before us and critical management personnel in the government is what our job is. It is about oversight, asking the right questions, learning the right things, holding people accountable, just like we are talking about in DHS, having accountable results for a management plan.

So I am proud that Senator Carper has held this hearing and the others that we have held and the hundreds that we are going to hold over the next couple of years. I appreciate you being here, and you will get the Questions for the Record (QFRs) from us in due time. Thank you.

Chairman CARPER. As Dr. Coburn says, I just do not hold hearings. We hold them. We try to work together to put together ideas for hearings. This was really his idea, this kind of top-to-bottom review, and I think it is a good idea and this has been a very good hearing. We appreciate your being here.

Cathleen, you were good enough to stay overtime. Anything else you want to add? We will give you the last word, if you want it. Is there anything else you want to say?

Ms. BERRICK. Just that it is my pleasure being here and GAO looks forward to supporting the Committee on its future oversight efforts. Thank you.

Chairman CARPER. Dr. Coburn had asked Jane Lute to have somebody stay from her team and I think we have somebody right behind Mr. Skinner waving his hand, and we thank you for being here. Please convey to her the relevant things that you heard here.

The last thing I will say is this: on this management issue which we are really focused on today, somebody said, penny wise and pound foolish, and I really think that what we are doing with our short-term CR is that.

I would like to say, leadership is key for any organization I have ever been a part of. I do not care if it was the military. I do not care if it was educational. I do not care if it was government or business. Leadership is the key to everything. And we have good leadership in this Department. Now we need to make sure they have the tools to build on the good track record that has been laid over the last 10 years, especially the last 5 years.

You have helped us in your testimony today. You have helped us a whole lot in what you have done with your life before today. And I leave encouraged that—I am mixing metaphors here, but in terms of changing the course of the aircraft carrier, you can stay with it. You can turn an aircraft carrier. And I think we are turning this aircraft carrier in very good ways. We have a shared responsibility to make sure we continue to make progress. Dr. Coburn and I are determined that we are going to do what we can from our perches and my hope and expectation is everyone on this panel and the one that preceded it will do the same.

Thank you all. And with that, this hearing is adjourned. But before I do that, the hearing record will remain open for 15 days, until April 5, for the submission of statements and questions for the record. If you are asked questions, which you probably will be, if you would respond to those in a timely way, we would be most grateful.

Thank you so much. That is it.

[Whereupon, at 12:22 p.m., the Committee was adjourned.]

A P P E N D I X



Senator Tom Carper, *Chairman*

FOR RELEASE: March 21, 2013

www.hsgac.senate.gov

CONTACT:

Emily Spain (202) 224-2441 or emily_spain@carper.senate.gov

Jennie Westbrook (202) 224-2627 or jennie_westbrook@hsgac.senate.gov

HEARING: "The Department of Homeland Security at 10 years: A Progress Report on Management"

WASHINGTON – Today, Senate Homeland Security and Governmental Affairs Committee Chairman Tom Carper (D-Del.) convened the hearing, "The Department of Homeland Security at 10 years: A Progress Report on Management." Chairman Carper's opening statement, as prepared for delivery, follows:

"At the beginning of each Congress, the Government Accountability Office (GAO) issues its report on 'High Risk' government operations that leave the government exposed to waste, fraud and abuse, or which pose management challenges that threaten crucial government services. I have always considered this list as a 'to do' list for Congress, and GAO's updated High Risk list will heavily influence our Committee's governmental affairs agenda for this Congress.

"We also have just marked the 10th anniversary of the date on which the Department of Homeland Security officially opened its doors. We plan to mark this milestone throughout the year by holding a series of hearings intended to take stock of how far the Department has come in maturing, how well it is doing in executing its core missions, and how we can help them do even better.

"This hearing fits into both of the broad categories that make up this committee's jurisdiction. First, from a governmental affairs perspective, the Department of Homeland Security's management challenges appear again on GAO's High Risk list, although GAO readily acknowledges that progress is being made. Like other agencies across the federal government, the Department has grappled in recent years with a number of issues related to acquisition, to financial management, and to human capital, among others. Unlike some of those other agencies, though, DHS is moving the needle.

"As we all know, sound and effective management practices are, of course, critical to the Department's ability to carry out all of its homeland security responsibilities, whether we're talking about cybersecurity, border protection, disaster response, or any of its other missions. As we look back on the past decade I think it is important to remember the circumstances in which the Department was stood up. The Homeland Security Act passed by Congress to create the Department was signed into law on November 25, 2002. The Department opened its doors on March 1, 2003. So in just over 4 months, 22 different agencies from across the government with

different cultures and different management practices and philosophies were merged into the new Department.

“In those early days at the Department, the focus of both the Administration and Congress was on moving quickly to prevent another 9/11-type attack on the homeland. Management took a backseat to those efforts. Former Department of Homeland Security Inspector General Richard Skinner, who is here again today as a witness, confirmed this fact when he testified before our Committee last year that the management foundation of the Department really got shortchanged in those early days. It has taken years to dig out of the hole that the initial lack of a strong management foundation left.

“That said, I want to give credit where credit is due. GAO’s most recent report confirms that there has been considerable progress at the Department in integrating the components that were folded into it, and in strengthening the Department-level management that overlay the components. The latest High Risk report is good news, because GAO acknowledges this progress and has narrowed the areas that remain on the High Risk list.

“The Department also deserves credit for its detailed, aggressive plan to address all of GAO’s concerns in its High Risk report, which I believe is unique among all the agencies on the High Risk list. I want to briefly review some of the major improvements to management at the Department of Homeland Security. In doing so, I would agree with GAO that the committed leadership at DHS has been critical to driving progress in these areas.

“The Department is on the doorstep of having a clean financial audit for the first time. Last year, the Department was able to get its financial systems in good enough order to attempt a full financial audit. That was a major milestone. That leaves the important goal of now passing a financial audit. And I know that the Secretary, the Deputy Secretary and their team are prepared to make the final push to earn a completely clean audit. If they are successful, this will be a major achievement.

“When the Department was stood up 10 years ago, there was no framework for accountability. There was also no guidance on which responsibilities lay with headquarters, and which responsibilities lay with the various components that made up the Department. Whenever that kind of Wild West environment in government exists, there is sure to be a lot of wasteful spending and inefficiency. Now, the Department has made clear who is in charge of what. This new, more disciplined environment will better enable the Department to control costs at the various components and better ensure that all of them operate as a more cohesive, effective and accountable agency.

“The Department used to have an abysmal record when it came to awarding contracts without competition. But departmental leadership has been aggressive in turning that record around. Just last month, a report from the Office of Inspector General showed that spending on noncompetitive contracts in fiscal year 2012 fell by about 89 percent from fiscal year 2008 levels. That means about \$3 billion in contract dollars that were previously spent without competition are now being spent in a manner that gets better value for taxpayer dollars. And the

Department, as government-wide procurement data shows, actually has a better record on competing contracts now than most major agencies.

“The Department has also revamped its processes for identifying technological solutions at the border. The Department has moved away from the SBInet model, which was a mega-contract to a single company to build a ‘virtual fence’ across the Southern border. It was an effort that went forward without the necessary work to identify what the Border Patrol really needed. As a result, it quickly became cost prohibitive and did not deliver the capabilities promised. The Department has now implemented a more rigorous process to identify needs sector by sector along the border, and where possible is using commercially-available technology to drive down costs and enable our Border Patrol agents to become more effective.

“In the area of information technology, the Department is now at the forefront of the federal government’s efforts to consolidate data centers and move services to the cloud. These efforts save money and enable the Department’s employees to achieve better results.

“Finally, there is no doubt that the response to Hurricane Sandy shows how much FEMA has improved since Hurricane Katrina struck the Gulf region in 2005. Simply put, this improvement would not have been possible without better management. For example, when Katrina hit, FEMA did not have necessary contracts in place to get needed assistance to victims in a timely manner. When Sandy hit, seven years later, FEMA was prepared, and as a result there is a dramatic reduction in no-bid contracts compared to the Katrina response.

“These are all significant accomplishments, and our witnesses will discuss other examples today. But I don’t want to white-wash the serious, remaining challenges with DHS management that remain on the High Risk list. The Department still has work to do, as both Comptroller General Dodaro and Deputy Secretary Lute will discuss today. As I like to say, the road to improvement is always under construction. For example, the Department still does not have a comprehensive financial management system that gives the Secretary real-time visibility over the spending of the 22 Department components. The workforce morale at DHS remains the lowest of all major departments. Many major acquisitions have exceeded cost estimates or fall short of promised performance.

“This hearing also provides a timely opportunity to discuss the possible impact of the Fiscal Year 2013 full year Continuing Resolution on the Department. I am concerned about the \$20 million cut that DHS management and the Secretary’s office would take under the bill, and I want to hear from our witnesses today about the likely impact of those cuts. I am also concerned that the level of funding for consolidation of the department at St. Elizabeth’s is insufficient to support the next phases, which could bring leadership and operations centers to one location – and realize efficiencies and effectiveness.

“Both the Administration and Congress need to work together to resolve these remaining High Risk areas, and we will. I welcome our witnesses today and look forward to working with you and the dedicated people you lead so that in two years when GAO releases its High Risk list, management challenges facing the Department of Homeland Security are off the list making our nation more secure and putting our finances in better shape, as well.”

Opening Statement for Dr. Coburn

“DHS at 10 Years: A Progress Report on Management”

HSGAC Hearing—Thursday, March 21, 2013

This week’s 10th anniversary of DHS is an appropriate time for Congress to be reviewing DHS’s mission and management, and set a clear course for the next decade.

I look forward to hearing from Deputy Secretary Lute and the Comptroller General today. I am also eager to hear from our second panel of witnesses, including Mr. Reese from the Congressional Research Service. I was interested to read his recent report which stated that—“ten years after September 11, 2011 terrorist attacks, “the U.S. government does not have a single definition for ‘homeland security.’”¹

As members of this committee know, I strongly believe in the need for Congressional oversight. Under Chairman Carper’s leadership, we plan to conduct a top to bottom review of DHS over the next four years. And today’s look at DHS management and the GAO high-risk list is a good place to start.

Improving the management of DHS relies on a shared commitment between Congress and DHS to clearly define the homeland security mission as it exists today and to prioritize the use of taxpayer funds to achieve that mission as efficiently and effectively as possible.

With limited resources and a national debt of nearly \$17 trillion, we simply cannot afford not to establish clear priorities for the department. Fortunately, several of these priorities can be found right in the Constitution itself. In the Constitution, we see the fundamental reason we need a federal government is “providing for the common defense” and to “secure the blessings of liberty”. Consistent with these responsibilities, we need to focus DHS on the clear national security threats facing our nation—including counter-terrorism, border security, and maritime security. It also includes preparing for and preventing clear threats like nuclear and biological terrorism.

¹ Shawn Reese, “Defining Homeland Security: Analysis and Congressional Considerations,” Congressional Research Service R42462, January 8, 2013. sreese@crs.loc.gov

Once these priorities are in place, we must look at DHS's programs to determine which are focused on them, and which are not. We simply can't afford to fund forever programs that are not focused on clear national security threats.

The recent budget sequester is a valuable test of whether Congress and DHS can work together to focus DHS's mission and resources on these national security priorities. I strongly believe there are plenty of wasteful and low-priority areas to cut the agency's budget before we cut its core missions. By working together, conducting tough but fair oversight, we should have no problem agreeing on what these are.

What we should avoid is cutting essential security missions if low-priority areas have not been cut first. It was simply unacceptable to hear that ICE has released thousands of detained illegal immigrants due to the threat of a looming sequester that had not even kicked in yet.

This morning, I want to hear from Ms. Lute how DHS plans to move forward with the budget sequester in a manner that does not jeopardize our national security. I also look forward to hearing from other witnesses on concrete steps that the Congress and DHS need to take to implement needed management reforms.

Thank you. I look forward to both panels' testimony.

United States Government Accountability Office

GAO

Testimony
Before the Committee on Homeland
Security and Governmental Affairs,
U.S. Senate

For Release on Delivery
Expected at 10 a.m. EDT
Thursday, March 21, 2013

HIGH-RISK SERIES

Government-wide 2013 Update and Progress Made by the Department of Homeland Security

Statement of Gene L. Dodaro
Comptroller General of the United States

To access this report
electronically, scan this
QR Code.

Don't have a QR code
reader? Several are
available for free online.



G A O

Accountability • Integrity • Reliability

GAO-13-444T



Highlights of GAO-13-444T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate.

Why GAO Did This Study

The federal government is a large and complex entity, with about \$3.5 trillion in outlays in fiscal year 2012 funding a broad array of programs and operations. GAO maintains a program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges. Since 1990, more than one-third of the areas previously designated as high risk have been removed from the list because sufficient progress was made to address the problems identified.

The biennial high risk update describes the status of high-risk areas listed in 2011 and identifies any new high-risk area needing attention by Congress and the executive branch. Solutions to high-risk problems offer the potential to save billions of dollars, improve service to the public, and strengthen the performance and accountability of the U.S. government.

What GAO Recommends

The high risk report contains GAO's views on progress made and what remains to be done to bring about lasting solutions for each high-risk area. Perseverance by the executive branch in implementing GAO's recommended solutions and continued oversight and action by Congress are essential to achieving progress. GAO is dedicated to continue working with Congress and the executive branch to help ensure additional progress is made.

View GAO-13-444T. For more information, contact J. Christopher Mihm at (202) 512-6806 or mihm@gao.gov, and Cathleen A. Berrick, (202) 512-3404 or berrickc@gao.gov.

March 21, 2013

HIGH-RISK SERIES

Government-wide 2013 Update and Progress Made by the Department of Homeland Security

What GAO Found

In the past 2 years, notable progress has been made in the vast majority of areas that were on GAO's 2011 High Risk List. Congress passed several laws and took oversight actions to help address high-risk areas. Top administration officials at the Office of Management and Budget and the individual agencies have continued to show their commitment to ensuring that high-risk areas receive attention and action. Additional progress is both possible and needed in all the high-risk areas on GAO's 2013 list.

Sufficient progress has been made to remove the high-risk designation from two high-risk areas on the 2011 list, *Management of Interagency Contracting* and *Internal Revenue Service Business Systems Modernization*. While these two areas have been removed from the list, GAO will continue to monitor them.

This year, GAO also has added two areas, *Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks*, and *Mitigating Gaps in Weather Satellite Data*.

In 2003, GAO designated implementing and transforming the Department of Homeland Security (DHS) as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to address associated risks could have serious consequences. While challenges remain across its missions, DHS has made considerable progress in transforming its original component agencies into a single department. As a result, GAO narrowed the scope of the high-risk area and changed the name from *Implementing and Transforming the Department of Homeland Security* to *Strengthening the Department of Homeland Security Management Functions*.

To more fully address this high-risk area, DHS needs to further strengthen its acquisition, information technology, and financial and human capital management functions. Of the 31 actions and outcomes GAO identified as important to addressing this area, DHS has fully or mostly addressed 8, partially addressed 16, and initiated 7. Moving forward, DHS needs to, for example, do the following:

- *Acquisition management.* Validate required acquisition documents in a timely manner, and demonstrate measurable progress in meeting cost, schedule, and performance metrics for its major programs. GAO reported in September 2012, for example, that 42 major programs experienced cost growth, schedule slips, or both, and most programs lacked foundational documents needed to manage risk and measure performance.
- *Information technology management.* Demonstrate for at least two consecutive investment increments that actual cost and schedule performance is within established baselines, and that associated mission benefits have been achieved. DHS has begun to implement a governance structure to improve program management consistent with best practices, but the structure covers less than 20 percent of DHS's major information technology investments.
- *Financial management.* Achieve clean opinions for at least two consecutive years on departmentwide financial statements, and implement new or upgrade existing components' financial systems. DHS received a qualified opinion on its fiscal year 2012 financial statements, and is in the early planning stages of its financial systems modernization efforts.

United States Government Accountability Office

GAO's 2013 High Risk List

Strengthening the Foundation for Efficiency and Effectiveness

- Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks (new)
- Management of Federal Oil and Gas Resources
- Modernizing the U.S. Financial Regulatory System and Federal Role in Housing Finance
- Restructuring the U.S. Postal Service to Achieve Sustainable Financial Viability
- Funding the Nation's Surface Transportation System
- Strategic Human Capital Management
- Managing Federal Real Property

Transforming DOD Program Management

- DOD Approach to Business Transformation
- DOD Business Systems Modernization
- DOD Support Infrastructure Management
- DOD Financial Management
- DOD Supply Chain Management
- DOD Weapon Systems Acquisition

Ensuring Public Safety and Security

- Mitigating Gaps in Weather Satellite Data (new)
- Strengthening Department of Homeland Security Management Functions
- Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland
- Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures
- Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests
- Revamping Federal Oversight of Food Safety
- Protecting Public Health through Enhanced Oversight of Medical Products
- Transforming EPA's Processes for Assessing and Controlling Toxic Chemicals

Managing Federal Contracting More Effectively

- DOD Contract Management
- DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management
- NASA Acquisition Management

Assessing the Efficiency and Effectiveness of Tax Law Administration

- Enforcement of Tax Laws

Modernizing and Safeguarding Insurance and Benefit Programs

- Improving and Modernizing Federal Disability Programs
- Pension Benefit Guaranty Corporation Insurance Programs
- Medicare Program
- Medicaid Program
- National Flood Insurance Program

Source: GAO.

Mr. Chairman, Ranking Member Coburn, and Members of the Committee:

Thank you for the opportunity to discuss our 2013 government-wide high risk update¹ and to focus especially on the progress made in one high-risk area—*Strengthening Department of Homeland Security Management Functions*. Since 1990, we have regularly reported on government operations that we identified as high risk due to their greater vulnerability to fraud, waste, abuse, and mismanagement, or the need for transformation to address economy, efficiency, or effectiveness challenges. Our high risk program, supported by this committee and the House Committee on Oversight and Government Reform, has brought much-needed focus to problems impeding effective government and costing billions of dollars each year.

In November 2000, we published our criteria and process of determining those areas across government deemed to be high risk.² That document, based on input we received from Congress and the executive branch, including heads of major agencies and the Chief Financial Officers Council, specified that to determine which federal government programs and functions should be added to GAO's High Risk List, we consider whether the program or function is of national significance or is key to government performance and accountability. Further, we consider qualitative factors, such as whether the risk

- involves public health or safety, service delivery, national security, national defense, economic growth, or privacy or citizens' rights, or
- could result in significantly impaired service, program failure, injury or loss of life, or significantly reduced economy, efficiency, or effectiveness.

In addition, we also review the exposure to loss in quantitative terms, such as the value of major assets being impaired; revenue sources not being realized; or major agency assets being lost, stolen, damaged, or wasted. We also consider corrective measures planned or under way to

¹GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

²GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: November 2000).

resolve a material control weakness and the status and effectiveness of these actions.

When legislative, administration, and agency actions, including those in response to our recommendations, result in significant progress toward resolving a high-risk problem, we remove the high-risk designation. As detailed in our November 2000 guidance, the five criteria for determining if a high-risk designation can be removed are:

- A demonstrated strong commitment and top leadership support to address the risk(s).
- The capacity (i.e., the people and other resources) to resolve the risk(s).
- A corrective action plan(s) that defines the root causes, identifies effective solutions, and provides for substantially completing corrective measures near term, including but not limited to steps necessary to implement solutions we recommended.
- A program instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.
- The ability to demonstrate progress in having implemented corrective measures.

In recent years, Congress has passed several laws—which are discussed in our 2013 high risk update—targeting high-risk areas. In addition, top administration officials have continued to show their commitment to ensuring that high-risk areas receive attention and oversight. The Office of Management and Budget (OMB) regularly convenes meetings for agencies to provide progress updates on high-risk issues. When a high-risk issue area ranges across agencies, OMB coordinates with representatives from multiple agencies to participate. These meetings typically include OMB's Deputy Director for Management, top leadership from the agencies, other administration and agency staff members responsible for addressing the high-risk issue, as well as myself and others from GAO.

This congressional and agency commitment is critical to resolving high-risk issues. For example, the Department of Homeland Security (DHS) has made considerable progress in transforming its original component agencies into a single cabinet-level department and positioning itself to

ultimately achieve its full potential. As a result, we narrowed the scope of the high-risk area as reflected in the changed name from *Implementing and Transforming the Department of Homeland Security* to *Strengthening the Department of Homeland Security Management Functions*.

While there has been notable progress addressing the 30 high-risk issues that are currently on GAO's High Risk List, much remains to be done. Our 2013 high risk update report and website³ provide details for each of these issues, describing the nature of the risks, what actions have been taken to address them, and what remains to be done to make further progress. The details in our report, along with successful implementation by agencies and continued oversight by Congress, can form a solid foundation for progress to address risks and improve programs and operations.

Government-wide 2013 High Risk Update

High-Risk Designation Removed

For our 2013 high risk update, we determined that two areas warranted removal from the High Risk List due to the progress that had been made—*Management of Interagency Contracting* and *IRS Business Systems Modernization*. Additional details for both areas can be found in Appendix I. A brief summary follows.

Management of Interagency Contracting

Interagency contracting—where one agency either places an order using another agency's contract or obtains contracting support services from another agency—can help streamline the procurement process, take advantage of unique expertise in a particular type of procurement, and achieve savings. While this method of contracting can save the government money and effort when properly managed, it also poses a variety of risks.

In 2005, we designated the management of interagency contracting as high risk due in part to unclear lines of accountability between customer

³GAO's High Risk website, <http://www.gao.gov/highrisk/>.

and assisting agencies and the potential for improper use, including out-of-scope work and noncompliance with competition requirements. We identified the continuing need for additional management controls and guidance and clearer definitions of roles and responsibilities as keys to addressing these issues. We also highlighted challenges agencies faced in fully realizing the benefits of interagency contracts, including the lack of data and the risk of potential duplication when new contracting vehicles are created. To address these issues, we identified the need for a policy framework and business case analysis requirements to support the creation of certain new contracts and improved data on existing interagency contracts.

As detailed in our 2013 high risk update report, we are removing the management of interagency contracting from the High Risk List based on: (1) continued progress made by agencies in addressing identified deficiencies, (2) establishment of additional management controls, (3) creation of a policy framework for establishing new interagency contracts, and (4) steps taken to address the need for better data on these contracts.

Specifically, most agencies have taken steps to implement and reinforce interagency contracting policies to address prior concerns about the improper use of these contracts. For example, we have noted improvements in procedures used in making purchases on behalf of the Department of Defense (DOD)—the largest user of interagency contracts. These included better defined roles and responsibilities and enhanced controls over funding procedures. Additionally, the DOD Inspector General has reported a significant decrease in problems with DOD procurements through other federal agencies in congressionally mandated reviews of interagency acquisitions. With respect to management controls, Federal Acquisition Regulation (FAR) provisions on interagency acquisitions were revised to require that agencies make a best procurement approach determination to justify the use of an interagency contract and prepare written interagency agreements outlining the roles and responsibilities of customer and assisting organizations.⁴ As we recently reported, OMB analyzed reports from the 24 agencies that account for almost all contract spending government-

⁴FAR § 17.502-1. The interim FAR rule was issued in December 2010; the final rule was issued in February 2012.

wide and found that most had implemented management controls to reinforce the new FAR requirements and strengthen the management of interagency acquisitions. All 24 agencies also reported having oversight mechanisms to ensure their internal controls were operating properly.⁵ In response to congressional direction⁶ and our prior recommendation, OMB established a policy framework in September 2011 to govern the creation of new interagency contract vehicles.⁷ The framework addresses concerns about potential duplication by requiring agencies to develop a thorough business case prior to establishing certain contract vehicles. Finally, in response to our recommendations, OMB and the General Services Administration have taken a number of steps to address the need for better data on interagency contract vehicles. These efforts should enhance both government-wide efforts to manage interagency contracts and agency efforts to conduct market research and negotiate better prices.

Importantly, congressional oversight sustained over several years has been vital in addressing the issues that led this area to be designated high risk. Removing the management of interagency contracting from the High Risk List does not mean that the federal government's use of these contracts is without challenges. But, we believe there are mechanisms in place that OMB and federal agencies can use to identify and address interagency contracting issues before they put the government at significant risk for waste, fraud, or abuse. We also will continue to monitor developments in this area.

IRS Business Systems
Modernization

Internal Revenue Service (IRS) Business Systems Modernization (BSM) is a multi-billion dollar, highly complex effort that involves the development and delivery of a number of modernized tax administration and internal management systems as well as core infrastructure projects

⁵GAO, *Interagency Contracting: Agency Actions Address Key Management Challenges, but Additional Steps Needed to Ensure Consistent Implementation of Policy Changes*, GAO-13-133R (Washington, D.C.: January 2013). We also reported on DOD's implementation of the new FAR requirements and found that for almost all of the selected orders, DOD effectively delineated roles and responsibilities by completing interagency agreements as required.

⁶Pub. L. No. 110-417, § 865 (2008).

⁷OMB, *Office of Federal Procurement Policy, Development, Review, and Approval of Business Cases for Certain Interagency and Agency-Specific Acquisitions* (Washington, D.C.: Sept. 29, 2011).

that are intended to replace the agency's aging business and tax processing systems.

In 1995, we identified serious management and technical weaknesses in IRS's modernization program that jeopardized its successful completion. We recommended many actions to fix the problems, and added IRS's modernization to GAO's High Risk List. In 1995, we also added IRS's financial management to GAO's High Risk List, due to long-standing and pervasive problems that hampered the effective collection of revenues and precluded the preparation of auditable financial statements.⁸ We combined the two issues into one high-risk area in 2005 since resolution of the most serious financial management problems depended largely on the success of the business systems modernization program. Throughout the years, Congress conducted oversight of the BSM program by, among other things, requiring that IRS submit annual expenditure plans that needed to meet certain conditions, including a review by GAO. Because of the significant progress made in addressing the high-risk area, starting in fiscal year 2012, Congress did not require the submission of an annual expenditure plan.

We are removing the BSM program from the High Risk List because of progress made in addressing significant weaknesses in information technology and financial management capabilities. IRS delivered the initial phase of its cornerstone tax processing project and began the daily processing and posting of individual taxpayer accounts in January 2012. This enhanced tax administration and improved service by enabling faster refunds for more taxpayers, allowing more timely account updates and faster issuance of taxpayer notices. IRS has improved its investment management and project oversight processes. IRS also took additional steps to strengthen its IT management capabilities. For example, in July 2011, we noted that IRS had in place close to 80 percent of the practices needed for an effective investment management process, including all of the practices needed for effective project oversight.⁹ In October 2011, we also reported that IRS had embarked on an effort to improve its software development practices using the Carnegie Mellon University Software

⁸GAO, *High-Risk Series: An Overview*, HR-95-1 (Washington, D.C.: Feb. 1, 1995).

⁹GAO, *Investment Management: IRS Has a Strong Oversight Process But Needs to Improve How It Continues Funding Ongoing Investments*, GAO-11-587 (Washington, D.C.: July 20, 2011).

Engineering Institute's Capability Maturity Model Integration (CMMI), which calls for disciplined software development and acquisition practices which are considered industry best practices. In September 2012, IRS's application development organization reached CMMI maturity level 3, a high achievement by industry standards.¹⁰

As with all areas removed from the High Risk List, we will continue to monitor how future events unfold both with the IRS modernization efforts and in the *Enforcement of Tax Laws*, which remains on the High Risk List.

New High-Risk Areas

This year, we added two new areas to the High Risk List—*Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks* and *Mitigating Gaps in Weather Satellite Data*. Additional details for both areas can be found in Appendix II. A brief summary follows.

Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks

Climate change is a complex, crosscutting issue that poses risks to many environmental and economic systems—including agriculture, infrastructure, ecosystems, and human health—and presents a significant financial risk to the federal government. Among other impacts, climate change could threaten coastal areas with rising sea levels, alter agricultural productivity, and increase the intensity and frequency of severe weather events. As observed by the United States Global Change Research Program, the impacts and costliness of weather disasters—resulting from floods, drought, and other events such as tropical cyclones—are expected to increase in significance as what are considered “rare” events become more common and intense due to anticipated changes in the global climate system. Moreover, according to the National Oceanic and Atmospheric Administration's National Climatic Data Center (NCDC), the United States has sustained 144 weather and climate-related disasters since 1980, in which overall damages reached

¹⁰The CMMI ranks organizational maturity according to five levels. Maturity levels 2 through 5 require verifiable existence and use of certain key process areas. At maturity level 3, known as the “defined” level, processes are well characterized and understood, and are described in standards, procedures, tools, and methods. The organization's set of standard processes, which is the basis for maturity level 3, is established and improved over time. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. In addition, processes are managed more proactively using an understanding of the interrelationships of process activities and detailed measures of the process, its work products, and its services.

or exceeded \$1 billion each, with 14 events in 2011 and 11 events in 2012. NCDIC estimates that 2012 will surpass 2011 in terms of aggregate costs for annual billion-dollar disasters, even with fewer disasters.

The federal government owns extensive infrastructure, such as defense installations, and manages 29 percent of the land in the United States; and insures property through the National Flood Insurance Program and crops through the Federal Crop Insurance Corporation. As of November 2012, FEMA owes the Treasury approximately \$20 billion—up from \$17.8 billion pre-Superstorm Sandy—and had not repaid any principal on the loan since 2010. Further, the federal government's crop insurance costs have increased in recent years—rising from an average of \$3.1 billion per year from fiscal years 2000 through 2006, to an average of \$7.6 billion per year from fiscal years 2007 through 2012—and, according to the Congressional Budget Office, are projected to increase further.

The federal government also provides emergency aid in response to natural disasters. For example, we reported in September 2012 that major disaster declarations have increased over recent decades to a record of 98 in fiscal year 2011 compared with 65 in 2004. Had FEMA adjusted the indicator on which it principally relies to determine whether to recommend that a jurisdiction receive public assistance funding, to reflect changes in personal income and inflation, 44 percent and 25 percent fewer disaster declarations, respectively, would have met the threshold for public assistance during fiscal years 2004 through 2011. Over that period, the Federal Emergency Management Agency (FEMA) obligated more than \$80 billion in federal assistance for major disasters.¹¹ The federal government's exposure to major disasters continues to pose risks. Most recently, Congress provided more than \$60 billion in budget authority for disaster assistance in the wake of Superstorm Sandy.¹²

We have found that the federal government is not well positioned to address the fiscal exposure presented by climate change, and needs a government-wide strategic approach with strong leadership to manage

¹¹GAO, *Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own*, GAO-12-838 (Washington, D.C.: Sept. 12, 2012).

¹²Congress provided \$9.7 billion in borrowing authority for the National Flood Insurance Program and about \$50.6 billion in appropriated funds. Pub. L. No. 113-1 (2013); Pub. L. No. 113-2 (2013).

related risks. We reported in 2009 that while policymakers increasingly viewed climate change adaptation—defined as adjustments to natural or human systems in response to actual or expected climate change—as a risk-management strategy to protect vulnerable sectors and communities that might be affected by changes in the climate, the federal government’s emerging adaptation activities were carried out in an ad hoc manner and were not well coordinated across federal agencies, let alone with state and local governments.¹³ Subsequently, in May 2011, we reported that there was no coherent strategic government-wide approach to climate change funding and that federal officials do not have a shared understanding of strategic government-wide priorities.¹⁴ At that time, we recommended that the appropriate entities within the Executive Office of the President clearly establish federal strategic climate change priorities, including the roles and responsibilities of the key federal entities, taking into consideration the full range of climate-related activities within the federal government. The relevant federal entities have not directly addressed this recommendation.

Federal agencies have made some progress toward better organizing across agencies, within agencies, and among different levels of government; however, the increasing fiscal exposure for the federal government calls for more comprehensive and systematic strategic planning, including, but not limited to, the following:

- A government-wide strategic approach with strong leadership and the authority to manage climate change risks that encompasses the entire range of related federal activities and addresses all key elements of strategic planning. Federal agencies recently released draft climate change adaptation plans. While individual agency actions are necessary, a centralized strategy driven by a government-wide plan is also needed to reduce the federal fiscal exposure to climate change, maximize investments, achieve efficiencies, and better position the government for success.

¹³GAO, *Climate Change Adaptation: Strategic Federal Planning Could Help Government Officials Make More Informed Decisions*, GAO-10-113 (Washington, D.C.: Oct 7, 2009).

¹⁴GAO, *Climate Change: Improvements Needed to Clarify National Priorities and Better Align Them with Federal Funding Decisions*, GAO-11-317 (Washington, D.C.: May 20, 2011).

-
- More information to understand and manage federal insurance programs' long-term exposure to climate change and analyze the potential impacts of an increase in the frequency or severity of weather-related events on their operations.
 - A government-wide approach for providing (1) the best available climate-related data for making decisions at the state and local level and (2) assistance for translating available climate-related data into information that officials need to make decisions.
 - Potential gaps in satellite data need to be effectively addressed.
 - Improved criteria for assessing a jurisdiction's capability to respond to and recover from a disaster without federal assistance, and to better apply lessons from past experience when developing disaster cost estimates.

Mitigating Gaps in Weather Satellite Data

Potential gaps in environmental satellite data beginning as early as 2014 and lasting as long as 53 months have led to concerns that future weather forecasts and warnings—including warnings of extreme events such as hurricanes, storm surges, and floods—will be less accurate and timely. A number of decisions are needed to ensure contingency and continuity plans can be implemented effectively. We and others—including an independent review team reporting to the Department of Commerce and the department's Inspector General—have raised concerns that problems and delays on environmental satellite acquisition programs will result in gaps in the continuity of critical satellite data used in weather forecasts and warnings. The importance of such data was recently highlighted by the advance warnings of the path, timing, and intensity of Superstorm Sandy.

Since the 1960s, the United States has used both polar-orbiting and geostationary satellites to observe the earth and its land, oceans, atmosphere, and space environments. Polar-orbiting satellites constantly circle the earth in an almost north-south orbit providing global coverage of environmental conditions that affect the weather and climate. As the earth rotates beneath it, each polar-orbiting satellite views the entire earth's surface twice a day. In contrast, geostationary satellites maintain a fixed position relative to the earth from a high-level orbit of about 22,300 miles in space. Used in combination with ground, sea, and airborne observing systems, both types of satellites have become an indispensable part of monitoring and forecasting weather and climate. Polar-orbiting satellites provide the data that go into numerical weather prediction models, which

are a primary tool for forecasting weather days in advance—including forecasting the path and intensity of hurricanes and tropical storms. Geostationary satellites provide frequently-updated graphical images that are used to identify current weather patterns and provide short-term warnings.

In regards to polar satellites, the National Oceanic and Atmospheric Administration (NOAA) must make decisions about (1) whether and how to extend support for legacy satellite systems so that their data might be available if needed, (2) how much time and resources to invest in improving satellite models so that they assimilate data from alternative sources, (3) whether to pursue international agreements for access to additional satellite systems and how best to resolve any security issues with the foreign data, (4) when and how to test the value and integration of alternative data sources, and (5) how these preliminary mitigation plans will be integrated with NOAA's broader end-to-end plans for sustaining weather forecasting capabilities. NOAA must also identify time frames for when these decisions will be made. We have ongoing work assessing NOAA's efforts to limit and mitigate potential polar satellite data gaps.

For the geostationary satellites, NOAA must demonstrate its progress in conducting training and simulations for contingency scenarios, evaluating the status of viable foreign satellites, and working with the user community to account for differences in product coverage under contingency scenarios. These steps are critical for NOAA to move forward in documenting the processes it will take to implement its contingency plans. Once these activities are completed, NOAA should update its contingency plan to provide more details on its contingency scenarios, associated time frames, and any preventative actions it is taking to minimize the possibility of a gap. We have ongoing work assessing NOAA's actions to ensure that its plans are viable and that continuity procedures are in place and have been tested.

Modified High-Risk Area

One area—*Modernizing the Outdated U.S. Financial Regulatory System*—has been modified due to changing circumstances to include the Federal Housing Administration (FHA). To reflect these changing circumstances, the name of the area has been changed to *Modernizing the U.S. Financial Regulatory System and Federal Role in Housing Finance*. We first designated this area as high risk in 2009 due to the urgent need to reform the fragmented and outdated U.S. financial regulatory system. As detailed in our 2013 high risk update report, many actions are under way to implement oversight by new regulatory bodies

and new requirements for market participants, although many rulemakings remain unfinished. Among the additional actions needed are resolving the role of the two housing-related government-sponsored enterprises—Fannie Mae and Freddie Mac—that continue operating under government conservatorships. However, a new challenge for the markets has also evolved as the decline in private sector participation in housing finance that began with the 2007-2009 financial crisis has resulted in much greater activity by FHA, whose single-family loan insurance portfolio has grown from about \$300 billion in 2007 to more than \$1.1 trillion in 2012. Although required to maintain capital reserves equal to at least 2 percent of its portfolio, FHA's capital reserves have fallen below this level, due partly to increases in projected defaults on the loans it has insured.

As a result, we are modifying this high-risk area to include FHA and acknowledging the need for actions beyond those already taken to help restore FHA's financial soundness and define its future role. One such action would be to determine the economic conditions that FHA's primary insurance fund would be expected to withstand without drawing on the Treasury. Recent events suggest that the 2-percent capital requirement may not be adequate to avoid the need for Treasury support under severe stress scenarios. Additionally, actions to reform the government-sponsored enterprises and to implement mortgage market reforms in the Dodd-Frank Act will need to consider the potential impacts on FHA's risk exposure.

Additional information on this area is provided on page 81 of our 2013 high risk update.¹⁵

¹⁵GAO-13-283.

Strengthening Department of Homeland Security Management Functions

Since our 2011 update, sufficient progress has been made to narrow the scope of three areas, including *Strengthening Department of Homeland Security Management Functions*.¹⁶ In 2003, we designated implementing and transforming the Department of Homeland Security (DHS) as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department. Further, failure to effectively address DHS's management and mission risks could have serious consequences for U.S. national and economic security. Given the significant effort required to build and integrate a department as large and complex as DHS, our initial high-risk designation addressed the department's initial transformation and subsequent implementation efforts, to include associated management and programmatic challenges. At that time, we reported that the creation of DHS was an enormous undertaking that would take time to achieve, and that the successful transformation of large organizations, even those undertaking less strenuous reorganizations, could take years to implement.

Over the past 10 years, the focus of this high-risk area has evolved in tandem with DHS's maturation and evolution. The overriding tenet has consistently remained the department's ability to build a single, cohesive and effective department that is greater than the sum of its parts—a goal that requires effective collaboration and integration of its various components and management functions. In 2007, in reporting on DHS's progress since its creation, as well as in our 2009 high risk update, we reported that DHS had made more progress in implementing its range of missions rather than its management functions, and that continued work was needed to address an array of programmatic and management challenges.

DHS's initial focus on mission implementation was understandable given the critical homeland security needs facing the nation after the department's establishment, and the challenges posed by its creation, integration and transformation. As DHS continued to mature, and as we reported in our assessment of DHS's progress and challenges 10 years after 9/11, we found that the department implemented key homeland security operations and achieved important goals in many areas to create

¹⁶Federal Oil and Gas Resources and Department of Energy's Contract Management for the National Nuclear Security Administration and Office of Environmental Management were the other high-risk areas that were narrowed. Appendix III has information on these issues.

and strengthen a foundation to reach its potential.¹⁷ However, we also identified that more work remained for DHS to address weaknesses in its operational and implementation efforts, and to strengthen the efficiency and effectiveness of those efforts. We further reported that continuing weaknesses in DHS's management functions had been a key theme impacting the department's implementation efforts. Recognizing DHS's progress in transformation and mission implementation, our 2011 high risk update focused on the continued need to strengthen DHS's management functions (acquisition, information technology, financial management, and human capital) and integrate those functions within and across the department, as well as the impact of these challenges on the department's ability to effectively and efficiently carry out its missions.

While challenges remain for DHS to address across its range of missions, the department has made considerable progress in transforming its original component agencies into a single cabinet-level department and positioning itself to achieve its full potential. As a result, we narrowed the scope of the high-risk area and changed the name from Implementing and Transforming the Department of Homeland Security to Strengthening the Department of Homeland Security Management Functions.

Since our last high risk update in January 2011, we have regularly met with senior DHS officials to discuss the department's progress in addressing this high-risk area and written letters summarizing our feedback on DHS's progress and work remaining to address the high-risk designation, most recently in December 2012. Our ongoing dialogue with DHS at the most senior levels has enabled us to understand DHS's perspectives and provided an opportunity for us to consistently communicate our views on DHS's progress and work remaining. DHS has made important progress in implementing, transforming, strengthening, and integrating its management functions, including taking numerous

¹⁷GAO, *Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11*, GAO-11-881 (Washington, D.C.: Sept. 7, 2011). This report addressed DHS's progress in implementing its homeland security missions since it began operations, work remaining, and issues affecting implementation efforts. Drawing from more than 1,000 GAO reports and congressional testimony issued related to DHS programs and operations, and approximately 1,500 recommendations made to strengthen mission and management implementation, this report addressed progress and remaining challenges in such areas as border security and immigration, transportation security, and emergency management, among others.

actions specifically designed to address our criteria for removing areas from the High Risk List; however, this area remains high risk because the department has significant work ahead.

Leadership commitment. The Secretary, Deputy Secretary, and Under Secretary for Management of Homeland Security and other senior officials have continued to demonstrate commitment and top leadership support for addressing the department's management challenges. They have also taken actions to institutionalize this commitment to help ensure the long-term success of the department's efforts. For example, in May 2012, the Secretary of Homeland Security modified the delegations of authority between the Management Directorate and its counterparts at the component level to clarify and strengthen the authorities of the Under Secretary for Management across the department. Senior DHS officials have also periodically met with us over the past 4 years to discuss the department's plans and progress in addressing this high-risk area, during which we provided feedback on the department's efforts. According to these officials, and as demonstrated through their progress, the department is committed to demonstrating measurable, sustained progress in addressing this high-risk area.

Corrective action plan. DHS has established a plan for addressing this high-risk area. Specifically, in a September 2010 letter to DHS, we identified and DHS agreed to achieve 31 actions and outcomes that are critical to addressing the challenges within the department's management areas and in integrating those functions across the department. These key actions and outcomes include, among others, validating required acquisition documents in accordance with a department-approved, knowledge-based acquisition process, and obtaining and then sustaining unqualified audit opinions for at least 2 consecutive years on the department-wide financial statements. In January 2011, DHS issued its initial Integrated Strategy for High Risk Management, which included key management initiatives and related corrective action plans for addressing its management challenges and the outcomes we identified. DHS provided updates of its progress in implementing these initiatives and corrective actions in its later versions of the strategy—June 2011, December 2011, June 2012, and September 2012. The comprehensive strategy, if implemented and sustained, provides a path for DHS to be removed from GAO's High Risk List.

Framework to monitor progress. DHS has established a framework for monitoring its progress in implementing its corrective actions and addressing the 31 actions and outcomes. In the June 2012 update to the

Integrated Strategy for High Risk Management, DHS included, for the first time, performance measures to track its progress in implementing all of its key management initiatives. Additionally, the Under Secretary for Management holds quarterly internal progress review meetings with senior officials from each management function to discuss progress toward achieving milestones and meeting performance goals. It will be important for DHS to continue to track progress toward achieving its goals and monitor and refine its measures and corrective actions, as needed.

Capacity. In June 2012, DHS identified the resources needed to implement most (154 of 173) of its corrective actions, but needs to continue to identify resources for the remaining corrective actions; determine that sufficient resources and staff are committed to initiatives; work to mitigate shortfalls and prioritize initiatives, as needed; and communicate to senior leadership critical resource gaps. DHS also identified ways in which it is leveraging resources to implement corrective actions, which is particularly important in light of constrained budgets. For example, in October 2012, DHS reported that it is pooling resources and working across functional lines to create cross functional, matrixed teams and executive steering committees to ensure timely implementation of the strategy. However, it is too soon to determine whether this approach is a sustainable way for DHS to address the resource challenges and capacity gaps that have affected its implementation efforts at the department and component levels.

Demonstrated, sustained progress. DHS has made important progress in implementing corrective actions across its management functions, but it has not yet demonstrated sustainable, measurable progress in addressing key challenges that continue to remain within these functions and in the integration of those functions. DHS has implemented a number of actions demonstrating the department's progress in improving its management functions. For example, DHS established the Office of Program Accountability and Risk Management in October 2011 to be responsible for the department's overall acquisition governance process. DHS also established a formal IT Program Management Development Track and staffed Centers of Excellence with subject matter experts to that as of March 2012, approximately two-thirds of the department's major IT investments we reviewed (47 of 68) were meeting current cost and schedule commitments (i.e., goals). Additionally, in the financial management area, DHS has reduced the number of material weaknesses in internal controls and obtained a qualified audit opinion on its fiscal year 2012 financial statements. DHS has also implemented common policies,

procedures, and systems, such as those related to human capital, across its management functions.

However, DHS still has considerable work ahead in many areas. For example, in September 2012, we reported that most of DHS's major acquisition programs continue to cost more than expected, take longer to deploy than planned, or deliver less capability than promised. We identified 42 programs that experienced cost growth or schedule slips, or both, with 16 of the programs' costs increasing from a total of \$19.7 billion in 2008 to \$52.2 billion in 2011—an aggregate increase of 166 percent. Further, while DHS has defined and begun to implement a vision for a tiered governance structure to improve information technology (IT) management, we reported in July 2012 that the governance structure covers less than 20 percent (about 16 of 80) of DHS's major IT investments and 3 of its 13 portfolios. DHS has also been unable to obtain an audit opinion on its internal controls over financial reporting, and needs to obtain and sustain unqualified audit opinions for at least two consecutive years on the department-wide financial statements. Finally, federal surveys have consistently found that DHS employees are less satisfied with their jobs than the government-wide average. Key to addressing the department's management challenges is DHS demonstrating the ability to achieve sustained progress across the 31 actions and outcomes we identified as needed to address the high-risk designation, to which DHS agreed. As shown in table 1, we believe DHS has fully addressed 6, mostly addressed 2, partially addressed 16, and initiated 7 of the 31 key actions and outcomes.

Table 1: Assessment of DHS's Progress in Addressing Key Actions and Outcomes

Key outcomes	Fully addressed ^a	Mostly addressed ^b	Partially addressed ^c	Initiated ^d	Total
Acquisition management			2	3	5
IT management	1	1	4		6
Financial management	2		3	4	9
Human capital management		1	6		7
Management integration	3		1		4
Total	6	2	16	7	31

Source: GAO analysis of DHS documents, interviews, and prior GAO reports.

^a"Fully Addressed": Outcome is fully addressed.

^b"Mostly Addressed": Progress is significant and a small amount of work remains.

^c"Partially Addressed": Progress is measurable, but significant work remains.

^d"Initiated": Activities have been initiated to address outcome, but it is too early to report progress.

To more fully address our high-risk designation, DHS needs to continue implementing its *Integrated Strategy for High Risk Management* and show measurable, sustainable progress in implementing its key management initiatives and corrective actions and achieving outcomes. In doing so, it will be important for DHS to:

- make continued progress in addressing the 31 actions and outcomes and demonstrate that systems, personnel, and policies are in place to ensure that progress can be sustained over time;
- maintain its current level of top leadership support and sustained commitment to ensure continued progress in executing its corrective actions through completion;
- continue to implement its plan for addressing this high-risk area and periodically report its progress to Congress and GAO;
- closely track and independently validate the effectiveness and sustainability of its corrective actions and make midcourse adjustments, as needed; and
- monitor the effectiveness of its efforts to establish reliable resource estimates at the department and component levels, address and work

to mitigate any resource gaps, and prioritize initiatives as needed to ensure it has the capacity to implement and sustain its corrective actions.

We will continue to monitor DHS's efforts in this high-risk area to determine if the actions and outcomes are achieved and sustained.

Additional information on this area is provided on page 161 of our 2013 high risk update.¹⁸

Sustaining Attention on High-Risk Programs

Overall, the government continues to take high-risk problems seriously and is making long-needed progress toward correcting them. Congress has acted to address several individual high-risk areas through hearings and legislation. Our high risk update and high risk website, <http://www.gao.gov/highrisk/>, can help inform the oversight agenda for the 113th Congress and guide efforts of the administration and agencies to improve government performance and reduce waste and risks. In support of Congress and to further progress to address high-risk issues, we continue to review efforts and make recommendations to address high-risk areas problems. Continued perseverance in addressing high-risk areas will ultimately yield significant benefits.

In that regard, the Government Performance Results Act (GPRA) Modernization Act of 2010 (GPRAMA) provides the Executive Branch and Congress with new tools to identify and address management weaknesses that are undermining agencies' capacity to achieve results. For example, the act requires agencies, in their annual performance plans, to describe the major management challenges they face—which, by definition, cover issues we have identified as high risk—as well as the actions they plan to address these challenges. In addition, agencies are to identify performance goals, performance measures, and milestones to gauge progress toward resolving these challenges.

In addition, OMB is required to develop long-term goals to improve management functions across the government. The act specifies that these goals should include five areas: financial management, human capital management, information technology management, procurement

¹⁸GAO-13-283.

and acquisition management, and real property management. We have identified these areas as key management challenges for the government. Moreover, some aspects of these areas have warranted our designation as high risk, either government-wide or at certain agencies. OMB is required to provide clear milestones and periodic status reports on progress being made and actions needed for additional progress.

Over the years, the Committee on Homeland Security and Governmental Affairs and its predecessors have done commendable work focusing attention on improving government management and performance—by reporting out legislation, such as the original GPRA and GPRAMA, and through hearings, such as this one. Moving forward, congressional oversight and sustained attention by top administration officials will be essential to ensure further improvement in the management and performance of federal programs and operations and addressing high-risk areas.

Thank you, Mr. Chairman, Ranking Member Coburn, and Members of the Committee. This concludes my testimony. I would be pleased to answer questions.

For further information on GAO's high risk program, contact J. Christopher Mihm at (202) 512-6806 or mihmj@gao.gov. For information on DHS, contact Cathleen A. Berrick, 202-512-3404 or berrickc@gao.gov. Contact points for the individual high-risk areas are listed in GAO-13-283 and on our high-risk website, <http://www.gao.gov/highrisk>. Contact points for our Congressional Relations and Public Affairs offices may be found on the last page of this statement.

Appendix I: High-Risk Designation Removed

Management of Interagency Contracting

We are removing the management of interagency contracting from the High Risk List based on (1) continued progress made by agencies in addressing previously identified deficiencies, (2) establishment of additional management controls, (3) creation of a policy framework for establishing new interagency contracts, and (4) steps taken to address the need for better data on these contracts. Congressional oversight and the leadership of the Office of Management and Budget's (OMB) Office of Federal Procurement Policy (OFPP)—which provides direction on government-wide procurement policies—have been vital in addressing the issues that led this area to be designated high risk.

Interagency contracting—where one agency either places an order using another agency's contract or obtains contracting support services from another agency—can help streamline the procurement process, take advantage of unique expertise in a particular type of procurement, and achieve savings. Interagency contracts are designed to leverage the government's buying power and allow for agencies to meet the demands for goods and services at a time when the federal government is focused on achieving efficiencies in the acquisition process. While this method of contracting can save the government money and effort when properly managed, it also poses a variety of risks.

In 2005, we designated the management of interagency contracting as high risk due in part to unclear lines of accountability between customer and assisting agencies and the potential for improper use, including out-of-scope work and noncompliance with competition requirements.¹ In our 2007 high risk update, we identified the continuing need for (1) additional management controls and guidance and (2) clearer definitions of roles and responsibilities as the keys to addressing these issues.² In our 2011 high risk update, we highlighted additional challenges agencies faced in fully realizing the benefits of interagency contracts, including the lack of data and the risk of potential duplication when new contracting vehicles are created.³ Duplication among interagency contracts can result in missed opportunities to leverage the government's buying power and may adversely affect the administrative efficiencies and cost savings expected

¹GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

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

³GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

with their use. To address these issues, our prior work identified the need for (1) a policy framework and business case analysis requirements to support the creation of certain new contracts and (2) improved data on existing interagency contracts.

The federal government has made significant progress in reducing the interagency contracting risks that led to our high-risk designation. In our 2009 and 2011 high risk updates we noted improvements in procedures used in making purchases on behalf of the Department of Defense (DOD)—the largest user of interagency contracts. These included better defined roles and responsibilities and enhanced controls over funding procedures. Additionally, the DOD Inspector General has reported a significant decrease in problems with DOD procurements through other federal agencies in congressionally mandated reviews of interagency acquisitions. We also noted that the General Services Administration (GSA) and OMB have established corrective action plans to implement our prior recommendations. Since our last update, as discussed in the following sections, federal agencies have continued to address weaknesses related to the use, creation, and oversight of interagency contracting vehicles.

Strengthened management controls for the use of interagency contracts. Most agencies have taken steps to implement and reinforce interagency contracting policies to address prior concerns about the improper use of these contracts. In response to congressional direction,⁴ Federal Acquisition Regulation (FAR) provisions on interagency acquisitions were revised to require that agencies make a best procurement approach determination to justify the use of an interagency contract and prepare written interagency agreements outlining the roles and responsibilities of customer and assisting organizations.⁵ The best procurement approach determination ensures that the requesting agency considers factors such as the suitability of the contract vehicle and compliance with laws and policies. Congress also strengthened requirements for interagency acquisitions performed on behalf of DOD as well as the competition rules for placing orders on multiple-award

⁴Pub. L. No. 110-417, § 865 (2008).

⁵FAR § 17.502-1. The interim FAR rule was issued in December 2010; the final rule was issued in February 2012.

contracts, which are commonly used in interagency acquisitions.⁶ As we recently reported, OMB's October 2012 analysis of reports from the 24 agencies that account for almost all contract spending government-wide found that most had implemented management controls to reinforce the new FAR requirements and strengthen the management of interagency acquisitions. All 24 agencies also reported having oversight mechanisms to ensure their internal controls were operating properly.⁷

New controls over creation of new interagency contract vehicles. In response to congressional direction⁸ and our prior recommendation, OMB established a policy framework in September 2011 to govern the creation of new interagency contract vehicles.⁹ The framework addresses concerns about potential duplication by requiring agencies to develop a thorough business case prior to establishing certain contract vehicles. The guidance further requires senior agency officials to approve the business cases and post them on an OMB website to provide interested federal stakeholders an opportunity to offer feedback. OMB then is able to conduct follow-up with sponsoring agencies if significant questions, including ones related to duplication, are raised during the vetting process. OMB also has established a new strategic sourcing governance council, which is expected to examine how to use existing interagency contract vehicles to support government-wide strategic sourcing efforts.

Improved data on interagency contracts. In response to our recommendations, OMB and GSA have taken a number of steps to address the need for better data on interagency contract vehicles. These efforts should enhance both government-wide efforts to manage interagency contracts and agency efforts to conduct market research and negotiate better prices. To promote better and easier access to data on

⁶Pub. L. No. 110-181, § 801(b) (2008) and Pub. L. No. 110-417, § 863 (2008).

⁷GAO, *Interagency Contracting: Agency Actions Address Key Management Challenges, but Additional Steps Needed to Ensure Consistent Implementation of Policy Changes*, GAO-13-133R (Washington, D.C.: January 2013). We also reported on DOD's implementation of the new FAR requirements and found that for almost all of the selected orders, DOD effectively delineated roles and responsibilities by completing interagency agreements as required.

⁸Pub. L. No. 110-417, § 865 (2008).

⁹OMB, *OFPP, Development, Review, and Approval of Business Cases for Certain Interagency and Agency-Specific Acquisitions* (Washington, D.C.: Sept. 29, 2011).

Appendix I: High-Risk Designation Removed

existing contracts, OMB has made improvements to its Interagency Contract Directory, a searchable online database of indefinite-delivery vehicles available for interagency use. It has also posted information on government-wide acquisition contracts and blanket purchase agreements available for use under the Federal Strategic Sourcing Initiative on an OMB website, accessible by federal agencies.¹⁰ Improving the availability of data is also a key facet of GSA's Schedules Modernization initiative, launched in June 2012. GSA has several pilot projects underway to collect and share data on its Multiple Award Schedules program, with the goal of improving pricing. GSA also has assembled a data team to improve access to comprehensive and reliable data across GSA contracting programs.

Removing the management of interagency contracting from the High Risk List does not mean that the federal government's use of these contracts is without challenges. For example, we and the DOD Inspector General have found instances in which DOD did not complete best procurement approach determinations as required.¹¹ Continued management attention is necessary. But, we believe there are mechanisms in place that OMB and federal agencies can use to identify and address interagency contracting issues before they put the government at significant risk for waste, fraud, or abuse. For example, the revised FAR rules on interagency acquisitions require senior procurement executives to submit an annual report on interagency acquisitions to OMB, which can use these to identify issues and risks at the agency level as well as government-wide trends. In addition, many agencies have reported building interagency contracting into internal reviews. Finally, we plan to continue to monitor the management of interagency contracts in our reviews of federal contracting.

¹⁰The Federal Strategic Sourcing Initiative was established in 2005 to address government-wide opportunities to strategically source commonly purchased products and services.

¹¹GAO-13-133R and Department of Defense, Inspector General, *Contracting Improvements Still Needed in DOD's FY 2011 Purchases Made Through the Department of Veterans Affairs*, DODIG-2013-028 (Alexandria, VA.: Dec. 7, 2012).

**IRS Business Systems
Modernization**

We are removing the Internal Revenue Service's (IRS) Business Systems Modernization (BSM) program from the High Risk List because of IRS's progress in addressing the significant weaknesses in information technology (IT) and financial management capabilities that led to the high-risk designation, and its commitment to sustaining progress in the future. As we have with other areas we have removed, we will continue to monitor this area, as appropriate, to ensure that the improvements we have noted are sustained.

BSM is a multi-billion dollar, highly-complex effort that involves the development and delivery of a number of modernized tax administration and internal management systems as well as core infrastructure projects that are intended to replace the agency's aging business and tax processing systems. It is critical to providing improved and expanded service to taxpayers and internal business efficiencies for IRS and providing the reliable and timely financial management information needed to better enable the agency to justify its resource allocation decisions and funding requests. IRS began modernizing its timeworn, paper-intensive approach to tax returns processing in the mid-1980s.

In 1995, we identified serious management and technical weaknesses in the modernization program that jeopardized its successful completion. We recommended many actions to fix the problems, and added IRS's modernization to our High Risk List. In 1995, we also added the agency's financial management to our High Risk List due to long-standing and pervasive problems which hampered the effective collection of revenues and precluded the preparation of auditable financial statements.¹² We combined the two issues into one high-risk area in 2005 since resolution of the most serious financial management problems depended largely on the success of the business systems modernization program.

In 2007 and 2009, we reported that IRS had made progress in establishing management capabilities and addressing financial management weaknesses.¹³ For example, in 2007, the agency developed a high-level modernization vision and strategy to address program changes and provide a modernization road map. In addition, it developed

¹²GAO, *High-Risk Series: An Overview*, HR-95-1 (Washington, D.C.: Feb. 1, 1995).

¹³GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: Jan. 22, 2009), and GAO-07-310.

policies, procedures, and tools for developing and managing project requirements. IRS also implemented the initial phase of several key automated financial management systems, including a cost accounting module that it populated with data; developed a methodology to allocate costs to its business units; improved the reliability of its property and equipment records; and made significant progress in addressing long-standing deficiencies in controls over tax revenue collections, tax refund disbursements, and hard-copy tax receipts and related data. In addition, IRS completed several pilot projects to demonstrate its ability to determine the full cost of its programs and activities.

However, we kept BSM on the High Risk List because many challenges remained, including (1) improving processes for delivering modernized IT systems within cost and schedule estimates, (2) developing the cost and revenue information needed to support day-to-day decision making, and (3) addressing outstanding weaknesses in information security.¹⁴ Throughout those years, Congress conducted oversight of the BSM program by, among other things, requiring that IRS submit annual expenditure plans that needed to meet certain conditions, including a review by GAO.

In our 2011 high risk update,¹⁵ we reported that IRS had continued to make progress in addressing weaknesses in response to our recommendations but needed to leverage its capabilities to successfully deliver its BSM projects. Specifically, we noted that IRS needed to successfully deliver the initial phase of the Customer Account Data Engine 2 (CADE 2)—its cornerstone tax processing project—by moving the processing of individual taxpayer accounts from a weekly processing cycle to a daily processing cycle and delivering a modernized individual taxpayer account database by 2012. We also noted that IRS needed to continue its efforts to achieve expected benefits, including faster refunds, improved customer service, and faster resolution of taxpayer account issues (phase 2 of CADE 2). For financial management issues, in addition to addressing outstanding recommendations, including those associated with information security controls affecting the reliability of financial data, we noted that IRS needed to (1) ensure corrective action plans address all issues and define root causes and (2) strengthen its program for

¹⁴GAO-09-271.

¹⁵GAO-11-278.

monitoring the effectiveness of corrective actions taken in response to our information security recommendations.

Since 2011, IRS has worked to address these issues. For example, the agency delivered the initial phase of CADE 2 and began the daily processing and posting of individual taxpayer accounts in January 2012, enhancing tax administration and improving service by enabling faster refunds for more taxpayers, allowing more timely account updates, and faster issuance of taxpayer notices.¹⁶ Also, in March 2012, IRS established the database housing all individual taxpayer account data and has plans underway to gradually increase its use for customer service and compliance purposes. Further, in May 2012, IRS initiated plans for phase 2 of CADE 2, which is in large part intended to address the unpaid assessment financial material weakness we have reported on in the past. As IRS progresses with this planning effort, it will be important for the agency to identify functionality it can deliver early on so it can begin reaping benefits for its employees and taxpayers and making progress towards retiring the legacy Individual Master File.

IRS also made important progress in addressing information systems-related internal control deficiencies, particularly those involving its networks and systems that had reduced the overall effectiveness of its information security controls and therefore the reliability of its financial data.¹⁷ Notable among these efforts were the (1) formation of cross functional working groups tasked with the identification and remediation of specific at-risk control areas, (2) improvement in controls over the encryption of data transferred between accounting systems, and (3) upgrades to critical network devices on the agency's internal network system. In addition, during fiscal year 2012, IRS continued to devote significant attention and resources to addressing information security controls, and resolved a significant number of the information system-related internal control deficiencies that we previously reported. For example, IRS (1) addressed its outdated operating system and

¹⁶According to IRS, during Filing Season 2012, CADE 2 allowed more timely account updates (taxpayer account updates are viewable by IRS customer service representatives within 48 hours versus an average of 9 days in Filing Season 2011), and faster issuance of taxpayer notices (2.7 million notices sent to taxpayers with accounts processed daily versus 284,000 in Filing Season 2011).

¹⁷GAO, *Financial Audit: IRS's Fiscal Years 2012 and 2011 Financial Statements*, GAO-13-120 (Washington, D.C.: Nov. 9, 2012).

application software so that the versions in use are now supported by vendors, (2) improved the auditing and monitoring capabilities of a general support system, and (3) tested its general ledger system for tax transactions in its current operating environment. Further, IRS funded critical software upgrades for some of its key financial reporting systems, including its administrative accounting system and its procurement system, which was an important step toward addressing its information system issues. These improvements led us to conclude that IRS's remaining deficiencies in internal controls over information security no longer constitute a material weakness for financial reporting as of September 30, 2012. However, IRS still needs to strengthen its program for monitoring the effectiveness of corrective actions taken in response to our information security recommendations.

IRS also took additional steps to strengthen its IT management capabilities. For example, in July 2011, we noted that IRS had in place close to 80 percent of the practices needed for an effective investment management process, including all of the practices needed for effective project oversight.¹⁸ In October 2011, we also reported that IRS had embarked on an effort to improve its software development practices using the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model Integration (CMMI), which calls for disciplined software development and acquisition practices which are considered industry best practices. In September 2012, IRS's application development organization reached CMMI maturity level 3, a high achievement by industry standards.¹⁹

Finally, in October 2011, we highlighted CADE 2 as one of seven successful acquisitions in the federal government because, up to that

¹⁸GAO, *Investment Management: IRS Has a Strong Oversight Process But Needs to Improve How it Continues Funding Ongoing Investments*, GAO-11-587 (Washington, D.C.: July 20, 2011).

¹⁹The CMMI ranks organizational maturity according to five levels. Maturity levels 2 through 5 require verifiable existence and use of certain key process areas. At maturity level 3, known as the "defined" level, processes are well characterized and understood, and are described in standards, procedures, tools, and methods. The organization's set of standard processes, which is the basis for maturity level 3, is established and improved over time. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. In addition, processes are managed more proactively using an understanding of the interrelationships of process activities and detailed measures of the process, its work products, and its services.

point, it had achieved cost, schedule, scope, and performance goals through the use of critical success factors, including program staff actively engaged with stakeholders, program staff having the right knowledge and skills, agency executives engaged in the program, and streamlined and targeted governance.^{20, 21} IRS officials are also applying these critical success factors to other programs at IRS. Because of the significant progress made in addressing this high-risk area over the years, starting in fiscal year 2012, Congress did not require the submission of an annual expenditure plan.

While we are removing IRS's BSM program from the High Risk List, we will nonetheless continue to closely monitor the agency's efforts because the modernization program is complex and critical to administering and enforcing tax laws. In addition, the remaining recurring deficiencies in information security, along with new deficiencies we identified during our audit of IRS's fiscal year 2012 financial statements, merit continued and consistent commitment and attention from IRS management. Specifically, IRS will need to continue to take steps to (1) improve its testing and monitoring capabilities, (2) ensure that policies and procedures are updated, and (3) address unresolved and newly identified control deficiencies, to sustain progress in improving its information system controls and have greater assurance that financial and taxpayer data will not remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected. We currently have a mandate to perform annual reviews of IRS's major information technology programs and also perform the annual audit of IRS's annual financial statements including the effectiveness of internal controls over financial reporting systems. We plan to continue to monitor IRS's BSM program through these reviews.

²⁰GAO, *Information Technology: Critical Factors Underlying Successful Major Acquisitions*, GAO-12-7 (Washington, D.C.: Oct. 21, 2011).

²¹In quarterly status briefings to us and the Senate and House of Representatives Appropriations Committees, IRS has been reporting that the first phase of the CADE 2 program is still generally on track.

Appendix II: New High-Risk Areas

Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks

Climate change poses risks to many environmental and economic systems—including agriculture, infrastructure, ecosystems, and human health—and presents a significant financial risk to the federal government. The United States Global Change Research Program (USGCRP) has observed that the impacts and costliness of weather disasters will increase in significance as what are considered “rare” events become more common and intense due to climate change.¹ Among other impacts, climate change could threaten coastal areas with rising sea levels, alter agricultural productivity, and increase the intensity and frequency of severe weather events such as floods, drought, and hurricanes. Weather-related events have cost the nation tens of billions of dollars in damages over the past decade. For example, in 2012, the administration requested \$60.4 billion for Superstorm Sandy recovery efforts. These impacts pose significant financial risks for the federal government, which owns extensive infrastructure, insures property through federal flood and crop insurance programs, provides technical assistance to state and local governments, and provides emergency aid in response to natural disasters. However, the federal government is not well positioned to address this fiscal exposure, partly because of the complex, cross-cutting nature of the issue. Given these challenges and the nation’s precarious fiscal condition, we have added *Limiting the Federal Government’s Fiscal Exposure to Climate Change* to our 2013 list of high-risk areas.²

Climate change adaptation—defined as adjustments to natural or human systems in response to actual or expected climate change—is a risk-management strategy to help protect vulnerable sectors and communities that might be affected by changes in the climate. For example, adaptation measures may include raising river or coastal dikes to protect

¹Thomas R. Karl, Jerry M. Melillo, and Thomas C. Peterson, eds. *Global Climate Change Impacts in the United States* (Cambridge University Press: 2009). USGCRP coordinates and integrates the activities of 13 federal agencies that conduct research on changes in the global environment and their implications for society. USGCRP began as a presidential initiative in 1989 and was codified in the Global Change Research Act of 1990 [Pub. L. No. 101-606, § 103 (1990)]. USGCRP-participating agencies are the Departments of Agriculture, Commerce, Defense, Energy, Interior, Health and Human Services, State, and Transportation; U.S. Agency for International Development; Environmental Protection Agency; National Aeronautics and Space Administration; the National Science Foundation; and the Smithsonian Institution.

²The focus of this high-risk area may evolve over time to the extent that federal climate change programs and policies change.

infrastructure from sea level rise, building higher bridges, and increasing the capacity of storm water systems. Policymakers increasingly view climate change adaptation as a risk-management strategy to protect vulnerable sectors and communities that might be affected by changes in the climate, but, as we reported in 2009, the federal government's emerging adaptation activities were carried out in an ad hoc manner and were not well coordinated across federal agencies, let alone with state and local governments.³

The federal government has a number of efforts underway to decrease domestic greenhouse gas emissions, but decreasing global emissions depends in large part on cooperative international efforts. Further, according to the National Research Council (NRC) and USGCRP, greenhouse gases already in the atmosphere will continue altering the climate system for many decades. As such, the impacts of climate change can be expected to increase fiscal exposure for the federal government in many areas:

- *Federal government as property owner.* The federal government owns and operates hundreds of thousands of buildings and facilities that could be affected by a changing climate. In addition, the federal government manages about 650 million acres—29 percent of the 2.27 billion acres of U.S. land—for a wide variety of purposes, such as recreation, grazing, timber, and fish and wildlife. In 2007, we recommended that the Secretaries of Agriculture, Commerce, and the Interior develop guidance for resource managers that explains how they are expected to address the effects of climate changes, and the three departments generally agreed with the recommendation. We have ongoing work related to adapting infrastructure and the management of federal lands to a changing climate.
- *Federal insurance programs.* Two important federal insurance efforts—the National Flood Insurance Program (NFIP) and the Federal Crop Insurance Corporation—are based on conditions, priorities, and approaches that were established decades ago and do not account for climate change. NFIP has been on our High Risk List since March 2006 because of concerns about its long-term financial

³GAO, *Climate Change Adaptation: Strategic Federal Planning Could Help Government Officials Make More Informed Decisions*, GAO-10-113 (Washington, D.C.: Oct. 7, 2009).

solvency and related operational issues.⁴ In March 2007, we reported that both of these insurance programs' exposure to weather-related losses had grown substantially, and that the agencies responsible for them had done little to develop the information necessary to understand their long-term exposure to climate change.⁵ We recommended that the responsible agencies analyze the potential long-term fiscal implications of climate change and report their findings to Congress. The agencies agreed with the recommendation and contracted with experts to study their programs' long-term exposure to climate change, but the results of the work have not yet been reported to Congress. In addition, in June 2011, we reported that external factors continue to complicate the administration of NFIP and affect its financial stability.⁶ In particular, the Federal Emergency Management Agency (FEMA), which administers NFIP, has not been authorized to account for long-term erosion when updating flood maps used to set premium rates for NFIP, increasing the likelihood that premiums would not cover future losses. We suggested that Congress consider authorizing NFIP to account for long-term flood erosion in its flood maps, and the Biggert-Waters Flood Insurance Reform Act of 2012 requires FEMA to use information on topography, coastal erosion areas, changing lake levels, future changes in sea levels, and intensity of hurricanes in updating its flood maps. While these provisions respond to our suggestion to Congress, their ultimate effectiveness will depend on their implementation by FEMA. It is too early to evaluate such efforts, but we plan to examine NFIP in the near future.

- *Technical assistance to state and local governments.* The federal government invests billions of dollars annually in infrastructure projects that state and local governments prioritize and supervise. These projects have large up front capital investments and long lead

⁴The potential losses generated by NFIP have created substantial financial exposure for the federal government and U.S. taxpayers. While Congress and Federal Emergency Management Agency (FEMA) intended that NFIP be funded with premiums collected from policyholders and not with tax dollars, the program was, by design, not actuarially sound. As of November 2012, FEMA owes the Treasury approximately \$20 billion—up from \$17.8 billion pre-Sandy—and had not repaid any principal on the loan since 2010.

⁵GAO, *Climate Change: Financial Risks to Federal and Private Insurers in Coming Decades Are Potentially Significant*, GAO-07-285 (Washington, D.C.: Mar. 16, 2007).

⁶GAO, *FEMA: Action Needed to Improve Administration of the National Flood Insurance Program*, GAO-11-297 (Washington, D.C.: June 9, 2011).

times that require decisions about how to address climate change to be made well before its potential effects are discernable. We reported in October 2009 that insufficient site-specific data—such as local temperature and precipitation projections—make it hard for state and local officials to justify the current costs of adaptation efforts for potentially less certain future benefits.⁷ We recommended that the appropriate entities within the Executive Office of the President develop a strategic plan for adaptation that, among other things, identifies mechanisms to increase the capacity of federal, state, and local agencies to incorporate information about current and potential climate change impacts into government decision making. USGCRP's 2012-2021 strategic plan for climate change science, released in April 2012, recognizes this need by identifying enhanced information management and sharing as a key objective, and USGCRP is undertaking several actions designed to better coordinate that use and application of federal climate science. We have ongoing work related to these issues. In addition, gaps in satellite coverage, which could occur as soon as 2014, are expected to affect the continuity of climate and space weather measurements important to developing the information needed by state and local officials.⁸ According to National Oceanic and Atmospheric Administration program officials, a satellite data gap would result in less accurate and timely weather forecasts and warnings of extreme events—such as hurricanes, storm surges, and floods. We have concluded that the potential gap in weather satellite data is a high-risk area and added it to the High Risk List this year.

- *Disaster aid.* In the event of a major disaster, federal funding for response and recovery comes from the Disaster Relief Fund managed by FEMA and disaster aid programs of other participating federal agencies. The federal government does not budget for these costs and runs the risk of facing a large fiscal exposure at any time. We reported in September 2012 that disaster declarations have increased over recent decades to a record of 98 in fiscal year 2011 compared with 65 in 2004. Over that period, FEMA obligated over \$80

⁷GAO-10-113.

⁸See, for example, GAO, *Environmental Satellites: Focused Attention Needed to Mitigate Program Risks*, GAO-12-841T (Washington, D.C.: June 27, 2012), and *Environmental Satellites: Strategy Needed to Sustain Critical Climate and Space Weather Measurements*, GAO-10-456 (Washington, D.C.: Apr. 27, 2010).

billion in federal assistance for disasters.⁹ We found that FEMA has had difficulty implementing longstanding plans to assess national preparedness capabilities and that FEMA's indicator for determining whether to recommend that a jurisdiction receive disaster assistance does not accurately reflect the ability of state and local governments to respond to disasters.¹⁰ In September 2012, we recommended, among other things, that FEMA develop a methodology to more accurately assess a jurisdiction's capability to respond to and recover from a disaster without federal assistance. FEMA concurred with this recommendation.

The federal government would be better positioned to respond to the risks posed by climate change if federal efforts were more coordinated and directed toward common goals. In 2009, we recommended that the appropriate entities within the Executive Office of the President develop a strategic plan to guide the nation's efforts to adapt to climate change, including the establishment of clear roles, responsibilities, and working relationships among federal, state, and local governments.¹¹ Some actions have subsequently been taken, including the development of an interagency climate change adaptation task force.¹² However, a 2012 NRC report states that while the task force has convened representatives

⁹GAO, *Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own*, GAO-12-838 (Washington, D.C.: Sept. 12, 2012).

¹⁰GAO, *Managing Preparedness Grants and Assessing National Capabilities*, GAO-12-526T (Washington, D.C.: Mar. 20, 2012). See also GAO, *Disaster Response: Criteria for Developing and Validating Effective Response Plans*, GAO-10-969T (Washington, D.C.: Sept. 22, 2010).

¹¹GAO-10-113.

¹²Executive Order 13514 on Federal Leadership in Environmental, Energy, and Economic Performance calls for federal agencies to participate actively in the already existing Interagency Climate Change Adaptation Task Force. The task force, which began meeting in Spring 2009, is co-chaired by the Council on Environmental Quality, the National Oceanic and Atmospheric Administration, and the Office of Science and Technology Policy, and includes representatives from more than 20 federal agencies and executive branch offices. The task force was formed to assess key steps needed to help the federal government understand and adapt to climate change.

of relevant agencies and programs, it has no mechanisms for making or enforcing important decisions and priorities.¹³

In May 2011, we found no coherent strategic government-wide approach to climate change funding and that federal officials do not have a shared understanding of strategic government-wide priorities.¹⁴ At that time, we recommended that the appropriate entities within the Executive Office of the President clearly establish federal strategic climate change priorities, including the roles and responsibilities of the key federal entities, taking into consideration the full range of climate-related activities within the federal government. The relevant federal entities have not directly addressed this recommendation.

Federal agencies have made some progress toward better organizing across agencies, within agencies, and among different levels of government; however, the increasing fiscal exposure for the federal government calls for more comprehensive and systematic strategic planning including, but not limited to, the following:

- A government-wide strategic approach with strong leadership and the authority to manage climate change risks that encompasses the entire range of related federal activities and addresses all key elements of strategic planning.
- More information to understand and manage federal insurance programs' long-term exposure to climate change and analyze the potential impacts of an increase in the frequency or severity of weather-related events on their operations.
- A government-wide approach for providing (1) the best available climate-related data for making decisions at the state and local level and (2) assistance for translating available climate-related data into information that officials need to make decisions.

¹³NRC, Committee on a National Strategy for Advancing Climate Modeling, Board on Atmospheric Studies and Climate, Division on Earth and Life Sciences, *A National Strategy for Advancing Climate Modeling* (Washington, D.C.: 2012).

¹⁴GAO, *Climate Change: Improvements Needed to Clarify National Priorities and Better Align Them with Federal Funding Decisions*, GAO-11-317 (Washington, D.C.: May 20, 2011).

Appendix II: New High-Risk Areas

-
- Actions to address potential gaps in satellite data.
 - Improved criteria for assessing a jurisdiction's capability to respond and recover from a disaster without federal assistance, and to better apply lessons from past experience when developing disaster cost estimates.

Additional information on this area is provided on page 61 of our 2013 high risk update.¹⁵

Mitigating Gaps in Weather Satellite Data

For 2013, we are designating a new high-risk area—*Mitigating Gaps in Weather Satellite Data*. We and others—including an independent review team reporting to the Department of Commerce and the department's Inspector General—have raised concerns that problems and delays on environmental satellite acquisition programs will result in gaps in the continuity of critical satellite data used in weather forecasts and warnings. The importance of such data was recently highlighted by the advance warnings of the path, timing, and intensity of Superstorm Sandy.

Since the 1960s, the United States has used both polar-orbiting and geostationary satellites to observe the Earth and its land, oceans, atmosphere, and space environments. Polar-orbiting satellites constantly circle the Earth in an almost north-south orbit providing global coverage of environmental conditions that affect the weather and climate. As the Earth rotates beneath it, each polar-orbiting satellite views the entire Earth's surface twice a day. In contrast, geostationary satellites maintain a fixed position relative to the Earth from a high-level orbit of about 22,300 miles in space. Used in combination with ground, sea, and airborne observing systems, both types of satellites have become an indispensable part of monitoring and forecasting weather and climate. For example, polar-orbiting satellites provide the data that go into numerical weather prediction models, which are a primary tool for forecasting weather days in advance, including forecasting the path and intensity of hurricanes and tropical storms. Geostationary satellites provide frequently-updated graphical images that are used to identify current weather patterns and provide short-term warnings.

¹⁵GAO-13-283.

Polar-orbiting Satellites

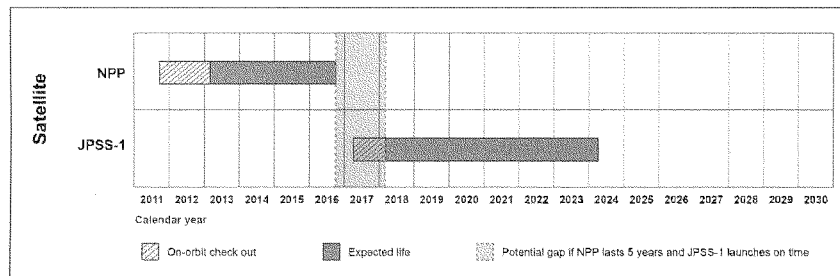
For more than 40 years, the United States has operated two separate operational polar-orbiting meteorological satellites systems: the Polar-orbiting Operational Environmental Satellite series, which is managed by National Oceanic and Atmospheric Administration (NOAA)—a component of the Department of Commerce; and the Defense Meteorological Satellite Program (DMSP), which is managed by the Air Force. The government also relies on data from a European satellite program, called the Meteorological Operational (MetOp) satellite series. These satellites are positioned so that they cross the Equator in the early morning, midmorning, and early afternoon in order to obtain regular updates throughout the day.

With the expectation that combining the two separate U.S. polar satellite programs would result in sizable cost savings, a May 1994 Presidential Decision Directive required NOAA and DOD to converge the two programs into a single new satellite acquisition, which became the National Polar-orbiting Operational Environmental Satellite System (NPOESS). However, in the years that followed, NPOESS encountered significant technical challenges in sensor development and experienced program cost growth and schedule delays, in part due to problems in the program's management structure. After several restructurings and recurring challenges, in February 2010, the Executive Office of the President's Office of Science and Technology Policy announced that NOAA and DOD would no longer jointly procure NPOESS; instead, each agency would plan and acquire its own satellite system. Specifically, NOAA, with support from the National Aeronautics and Space Administration (NASA), would be responsible for the afternoon orbit, and DOD would be responsible for the early morning orbit. The U.S. partnership with the European satellite agency for data from the midmorning orbit would continue as planned.

Subsequently, NOAA initiated its replacement program, the Joint Polar Satellite System (JPSS). JPSS consists of a demonstration satellite—called the Suomi National Polar-orbiting Partnership (NPP)—launched in October 2011; two satellites, with at least five instruments planned for each, to be launched by March 2017 and December 2022, respectively; two stand-alone satellites to accommodate three additional instruments; and ground systems for the entire program. The program is currently estimated to cost \$12.9 billion. In June 2012, we reported that NOAA and NASA made progress in establishing the JPSS program and in launching and operating the demonstration satellite, but noted that program officials expect there to be a gap in satellite observations before the first JPSS satellite is launched.

Specifically, NOAA officials anticipate a gap in the afternoon orbit from 18 to 24 months between the time that NPP reaches the end of its lifespan and when the first JPSS satellite is fully ready for operational use. We identified other scenarios where the gap could last from 17 to 53 months. For example, the gap would be 17 months if NPP lasts 5 years until October 2016 and JPSS is launched as planned in March 2017 and undergoes a 12-month on-orbit checkout before it is fully operational. Alternatively, if NPP lasts only 3 years—which NASA engineers consider possible due to poor workmanship in the fabrication of the instruments—and JPSS launches 1 year later than currently planned, the gap in satellite observations could reach 53 months. Figure 1 depicts a potential gap in the afternoon orbit.

Figure 1: A Potential Gap in the Afternoon Orbit



Source: GAO analysis of NOAA data.

After NPOESS was disbanded, DOD also began planning its own follow-on polar satellite program. However, it halted work in early 2012 because it still has two legacy DMSP satellites in storage that will be launched as needed to maintain observations in the early morning orbit. The agency currently plans to launch its two remaining satellites in 2014 and 2020. Moreover, DOD is working to identify alternatives to meet its future environmental satellite requirements. However, in June 2012, we reported that there is a possibility of satellite data gaps in DOD's early morning orbit. The two remaining DMSP satellites may not work as intended because they were built in the late 1990s and will be quite old by the time they are launched. If the satellites do not perform as expected, a data gap in the early morning orbit could occur as early as 2014.

Satellite data gaps in the morning or afternoon polar orbits would lead to less accurate and timely weather forecasting; as a result, advanced warning of extreme events would be affected. Such extreme events could include hurricanes, storm surges, and floods. For example, the National Weather Service performed case studies to demonstrate how its forecasts would have been affected if there were no polar satellite data in the afternoon orbit, and noted that its forecasts for the "Snowmageddon" winter storm that hit the Mid-Atlantic coast in February 2010 would have predicted a less intense storm further east, with about half of the precipitation at 3, 4, and 5 days before the event. Specifically, the models would have under-forecasted the amount of snow by at least 10 inches. Similarly, a European weather organization¹⁶ recently reported that NOAA's forecasts of Superstorm Sandy's track could have been hundreds of miles off without polar-orbiting satellites—rather than identifying the New Jersey landfall within 30 miles 4 days before landfall, the models would have shown the storm remaining at sea.

In June 2012, we reported that while NOAA officials communicated publicly and often about the risk of a polar satellite data gap, the agency had not established plans to mitigate the gap. At the time, NOAA officials stated that the agency would continue to use existing satellites as long as they provide data and that there were no viable alternatives to the JPSS program. However, our report noted that a more comprehensive mitigation plan was essential since it is possible that other governmental, commercial, or foreign satellites could supplement the polar satellite data. For example, other nations continue to launch polar-orbiting weather satellites to acquire data such as sea surface temperatures, sea surface winds, and water vapor. Also, over the next few years, NASA plans to launch satellites that will collect information on precipitation and soil moisture. Because it could take time to adapt ground systems to receive, process, and disseminate an alternative satellite's data, we noted that any delays in establishing mitigation plans could leave the agency little time to leverage its alternatives. We recommended that NOAA establish mitigation plans for pending satellite gaps in the afternoon orbit as well as potential gaps in the early morning orbit.

¹⁶The European Centre for Medium Range Weather Forecasts is an independent, intergovernmental organization supported by 34 European nations, providing global medium-to-extended range forecasts.

In September 2012, the Under Secretary of Commerce for Oceans and Atmosphere (who is also the NOAA Administrator) reported that NOAA had several actions under way to address polar satellite data gaps, including (1) an investigation on how to maximize the life of the demonstration satellite, (2) an investigation on how to accelerate the development of the second JPSS satellite, and (3) the development of a mitigation plan to address potential data gaps until the first JPSS satellite becomes operational. The Under Secretary also directed NOAA's Assistant Secretary to, by mid-October 2012, establish a contract to conduct an enterprise-wide examination of contingency options and to develop a written, descriptive, end-to-end plan that considers the entire flow of data from possible alternative sensors through data assimilation and on to forecast model performance. In October 2012, NOAA issued a mitigation plan for a potential 14 to 18 month gap in the afternoon orbit, between the current polar satellite and the first JPSS satellite. The plan identifies and prioritizes options for obtaining critical observations, including alternative satellite data sources and improvements to data assimilation in models. It also lists technical, programmatic, and management steps needed to implement these options.

However, these plans are only the beginning. The agency must make difficult decisions on which steps it will implement to ensure that its mitigation plans are viable when needed. For example, NOAA must make decisions about (1) whether and how to extend support for legacy satellite systems so that their data might be available if needed, (2) how much time and resources to invest in improving satellite models so that they assimilate data from alternative sources, (3) whether to pursue international agreements for access to additional satellite systems and how best to resolve any security issues with the foreign data, (4) when and how to test the value and integration of alternative data sources, and (5) how these preliminary mitigation plans will be integrated with the agency's broader end-to-end plans for sustaining weather forecasting capabilities. NOAA must also identify time frames for when these decisions will be made. We have ongoing work assessing NOAA's efforts to limit and mitigate potential polar satellite data gaps.

Geostationary Satellites

Geostationary environmental satellites transmit frequently updated images of the weather currently affecting the United States to every national weather forecast office in the country. These are the satellite images that the public often sees on television news programs. NOAA plans to have its \$10.9 billion Geostationary Operational Environmental Satellite-R (GOES-R) series replace the current fleet of geostationary satellites, which will begin to reach the end of their useful lives in 2015.

The GOES-R program has undergone a series of changes since 2006 and now consists of four geostationary satellites and a ground system. However, problems with instrument and ground system development caused a 19-month delay in completing the program's preliminary design review, which occurred in February 2012. In June 2012, we reported that GOES-R schedules were not fully reliable and that they could contribute to delays in satellite launch dates. Program officials acknowledged that the likelihood of meeting the October 2015 launch date was 48 percent.

While NOAA's policy is to have two operational satellites and one backup satellite in orbit at all times, continued delays in the launch of the first GOES-R satellite could lead to a gap in satellite coverage. This policy proved useful in December 2008 and again in September 2012 when the agency experienced problems with one of its operational satellites, but was able to move its backup satellite into place until the problems were resolved. However, beginning in April 2015, NOAA expects to have only two operational satellites and no backup satellite in orbit until GOES-R is launched and completes an estimated 6-month post-launch test period. As a result, there could be a year or more gap during which time a backup satellite would not be available. If NOAA were to experience a problem with either of its operational satellites before GOES-R is in orbit and operational, it would need to rely on older satellites that are beyond their expected operational lives and may not be fully functional. Any further delays in the launch of the first satellite in the GOES-R program would likely increase the risk of a gap in satellite coverage.

In September 2010, we reported that NOAA had not established adequate continuity plans for its geostationary satellites. Specifically, in the event of a satellite failure, with no backup available, NOAA planned to reduce its operations to a single satellite and if available, rely on a satellite from a foreign nation. However, the agency did not have plans that included processes, procedures, and resources needed to transition to a single or foreign satellite. Without such plans, there would be an increased risk that users would lose access to critical data. We recommended that NOAA develop and document continuity plans for the operation of geostationary satellites that included implementation procedures, resources, staff roles, and timetables needed to transition to a single satellite, foreign satellite, or other solution. In September 2011, NOAA developed an initial continuity plan that generally includes these elements. Specifically, NOAA's plan identified steps it would take in transitioning to a single or foreign satellite; the amount of time this transition would take; roles of product area leads; and resources such as imaging product schedules, disk imagery frequency, and staff to execute

the changes. In December 2012, NOAA issued an updated plan that provides additional contingency scenarios.

However, it is not evident that critical steps have been implemented, including simulating continuity situations and working with the user community to account for differences in various continuity scenarios. These steps are critical for NOAA to move forward in documenting the processes it will take to implement its contingency plans. Once these activities are completed, NOAA should update its contingency plan to provide more details on its contingency scenarios, associated time frames, and any preventative actions it is taking to minimize the possibility of a gap. We have ongoing work assessing NOAA's actions to ensure that its plans are viable and that continuity procedures are in place and have been tested.

Additional information on this area is provided on page 155 of our 2013 high risk update.¹⁷

¹⁷GAO-13-283.

Appendix III: Narrowing High-Risk Areas

Management of Federal Oil and Gas Resources

Progress has been made in one of the three areas we identified in our 2011 High Risk List—the Department of the Interior's (Interior) reorganization of its oversight of offshore oil and gas activities.

- *Reorganization.* In October 2011, following the transfer of the Minerals Management Service's oil and gas revenue collection functions to the newly created Office of Natural Resources Revenue, Interior established two new bureaus to provide oversight of offshore resources and operational compliance with environmental and safety requirements. The new Bureau of Ocean Energy Management (BOEM) is responsible for leasing and approval of offshore development plans while the new Bureau of Safety and Environmental Enforcement (BSEE) is responsible for lease operations, safety, and enforcement. Because the responsibilities of these two bureaus are closely interconnected and depend on effective coordination, Interior developed memoranda and standard operating procedures to define roles and responsibilities and facilitate and formalize coordination. Interior also enacted numerous policy changes intended to improve its oversight of offshore oil and gas activities, such as new requirements and policies designed to mitigate the risk of a subsea well blowout or spill. In July 2012, we concluded that Interior has fundamentally completed its reorganization of its oversight of offshore oil and gas activities.

In ongoing and future reviews, our primary focus will be to assess Interior's remaining challenges to managing oil and gas resources—revenue collection and human capital. In so doing, we will also continue to consider Interior's reorganization and its effect on the agency's ability to oversee federal lands and waters.

- *Revenue collection.* In 2008, we reported that Interior collected lower levels of revenues for oil and gas production than all but 11 of 104 oil and gas resource owners whose revenue collection systems were evaluated in a comprehensive industry study—these resource owners included many other countries as well as some states. We recommended that Interior (1) undertake a comprehensive reassessment of its revenue collection policies and processes and (2) establish a balance between collecting revenues and ensuring that public lands and waters remain an attractive option for oil and gas development. In response to our recommendation, Interior contracted for a study called "Comparative Assessment of the Federal Oil and Gas Fiscal System" with the goal to inform decisions about federal lease terms, such as royalties, by consistently comparing the federal oil and gas fiscal systems with those of other countries and identifying

ways to increase revenues and improve diligent development. Interior completed this study in October 2011 but Interior is still in the process of deciding if and how to use the results of the study to alter its lease terms. In addition, Interior continues to work to implement a number of our recommendations directed at improving Interior's ability to conduct oil and gas production verification inspections. Finally, Interior is working to implement our recommendations to correct numerous problems with its efforts to collect data on oil and gas produced on federal lands, including missing data, errors in company-reported data on oil and gas production, sales data that did not reflect prevailing market prices for oil and gas, and a lack of controls over changes to the data that companies reported. We are currently engaged in a review of Interior's revenue collection practices that will evaluate, among other things, Interior's progress in addressing our recommendations.

- *Human capital.* We have reported that the bureaus responsible for oversight and management of federal oil and gas resources on federal lands and in federal waters—Bureau of Land Management (BLM) and the Minerals Management Service (the predecessor to BOEM and BSEE)—have encountered persistent problems in hiring, training, and retaining staff. For example, in 2010, we found that both BLM and the Minerals Management Service experienced high turnover rates in key oil and gas inspection and engineering positions, potentially affecting their oversight of oil and gas development on federal leases. For fiscal years 2012 and 2013, Congress provided funds to BOEM and BSEE in the Gulf of Mexico to establish higher minimum rates of pay for key positions—chiefly geophysicists, geologists, and petroleum engineers—for up to 25 percent of the usual minimum rate of pay. BOEM and BSEE officials in the Gulf of Mexico told us that the pay increase reduced attrition rates for these positions. However, it is uncertain how Interior will address staffing shortfalls to oversee offshore resources in the long term. In July 2012, we reported that Interior was creating a new training program for its inspection staff (such as BSEE's National Offshore Training Program to train inspectors and engineers), but that it may take up to 2 years before new inspection staff are fully trained. Further, human capital issues also exist at BLM and the management of onshore oil and gas. For example, BLM faces similar challenges in hiring, training, and retaining staff for key positions but Interior has not received congressional approval or funds to establish higher minimum rates of pay for these positions as did BOEM and BSEE. We are currently engaged in a review of Interior's efforts to meet its human capital challenges. As part of this effort, we will focus on the causes of

Appendix III: Narrowing High-Risk Areas

Interior's human capital challenges, actions taken, and how Interior plans to measure the effectiveness of corrective actions.

Additional information on this area is provided on page 76 of our 2013 high risk update.¹

DOE's Contract Management for the National Nuclear Security Administration and Office of Environmental Management.

To recognize progress at the Department of Energy (DOE) on the National Nuclear Security Administration's (NNSA) and Office of Environmental Management's (EM) execution of nonmajor projects—projects with values of less than \$750 million—we are shifting the focus of its high-risk designation to major contracts and projects executed by NNSA and EM, those contracts and projects with values of \$750 million or greater. Two of our reviews completed in 2012 focused on nonmajor projects found that these projects were being completed in large part, although additional and sustained attention by DOE is needed to adequately set and document performance baselines and further demonstrate that these actions result in improved performance. These reports included recommendations to DOE to clearly define, document, and track the scope, cost, and completion date targets for each of its projects, as required by DOE's project management order. DOE agreed with these recommendations and plans to apply lessons learned from successful EM projects to its broader portfolio of projects and activities. With further monitoring of this area to ensure that progress is sustained, coupled with continued efforts and commitment by top leadership to address contract and project management weaknesses, nonmajor project performance issues will have been sufficiently addressed.

DOE continues to demonstrate strong commitment and top leadership support for improving contract and project management in EM and NNSA, building on its corrective action plan developed in 2008. In December 2010, the Deputy Secretary convened a DOE Contract and Project Management Summit to discuss strategies for additional improvement in contract and project management. The participants identified six barriers to improved performance and reported in April 2012 on the status of initiatives to address these barriers. In addition, DOE has continued to release guides for implementing its revised order for Program and Project Management for the Acquisition of Capital Assets (DOE O 413.3B), such as for cost

¹GAO-13-283.

estimating, using earned value management, and for forming project teams. Further, DOE has taken steps to enhance project management and oversight by requiring peer reviews and independent cost estimates for projects with values over \$100 million and by improving the accuracy and consistency of data in DOE's central repository for project data.

Challenges remain for the successful execution of major projects. NNSA and EM are currently managing 10 major projects with combined estimated costs totaling as much as \$65.7 billion. We have continued to document significant cost increases and schedule delays as well as technical challenges impacting project design. NNSA is tasked with modernizing the nation's aging nuclear weapons production facilities, a challenging effort that will take years and cost billions of dollars. EM faces ongoing complex and long-term challenges in removing radioactive and hazardous chemical contaminants—left over from decades of weapons production—from soil, groundwater, and facilities. Billions of dollars have already been spent, and will continue to be spent over the coming decades to treat and dispose of this waste. In recognition of the significance of these challenges, particularly in a time of fiscal constraint, in 2012, multiple committees of the Senate and House of Representatives held oversight hearings focused on needed improvements to DOE contract management and project performance. Further, the *National Defense Authorization Act for Fiscal Year 2013* includes provisions significant to considerations about NNSA contract and project management, such as cost containment provisions for two of NNSA's largest construction projects, both of which have experienced cost and schedule delays; a requirement that NNSA submit to Congress reports including expected cost savings associated with the award of contracts to manage and operate NNSA facilities; and creation of an advisory panel to make recommendations on revising the governance of the nuclear security enterprise. Until DOE can consistently demonstrate that recent changes to policies and processes are resulting in improved performance on major projects, NNSA and EM will remain on the High Risk List.

Additional information on this area is provided on page 218 of our 2013 high risk update.²

²GAO-13-283.



Testimony of
Deputy Secretary Jane Holl Lute
U.S. Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
March 21, 2013

Introduction

Good morning Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the progress the Department of Homeland Security (DHS) has made since its creation in 2003 and the challenges that confront the Department. Specifically, I will focus on the Department's success in implementing the recommendations of the Government Accountability Office's (GAO) biennial High Risk Series Update and the work we must undertake in order to more efficiently secure the safety of our Nation's citizens.

As we approach the ten-year anniversary of DHS operations, our Nation is more secure than it was ten years ago. We have progressed on every front, using the lessons of experience to become more resilient to terrorist attacks as well as to threats and hazards of all kinds.

The DHS mission is clear: create a safe, secure, and resilient place where the American way of life can thrive. In order to meet that mission, DHS must do the following:

- Prevent terrorism and enhance security;
- Secure and manage our borders;
- Enforce and administer our immigration laws;
- Safeguard and secure cyberspace; and
- Ensure resilience to disasters.

We do not do this alone. While DHS plays a central role in the effort to ensure the safety of our Nation, we rely heavily on our partners in homeland security, including our partners at the Federal level; our state, local, tribal and territorial governmental partners; non-governmental organizations like faith-based, and non-profit groups and private sector industry; and most importantly, individuals, families, and communities, who continue to be our greatest assets and the key to our success. Together we form the homeland security enterprise and through continued partnership, we leverage our shared capabilities to secure America.

DHS's Relationship with the GAO

We take our responsibilities to Congress very seriously. The GAO, an arm of Congress, is one of our essential partners. In many cases, GAO audits, investigations, and reports borne out of congressional guidance provide solid recommendations on improving management and operations at DHS. Indeed, the Department and Components tend to agree with many GAO recommendations, and work diligently to close out recommendations that provide the Department with a clear understanding of the requirements necessary for full implementation.

Both DHS and GAO have benefitted from the open line of communication we have put in place over the past four years. The culture of engagement, responsiveness, and mutual respect is the result of hard work on the part of both agencies. Today I am proud to say that our relationship with GAO has never been better.

Maintaining and improving this important relationship requires ongoing efforts to ensure that we continue to make progress. For that reason, DHS and GAO senior leaders meet at least quarterly to ensure continued progress and to address emerging issues.

Since we began meeting regularly, the number of open GAO recommendations for DHS has steadily decreased as the Department has successfully addressed and closed out more recommendations. During 2011 and 2012, GAO issued a total of 327 recommendations, and DHS closed 654 recommendations (including some from prior years). We will continue to work with GAO to close out the many recommendations we believe DHS has already implemented, including several referenced in the latest GAO High Risk Series Update. The Department is grateful for the level of coordination and professionalism displayed in our work together.

GAO's biennial High Risk Series Update provides an important opportunity to evaluate just how far we have come as a Department and how far we have yet to go. We have worked hard to demonstrate sustained improvement on the areas of greatest concern to Congress and are proud of the progress we have made since the issuance of the last High Risk Series Update. In its most recent High Risk Series Update, GAO lists the following four areas in which DHS is the lead Federal agency:

- Strengthening Department of Homeland Security Management Functions;
- Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland;
- Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures; and
- National Flood Insurance Program.

While we work with and support other Federal agencies on items included in the High Risk Series Update, my testimony today will focus on the progress we have made in these key areas, and the work that remains.

Strengthening Department of Homeland Security Management Functions

The creation of DHS presented a series of enormous challenges, many of which were described in the GAO High Risk area added in 2003: "Implementing and Transforming DHS." We appreciate GAO's acknowledgement of the significant improvement DHS has made, by narrowing the High Risk area this year, from "Implementing and Transforming DHS" to "Strengthening DHS Management Functions."

The refocusing by GAO of this High Risk category is a reflection of the Management Directorate's efforts to systematically address serious concerns raised by Members of Congress. In September 2010, GAO identified 31 recommended actions for DHS to address in order to be considered for removal from its High Risk List in the areas of management integration, financial management, Information Technology, human capital, and acquisitions program management. In January 2011, DHS created and issued the *Integrated Strategy for High Risk Management*, a comprehensive operational framework composed of 18 specific initiatives with detailed

corrective action plans for several critical management functions to address GAO's recommended actions. Since then, DHS has provided GAO with thorough periodic updates documenting the progress it is making in implementing these recommended actions. Over the past two years, the Department has made substantial progress in implementing the 18 initiatives, which should result in the systematic closure of each of GAO's 31 outcomes. The most recent update, given to GAO in September 2012, covered the status of the 18 specific initiatives, on areas such as workforce strategy, IT program governance, strategic sourcing, and business intelligence. DHS remains committed to sustaining this growing momentum over the coming years, and will continue to implement the *Integrated Strategy for High Risk Management* and regularly track the progress of the initiatives using quarterly internal progress reviews.

The High Risk Series Update mentions several areas of improvement, including acknowledgement of the considerable progress made in the area of management integration. Examples include strengthening the delegations of authority to clarify the roles between Headquarters and Components; improving the quality and integrity of financial statements; implementing the framework for Integrated Investment Life Cycle Management (IILCM) to ensure that the total budget (\$59.8 billion in Fiscal Year 2012) is spent wisely and efficiently; and enhancing oversight responsibility for acquisition programs and investment support to DHS's Office of Program Accountability and Risk Management.

GAO's report also mentions the need to make progress in key management areas, including acquisitions, IT, financial management, human capital, and management integration. DHS agrees, issuing the *Integrated Strategy for High Risk Management* for exactly this reason, and the results are starting to demonstrate clear success. Over the next year, DHS expects to continue to build upon this progress. Specifically, DHS plans to:

- Enhance IT infrastructure by continuing to consolidate systems within DHS data centers and minimize paperwork and reporting burdens on the public;
- Continue establishing public and private cloud services to facilitate access to mission-enabling enterprise services;
- Execute the Department's Diversity and Inclusion Strategy;
- Consolidate Human Resource Information Technology efforts, including rolling out a Personnel Accountability System;
- Lead activities to increase employee engagement, morale, and leadership development;
- Continue developing a centralized business intelligence solution that will provide management information across organizational boundaries and from disparate systems to support informed decision making by Department leadership;
- Continue to improve governance through coordinated program reviews to reduce redundancies and support the Department's integrated investment management efforts;
- Develop a sustainment plan to maintain a clean audit opinion and strengthen internal controls.

I would also like to briefly mention a few accomplishments and initiatives that DHS has undertaken to address some of the areas mentioned by GAO.

Audit Opinion

In 2012, DHS earned a qualified audit opinion on all FY 2012 financial statements, a first for the Department. This full-scope audit opinion is a result of DHS's ongoing commitment to instituting sound financial management practices to safeguard taxpayer dollars. DHS also provided qualified assurance of the effectiveness of internal controls over financial reporting for the first time in its history. These efforts represent significant progress in prudent financial management.

Enhancing Acquisition Management

Over the past four years, the Under Secretary for Management led an effort to improve the Department's overall acquisition process, including reforming the early requirements development process and enhancing our ability to manage the implementation and execution of acquisition programs. As a part of these enhancements, DHS appointed Component Acquisition Executives in all Components and developed a Decision Support Tool to reduce risk and improve program performance by actively supporting programs throughout their lifecycle. The Office of the Inspector General recently acknowledged these efforts in noting that DHS has significantly strengthened its acquisition management oversight.

Small Business Contracting

DHS continues to support small businesses around the country. Since FY 2009, the Small Business Administration has evaluated agencies based on small business prime contracting, small business subcontracting, and a written progress plan. DHS has consistently received a grade of A.

Data Center Consolidation

DHS is strategically consolidating data centers to drive IT efficiencies. To date, 16 primary data centers have been consolidated, with an additional six consolidations scheduled for completion in FY 2013. At current funding, DHS expects to realize savings by FY 2020, with an anticipated overall cost avoidance of \$2.8 billion by FY 2030.

Promoting Efficient Operations

Since the beginning of the Administration, DHS made an unprecedented commitment to efficiency to support our frontline operations by building a culture of fiscal discipline and accountability. Through the Efficiency Review and Component initiatives, DHS has identified more than \$4 billion in cost avoidances and implemented more than 45 efficiency initiatives across the Department.

Overall, the *Integrated Strategy for High Risk Management* allows DHS to realize greater efficiencies through good management practices while also addressing the GAO High Risk designation. DHS remains committed to demonstrating measurable, sustained progress over the

coming years so that all management functions can be eligible for removal from the High Risk List.

While DHS is extremely proud of its management transformation efforts, we know that we must continue to be vigilant, and our work is not done. We appreciate GAO's partnership in our efforts. To ensure that future discussions on DHS management are as productive as possible, we should agree upon a clear definition and timeline for what constitutes sustainable and measurable progress in key management areas. Working through the *Integrated Strategy for High Risk Management*, we look forward to continuing our dialogue with GAO.

Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland

While we have made important progress in securing our Nation since the tragic attacks on September 11, 2001, we continue to face persistent and evolving threats. Ensuring all of those who protect the Homeland have and share the necessary information to execute our missions, while safeguarding individual privacy and civil liberties, is critical. For that reason, we have worked diligently with our homeland security partners to build a new architecture for information sharing. The four essential elements of the distributed homeland security architecture – The National Network of Fusion Centers, the Nationwide Suspicious Activity Reporting Initiative, the National Terrorism Advisory System, and the “If You See Something, Say Something” campaign – each learn from and build upon one another. These four elements require the engagement of the extended homeland security enterprise.

Fusion Centers

DHS works closely with state and local governments to support 78 state and major urban area fusion centers through personnel, training, technical assistance, exercise support, security clearances, and connectivity to Federal systems, technology, and grant funding. These state and locally owned and operated centers have become the nexus of the Federal Government's day to day information sharing efforts with state and local partners. DHS also has provided considerable resources and training to these fusion centers to support privacy and civil liberties.

Nationwide Suspicious Activity Reporting Initiative

Through the Nationwide Suspicious Activity Reporting Initiative, which is conducted in partnership with the Department of Justice, DHS works to train state and local law enforcement and homeland security partners to recognize behaviors and indicators potentially related to terrorism and terrorism-related crime; standardize how those observations are documented and analyzed; and share those reports with fusion centers and Joint Terrorism Task Forces for further analysis and investigation. Over the past four years, more than 234,000 law enforcement officers have received training under this initiative. DHS has also expanded the Nationwide Suspicious Activity Reporting Initiative to include the Nation's 16 critical infrastructure sectors.

National Terrorism Advisory System (NTAS)

In April 2011, DHS replaced the former color-coded alert system with the NTAS, which provides timely, detailed information to the public and the private sector, as well as to state, local, tribal, and territorial governments about credible terrorist threats and recommended security measures. NTAS alerts will be issued in addition to the regular intelligence and information bulletins that DHS shares with law enforcement.

“If You See Something, Say Something™”

Through the nationwide expansion of the “If You See Something, Say Something™” campaign, DHS encourages Americans to alert local law enforcement if they see something potentially suspicious. The campaign has been launched with a variety of partners, including numerous sports teams and leagues, transportation agencies, private sector partners, states, municipalities, and colleges and universities. DHS has also produced “If You See Something, Say Something™” Public Service Announcements, which have been distributed to television and radio stations across the country.

DHS’s “Information Sharing and Safeguarding Strategy”

In January 2005, GAO designated terrorism-related information sharing as high risk. Since then, GAO has monitored Federal efforts to implement the Federal Information Sharing Environment (Federal ISE). The Federal ISE serves as an overarching solution to strengthening the sharing of intelligence, terrorism, law enforcement, and other information among public and private sector partners. DHS also consults with law enforcement officials from across the country to tailor the Department’s products and briefings to better support state and local law enforcement and homeland security officials.

DHS’s *Information Sharing and Safeguarding Strategy*, issued in January 2013, sets forth the Department’s information sharing and safeguarding direction and priorities for the homeland security enterprise. It outlines goals and objectives that guide the activities of participants in the homeland security enterprise towards a common information sharing and safeguarding end within the context of our distributed homeland security architecture. Our success in gauging our performance will allow us to make decisions that are more informed during the implementation phase. This document also supports the policy positions set forth by the White House in the *National Strategy for Information Sharing* (2007), as well as the *National Strategy for Information Sharing and Safeguarding* (2012), and presents how the Department will enable its missions through sharing and safeguarding information.

DHS has made progress in both its contributions to the Federal ISE as well as executing its own information-sharing and safeguarding mission. In September 2012, GAO found that DHS has demonstrated leadership in sharing terrorism-related information to protect the homeland through its establishment and operation of the Information Sharing and Safeguarding Governance Board (ISSGB), which serves as the decision-making body for DHS information sharing and safeguarding issues. The ISSGB has enhanced collaboration among DHS Components by

identifying key information-sharing initiatives, while developing and documenting a process to prioritize initiatives for additional oversight and support.

DHS plans to address all of GAO's recommendations in our *FY 2013-2017 DHS Information Sharing and Safeguarding Strategy* ("DHS Strategy") and *Fiscal Years 2013-2017 Information Sharing and Safeguarding Implementation Plan* ("Implementation Plan"). The *DHS Strategy* and *Implementation Plan* will focus on 16 priority objectives, including a gap analysis as well as key activities and milestones to address the identified gaps. The *DHS Strategy* calls for indicators and measures that (1) assess accomplishments; (2) facilitate decision making; (3) hold DHS leaders accountable; and (4) allow the homeland security enterprise to continuously improve. Those measures will be used in the development and execution of the *Implementation Plan*. The *Implementation Plan* will allow the ISSGB to support the Department's investments in information-sharing solutions to reduce risks most effectively. DHS will update its current *Information Sharing and Safeguarding Roadmap* ("Roadmap") as well as the *Roadmap Implementation Guide* ("Guide") to track the implementation of the 16 priority objectives. The revised *Guide* and updates will also provide the Department with an institutional record to sustain ongoing implementation efforts that improve information sharing. DHS expects to develop the *Implementation Plan*, update the *Roadmap*, and revise the *Guide* by the summer of 2013.

DHS, working closely with the Federal Bureau of Investigation (FBI) and other Federal partners, has re-focused its information sharing and production efforts to better address the needs of state and local governments and private-sector partners. DHS consults with law enforcement officials from major metropolitan areas, fusion center directors, and state Homeland Security Advisors to tailor the Department's products and briefings to better support state and local law enforcement and homeland security officials.

Consistent with the direction the President has set for a robust information-sharing environment, DHS provides, in coordination with the FBI and other Federal partners, regular training programs for local law enforcement and homeland security officials to help them identify indicators of terrorist activity. In addition, DHS continues to improve and expand the information-sharing mechanisms by which front line personnel are made aware of the threat picture, vulnerabilities, and what it means for their local communities.

Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures

Cybersecurity is one of DHS's five critical missions because it is impossible to imagine a safe, secure, and resilient place where our way of life can thrive without a safe, secure, and resilient cyberspace. At the heart of securing cyberspace are two challenges, which constitute the irreducible minimum with which we must be concerned: protecting our critical infrastructure today and building a stronger cyber ecosystem for tomorrow.

DHS continues to advance its cyber analysis and warning capabilities, building its capacity to protect the Federal .gov space, and strengthening public-private partnerships and appropriate

information sharing. The United States Computer Emergency Readiness Team (US-CERT) receives and analyzes incident reports from public and private organizations, a majority of which come from outside of the Federal Government. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides similar analysis of incidents affecting critical infrastructure systems.

DHS's Science and Technology Directorate (S&T) is leading efforts to secure two of the Nation's major technology vulnerabilities: security weaknesses in the Internet's domain name system (DNS), and vulnerabilities in the Internet routing system. Both DNS and routing vulnerabilities can deny service to small or large portions of the Internet, make tracking and tracing Internet communications very difficult, or allow communications to be redirected without the user's knowledge. By working in a collaborative effort across Federal agencies, private industry, and global Internet owners and operators, S&T, in cooperation with the National Institute on Standards and Technology (NIST) and the Department of Commerce, leads the effort to deploy domain name security extensions, and we work with international counterparts and key technical groups to develop improvements to the standards that govern addressing and routing.

To build the stronger cyber ecosystem for tomorrow, we need to educate young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts. There is a shortage today of technically skilled people required to manage and protect network infrastructure. DHS S&T provides funding to support the National Initiative on Cyber Education (NICE) through the development and execution of cybersecurity competitions. Competitions provide a unique venue to attract talented students to a career in cybersecurity, and provide them with practical, hands-on experience in a realistic setting. In FY 2012, we saw over 1,500 students from 131 colleges and universities participate in the Collegiate Cyber Defense Competitions. Additionally, the U.S. Cyber Challenge had over 1,000 high school student participants.

Securing Federal Civilian Networks

DHS is responsible for securing unclassified Federal civilian government networks. To protect Federal civilian agency networks, DHS is deploying technology to detect and block cyber intrusions with support from the Department of Defense. In addition, DHS is responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the Government.

More than 80 percent of the time, exploits target known vulnerabilities on networks, computers, and commercial software. Until recently, most agencies did not routinely check their systems for those vulnerabilities. DHS is now deploying proven diagnostic technology across the .gov realm to automate scanning government networks every three days, enabling agencies to identify and repair the worst problems first on their networks and commercial software. This automated, Continuous Diagnostics and Mitigation (CDM) program will replace costly and infrequent manual inspections of systems.

The National Cybersecurity Protection System, also referred to as EINSTEIN, is an integrated intrusion detection, analytics, information sharing, and intrusion prevention system that uses

hardware, software, and other components to support DHS's cybersecurity responsibilities. Intrusion detection and cyber analytics capabilities are now installed at all Federal departments, allowing a more agile response to cyber threats. Additionally, the intrusion prevention service, known as E³A, will reach initial operating capability this year, preventing known unauthorized intrusions into Federal networks. Together, these efforts will ensure that Federal cybersecurity capabilities are efficiently keeping pace with cutting-edge technologies and adapting to emerging threats.

Inter-Governmental Partnerships to Secure Networks

DHS builds partnerships with non-Federal public sector stakeholders as well to protect critical network systems. The Multi-State Information Sharing and Analysis Center (MS-ISAC) opened its Cyber Security Operations Center in November 2010, which has enhanced NCCIC situational awareness at the state and local government level and allows the Federal Government to quickly and efficiently provide critical cyber threat, vulnerability, and mitigation data to state and local governments. Since 2010, MS-ISAC has grown to include all 50 states, three U.S. territories, the District of Columbia, and more than 200 local governments.

Partnership with the Private Sector

The DHS cybersecurity approach reflects the need for ongoing collaboration at all levels of government and with the private sector. DHS works with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks by sharing actionable cyber threat information with our private sector partners, helping companies to identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident.

DHS's US-CERT responds to more than 100,000 incident reports each year, including multi-agency response activities for cyber incidents such as those at NASDAQ and RSA. In addition, ICS-CERT provides industry stakeholders with situational awareness and analytical support to manage risks to their computers and networks. Since it was established in 2009, ICS-CERT has deployed 20 teams to respond to significant private sector cyber incidents involving control system entities. DHS also works to empower owners and operators by providing a cyber self-evaluation tool, as well as in-person and online training sessions.

Executive Order and Presidential Policy Directive on Cybersecurity

The February 2013 Executive Order 13636 on Improving Critical Infrastructure Cybersecurity and the Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience also articulate a whole-of-government approach to critical infrastructure cybersecurity. These documents reinforce the need for everyone to play their parts in protecting the cyber and physical security of our critical infrastructure. Implementation efforts will drive action toward system and network security and resiliency as well as more efficient sharing of cyber threat information with the private sector. In accordance with these orders, DHS is expanding its existing information sharing efforts, including the enhanced cybersecurity services initiative and the Critical

Infrastructure Information Sharing and Collaboration Program, so that the private sector can better protect itself. Consistent with the requirements of the Executive Order, DHS is also leading the way in ensuring that privacy and civil liberties protections are incorporated into our cybersecurity initiatives. DHS is also working with NIST and the private sector to develop voluntary standards, methodologies, procedures, and processes to address cyber risks.

While DHS has made significant progress in ensuring the cybersecurity of our Nation, the Executive Order and Presidential Policy Directive are important steps towards further strengthening the Nation's cybersecurity.

DHS's Work with GAO and Congress on Cybersecurity

GAO recognized these and other accomplishments through the closure of 16 recommendations to DHS over the last year regarding cyber analysis and warning, the Trusted Internet Connections (TIC) initiative, and EINSTEIN. The tenor of GAO's High Risk report over the last six years has shifted, focusing now on a whole-of-government approach to cybersecurity as opposed to DHS-specific challenges. DHS is well positioned to support this shift in focus, and its cybersecurity strategy, *Blueprint for a Secure Cyber Future*, focuses on identifying the capabilities needed to adopt such an approach.

DHS works closely with GAO on cybersecurity. Senior NPPD and GAO officials meet quarterly to share information on ongoing cyber activities, discuss DHS's strategic direction in cybersecurity, and review the status of open recommendations. This year, DHS has provided GAO with significant documentation to close nearly all open recommendations, including those related to cyber analysis and warning, public-private partnerships, and the TIC and EINSTEIN initiatives. Where recommendations remain open, DHS has demonstrated to GAO and Congress significant progress in strengthening the effectiveness of partnerships and is continuing to support GAO's request for additional information on the NCCIC.

Congress can support our continuing progress in cybersecurity in two ways: first, you can ask GAO for a clearer articulation of its High Risk criteria so that DHS can use these criteria as a reference when working with our public and private sector partners; and second, passage of comprehensive cyber legislation would allow us to implement the full range of steps needed to build a strong public-private partnership. Secretary Napolitano and I look forward to continuing our work with you to provide the legislative framework for a truly whole-of-Nation approach to securing cyberspace.

National Flood Insurance Program

The National Flood Insurance Program (NFIP) serves as the foundation for national efforts to reduce the loss of life and property from flood disasters, and is estimated to save the Nation \$1.6 billion annually in avoided flood losses. By encouraging and supporting mitigation efforts, the NFIP reduces the impact of disasters. While the NFIP has experienced significant successes since it was created more than 40 years ago, there are a number of challenges facing the program. The most significant challenge is balancing the program's affordability with its fiscal soundness. The NFIP must continue to offer affordable insurance that will properly identify those at risk and provide them adequate coverage, while reducing the need for taxpayer-financed disaster assistance.

Today, more than 21,000 communities in 56 states and territories participate in the NFIP, resulting in more than 5.6 million NFIP policies providing over \$1.2 trillion in coverage. This past fiscal year, the NFIP increased the number of existing flood insurance policies by 47,992.

While the NFIP has been a successful program throughout its 42 years of existence, GAO offers helpful and instructive recommendations for improving the program and DHS/FEMA has already made great progress towards implementing these recommendations.

Flood Mapping

To directly respond to the flood-risk reduction needs of communities, FEMA has produced digital flood hazard data for more than 88 percent of the Nation's population. The NFIP floodplain management standards in each participating community can reduce flood damage in newly constructed buildings by more than 80 percent.

Prior to 2003, more than 70 percent of FEMA's flood maps were at least 10 years old. These maps were developed using what is now outdated technology, and, more importantly, many maps no longer accurately reflected current flood hazards. Over the last eight years, Congress has provided over \$1 billion to update and digitize our Nation's flood maps so we better understand the risks that our Nation faces from flooding. Since the start of FY 2009, we have been implementing the Risk Mapping, Assessment, and Planning (Risk MAP) program, which not only addresses gaps in flood hazard data, but uses updated data to form a solid foundation for risk assessment and floodplain management, and to provide state, local, and tribal governments with information needed to mitigate flood-related risks. Risk MAP is introducing new products and services extending beyond the traditional digital flood maps produced in Flood Map Modernization, including visual illustration of flood risk, analysis of the probability of flooding, economic consequences of flooding, and greater public engagement tools. FEMA is increasing its work with officials to help use flood risk data and tools to communicate risk to citizens more effectively, and enable communities to enhance their mitigation plans.

FEMA also initiated 600 Risk MAP projects affecting 3,800 communities and addressed their highest priority engineering data needs, including coastal and levee areas.

Actuarial Soundness

The passage of the Biggert-Waters Flood Insurance Reform Act in July 2012 was a critical priority for FEMA. The reauthorization and reform means predictable authorization for the NFIP for the next five years. It also established Congress' intent for the NFIP to become a more fiscally sound program through risk-based rates for policy holders. The passage of this important law provides FEMA the authority to address the structural challenges that face the NFIP, and allows FEMA to phase in actuarially sound rates to previously subsidized policies and establish a reserve fund to pay claims in high-loss years.

FEMA has already begun to provide instruction to its Write Your Own insurance company partners to implement the removal of certain subsidies outlined in the law. Starting January 1, 2013, rates for subsidized non-primary residences began increasing upon renewal. In the Fall of 2013, FEMA anticipates releasing further instruction on phasing out subsidies for business properties, substantially damaged or improved properties, severe repetitive loss properties, properties that have incurred flood-related damages where claim payments exceed the fair market value of the property, and newly-purchased property.

In addition, FEMA is also working closely with our governmental partners, including GAO, the Army Corps of Engineers, and the Federal Insurance Office, on the required studies including studies on affordability, reinsurance, NFIP participation by Indian Tribes, and repayment of the NFIP debt to the Treasury.

Strategic Planning Efforts

GAO also recommends that DHS/FEMA complete a strategic plan for the NFIP. We agree with GAO on the importance of multi-year planning, as we must simultaneously execute during the current fiscal year, as well as prioritize and set targets for the upcoming fiscal year, and plan for two years out. FEMA's Federal Insurance and Mitigation Administration has developed a Leadership Guide to Multi-Year Planning that complements their published FY 2012-2014 Strategic Plan. The vision for the multi-year planning process is to ensure the NFIP aligns to FEMA's Planning, Programming, Budget, and Execution (PPBE) process designed to link budget to performance. The goals for multi-year planning include:

- Improving alignment between HQ and Regions;
- Reducing redundant efforts;
- Yielding better quality inputs;
- Preparing for PPBE data calls; and
- Taking advantage of PPBE opportunities.

Establishing a vision for its multi-year planning process and setting goals directly aligned to the Mitigation and Insurance Strategic Plan allows FEMA to better manage its performance and outputs in a time of declining resources.

Claims Management System

FEMA continues to maintain focus on its effort to modernize the NFIP insurance and claims management system. An NFIP Executive Steering Committee was established to provide executive oversight on the development of the new system. The Executive Steering Committee includes representation from a number of FEMA's senior leaders and the DHS Chief Information Officer, as recommended by GAO. Modernizing FEMA's NFIP IT system will address performance gaps by developing and utilizing modern technology to monitor the overall performance of the NFIP in real time. The modernization of the NFIP IT system will provide the necessary automation for the complex business model that the NFIP requires for use by both FEMA and its insurance partners.

While we continue to implement GAO's recommendations and make improvements to the NFIP, we believe that we have already implemented many of GAO's recommendations in this area, and look forward to continuing our close collaboration with GAO in order to close out the recommendations that we have already completed and focusing our energies on the work that remains.

Government-Wide GAO High Risk Series Areas

In addition to the GAO High Risk Series Update areas where DHS is the lead, we also work to improve our operations on several Government-wide GAO High Risk Series areas that have DHS equities, including "Strategic Human Capital Management," "Managing Federal Real Property," and the newly-created area, "Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks." We will continue to make progress on the first two areas in coordination with Congress, GAO and our inter-agency partners, and look forward to a productive dialogue with Congress and GAO on this newly-created GAO High Risk area.

Conclusion

Thank you again for the opportunity to appear before you today to discuss the progress DHS has made in implementing GAO's recommendations, as well as the work we still must do in order to ensure the safety and security of our Nation.

I am happy to answer any questions you may have.

Statement for the Record

**“The Department of Homeland Security at 10 Years: Better
Management and Better Results”**

Elaine C. Duke

**Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
March 21, 2013**

Chairman Carper, Ranking Member Coburn, and members of the Committee, I am pleased to be before this Committee regarding the critical topic of management integration at the Department of Homeland Security. Management integration was important to me when I was the Department's Chief Procurement Officer as a career senior executive, as well as after confirmation by this Committee as the Department's Under Secretary for Management. And it continues to be important to me today, even after my retirement from Federal service. So I thank you for the opportunity to testify in this hearing. I'd like to touch on three phases of DHS management integration in my testimony today: the past, present and future.

First, the past; what I often call the building block stage. Some have the misperception that DHS was formed as a blank slate. That actually would have been easier than the reality of DHS' start up. The truth is it was a melding of 22 different agencies, with many different and disparate systems, cultures, missions; all united by legislation. Each of the legacy agencies brought with them both the good and challenging aspects of their organizations and infrastructure. To achieve the management integration contemplated by the GAO High Risk List, DHS had to reconcile and align the existing, before it could begin integrating for the future. For instance, it could not just lease real property or build a new financial system without constraint; it had to manage through existing infrastructure and systems. One of the most complex problems inherited at the stand-up of DHS was its acquisition system. For example, when DHS was formed, about 90% of its major programs, those over \$1 billion, were not run by a program manager with the necessary qualifications and experience. That drove many of the requirements and program management issues that plagued early DHS programs. One building block to address this issue that was put in place was a certification and training program for program managers and other acquisition professionals, such as contracting officers, and quality assurance specialists. As a result, the numbers have reversed and over 75% of the major programs DHS-wide are run by a properly certified, trained, and experienced program manager.

Now I will briefly address some the present initiatives to further enhance management integration. DHS continues to strengthen some of the building blocks initiated in its early phases. It has expanded or is preparing to expand the acquisition professional certification and training program to other acquisition careers fields such as cost estimating, logistics, test and evaluation, and systems engineering, and it is developing acquisition centers of excellence to build those skills sets. It has put into place Component Acquisition Executives (CAE) at each operating component with major acquisition responsibilities. The CAE is responsible for ensuring successful acquisition in terms of cost, schedule and mission performance. It has also raised the level of acquisition oversight to the Program Accountability and Risk Management Office (PARM) to help increase its authority and effectiveness.

DHS has made significant accomplishments toward management integration. It has put in place several measures to increase accountability and place appropriate responsibility. It has better defined and strengthened the authorities of the six business lines that report to the Under Secretary for Management, including the Chief Procurement Officer and Chief Information Officer. That is an important step to driving the necessary integration throughout DHS. Additionally, it has strengthened the functional integration between the Department's chiefs and their counterparts in the operating components. For example, the component acquisition executive role aligns accountability and authority within the operational components and helps ensure a consistent focus on acquisition program performance. DHS has also strengthened its management governance through portfolio reviews by the Chief Information Officer and stronger investment review boards for major programs. Under the DHS OCIO, integration of the IT infrastructure has been a high priority, both to support efficiency in our IT, but also to support improved mission effectiveness. DHS chartered two Federal Funded Research and Development Centers, Homeland Security Studies and Analysis Institute and MITRE to provide the objective support to its continued integration efforts.

The results of the initial and continued efforts of DHS leadership and management personnel throughout the business lines are beginning to show demonstrated and sustained improvements. First started in USCG as the Blueprint for Acquisition Reform, DHS has applied the best acquisition practices throughout the Department. It has taken back systems integration responsibilities in key programs such as Deepwater and SBInet. It has used the acquisition review process to redirect programs that are breaching cost, schedule and performance measurements. DHS has made significant improvements on its financial audits, despite the fact that the financial systems continue to be disparate, and is launching a plan to improve the financial systems. To date, DHS has closed 18 data centers as it works to consolidate to two enterprise, state-of-the-art data centers. Further, DHS has embraced cloud computing, and has 11 cloud services in production. For instance, more than 100,000 DHS employees are on the DHS Email-as-a-Service, with other Components, such as CIS, poised to migrate shortly. And its strategic sourcing program has rightfully received many laudatory comments for its demonstrated cost savings.

Finally, I will give my recommendations for the future. DHS has a comprehensive strategy in its Integrated Investment Lifecycle Model (IILCM). This model is ideal for the next phase of management integration. It does two important things. First, it develops some much needed management structure around policy and joint requirements. Second, it seeks to integrate and flow the decision making of the various governance processes and boards established as stand-alone building blocks. The integration of the policy, joint capabilities and requirements, resources, and acquisition under the IILCM is critical for the continued maturation and integration of DHS management. It will result in consistent and informed decision making. Under the IILCM, policy will inform capabilities and requirements which will drive resource allocation and set the

stage for strong performance management during program execution. It also expands the portfolio approach to mission which is essential for both improved mission effectiveness and efficiency. The upcoming second DHS Quadrennial Homeland Security Review (QHSR) provides an ideal launching point for DHS to use its IILCM to show a systemic and consistent approach to management decision making throughout the lifecycle. The IILC will, once completely implemented, integrate the work of Policy, Program Accountability and Risk Management, Program Analysis and Evaluation (PA&E), and Science and Technology, driving more effective management of resources and the integration of DHS mission and management throughout the Department.

I believe there are several key things that DHS and GAO, supported by this Committee and other committees of Congress, must do to continue its progress on management integration.

- DHS and its oversight bodies must continue to focus on effectiveness and efficiency. Mission effectiveness must be the primary goal, with efficiency built in to every aspect of mission performance.
- DHS and its oversight bodies must continue to appropriately and allocate resources, both financial and human capital, toward the business lines that drive management integration and sound business practices. It often takes an initial investment to recoup significant long term savings and more effective mission performance. DHS should develop sound business plans with analysis of alternatives and break even analysis to drive investments in management integration, and receive the commensurate financial and policy support to execute those plans. It is important not to be shortsighted with budget for management integration efforts if DHS is to continue its integration progress. DHS has several key initiatives underway, including its three portfolio reviews under the IILCM, and critical efficiency projects under the Chief Readiness Support Officer critical to DHS at this time of budget constraint. It has a key opportunity to build a critically necessary integrated broadband communications/data network, leveraging the FirstNet Public Safety Network. It has also begun, and needs the resources and continued emphasis, to build a multilayered approach to border and transportation security.
- DHS and its oversight bodies must appropriately recognize the efforts DHS employees have made and continue to make, and the results that have been accomplished. Much has been discussed about the poor employee satisfaction at DHS. This clearly must be a DHS leadership priority. However we must not underestimate the negative effect of continued criticism without appropriate recognition by outside parties. Being an employee of DHS, because of its critical mission, public presence, and continued need more maturation, is a challenge. I worked in several different Departments in my career and none was nearly as demanding as DHS. If we are to expect DHS career employees to keep up the good fight for their 30 to 35 year careers, we

must ensure that appropriate positive support accompanies the continued oversight, so those employees can sustain the energy and drive to provide superb mission results.

- DHS must continue implementing its Integrated Investment Lifecycle Model, and should be given the resources to ensure it can do that. The IILCM is a comprehensive integration of the building blocks DHS has put in place to date. The upcoming second Quadrennial Homeland Security Review is an ideal point in time to ensure there is an integrated approach to mission policy and integration at DHS.

DHS remains on the GAO High Risk list for management integration. As time progresses, I would recommend to GAO, DHS, and this Committee to consider the following regarding that continued designation:

- Mr. Dodaro in his February 14 statement to this Committee noted that "DHS has made more progress in implementing its range of missions than in its management functions..." I would argue that the progress in missions could not have been made without improvements in the management functions. DHS is a very mission oriented organization. One needs to consider the "applied management integration" in addition to the pure processes of governance and oversight that are evaluated under the High Risk List. DHS has spent a considerable amount of its limited management resources, throughout its history to support and build mission, after all that is why DHS was formed. I agree with Mr. Dodaro's statement that DHS has "more work" to do toward management integration, but the positive effect of work to date on mission should not be discounted.
- Is DHS managing its management integration risk? Every Department, not just DHS, has many of the key actions in being tracked by related to management integration. For instance, major acquisition programs with cost, schedule, and performance slippage is not unique to DHS, so it begs the question: Should DHS uniquely be on the high risk list for this reason, or is it part of any overall Federal risk? As DHS transitions to managed risk, GAO should consider in its evaluation if DHS is uniquely lacking in an area, and as a result should have this unique designation on the high risk list; or is DHS similar to other Departments in needs to continually focus on and enhance its human capital, financial, acquisition, and information technology management and integration.

I thank this Committee and GAO for their continued commitment to supporting DHS in driving management integration. You have always worked in partnership, toward results in a way that drives change in a bipartisan manner. I also thank the thousands of civil servants at DHS for their continued service to their country and homeland security, for their dedication and tenacity.

Finally, thank you for the strong support you provided DHS while I was there, and that you continue provide today. I am confident that DHS' continued focus and work on management integration, coupled with your leadership, will ensure DHS accomplishes its management integration plan, and protecting our homeland effectively and efficiently. I look forward to your questions.

STATEMENT OF RICHARD L. SKINNER
FORMER INSPECTOR GENERAL
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
U.S. SENATE

The Department of Homeland Security at 10 Years: A Progress Report
on Management

March 21, 2013

Good afternoon Chairman Carper, Ranking Member Coburn, and Members of the Committee. It is truly an honor to be here today to discuss the progress that the Department of Homeland Security has made over the past 10 years and the challenges that remain in improving the management of the department. I thank you for this opportunity.

Since its inception in 2003, the department has worked strenuously to accomplish the largest reorganization of the federal government in more than half a century. Creating the third largest Cabinet agency with the missions of protecting the country against another terrorist attack, responding to threats and hazards, ensuring safe and secure borders, welcoming lawful immigrants and visitors, and promoting the free flow of commerce, has proven, to say the very least, a very difficult task. While the department has made commendable progress over the past 10 years developing and implementing initiatives to carry out its homeland security mission, it has moved at a much slower pace developing and implementing an integrated management platform to support those initiatives. Although progress is being made, it still has much to do to establish a cohesive, efficient, and effective organization.

Both the GAO's biennial update to its High-Risk Series report, dated February 14, 2013, and the DHS OIG's annual Major Management Challenges report, dated December 21, 2012, continue to highlight management support weaknesses that could adversely affect the department's ability to carry out its homeland security mission, ensure the effective and efficient use of limited resources, and provide accountability for its programs and operations. These challenges are essentially the same management challenges that both the GAO and OIG reported as early as 2005. Today, I would like to talk about four of them:

- Financial management
- Information technology management
- Acquisition management
- Grants management

These management support functions constitute the platform upon which the department's programs must operate and are critical to the accomplishment of the department's mission. The weaknesses associated with these support functions, for the most part, were inherited by the department from legacy agencies, and were compounded by the management and program challenges posed by the creation of a large, diverse, and complex organization. Also, the urgency and critical nature of the department's mission hampered efforts, at least in the early years, to focus on and build a strong, integrated management support foundation.

Senior officials at the department have recognized the significance of these challenges and understand that addressing them will take a sustained and focused effort. They have taken actions over the past several years to implement, transform, and strengthen the department's management support functions.

FINANCIAL MANAGEMENT

Financial management has been and continues to be a major management challenge for the department since its creation in 2003. The department has made progress from its early days, however. It has reduced the number of material weaknesses in internal controls from 18 to 5. It also received a qualified audit opinion on its consolidated balance sheet and custodial activity for the first time in fiscal year 2011. Unfortunately, unless it modernizes its financial systems, it is unlikely the department can sustain this progress. As the OIG pointed out in its 2012 Major Management Challenges report, achieving a qualified opinion resulted from the herculean efforts of the department's accountants, rather than reliance on a sound financial management system.

The department twice unsuccessfully attempted to implement an integrated department-wide financial management system, wasting millions of dollars. In 2007, the department ended its first attempt, the Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency system after determining it would not provide the expected functionality and performance. In 2011, the department decided to change its strategy for financial system modernization. Rather than implement a department-wide integrated financial management system solution, the department decided to take a decentralized approach to financial management systems modernization at the component level. Specifically, the department reported in its December 2011 strategy that it plans to replace financial management systems at three components it has identified as most in need, e.g., FEMA, USCG, and ICE. However, due to FY 2012 budget reductions, these initiatives have been put on hold indefinitely. It is now not clear when the department will resume its modernization strategy, nor is it clear whether this new, decentralized approach, if and whenever it is implemented, will ensure that components' financial management systems can generate reliable, useful, timely information for day-to-day decision making; enhance the department's ability to comprehensively view financial information across the department; and comply with related federal requirements at the department and its components. In the interim, the department must continue to use archaic, unreliable systems to manage its financial resources, which is unfortunate, particularly nowadays of budget austerity and the public demand for increased fiscal transparency and accountability.

INFORMATION TECHNOLOGY MANAGEMENT

Integrating the IT systems, networks, and capabilities of legacy agencies to form a single infrastructure for communications and information exchange remains one of the department's biggest challenges. It was by far, in my opinion, one of the department's biggest challenges when it was created in 2003. The department inherited thousands of IT systems from 22 legacy agencies. It took the department nearly 18 months just to inventory the number of systems that it had inherited. Many were archaic and redundant, and almost all were not properly secured.

According to recent OIG and GAO reports, DHS and its components are still struggling to upgrade or transition their respective IT infrastructures, both locally and enterprise wide. For example, in November 2011, the OIG reported that US Citizen and Immigration Services delayed implementing its IT transformation program because of changes in the deployment strategy and system requirements that were insufficiently defined before selecting the IT system solution. Consequently, USCIS must rely on paper-based processes to support its mission, which makes it difficult to process immigration benefits efficiently, combat identity fraud, and share information promptly on possible criminals and terrorists.

Before his retirement in January 2012, the Assistant IG for Emergency Management Oversight, Matt Jadacki, testified before Congress that FEMA's existing information technology systems do not effectively support disaster response activities. FEMA had not completed its efforts to establish an enterprise architecture, and its IT strategic plan was not comprehensive enough to coordinate and prioritize its modernization initiatives and IT projects. The plan did not include clearly defined goals and objectives, nor did it address program office IT strategic goals. Without these critical elements, FEMA is challenged to establish an effective approach to modernize its information technology infrastructure and systems.

In June 2012, the OIG reported that the information technology environment and the aging IT infrastructure within CBP does not fully support CBP's mission needs. According to the OIG, interoperability and functionality of the technology infrastructure have not been sufficient to support CBP mission activities fully. As a result, CBP employees have created workarounds or employed alternative solutions, which may hinder CBP's ability to accomplish its mission and ensure officer safety.

More recently, in October 2012, the OIG completed an evaluation of the department's information security program and practices to comply with the requirements of the *Federal Information Security Management Act*. The OIG reported that DHS components still are not executing all the department's policies, procedures, and practices, and thereby weakening the department's overall information security posture.

Similar problems also have been reported at the Coast Guard, ICE, and Secret Service. Technical and cost barriers, aging infrastructure that is difficult to support, outdated IT strategic plans to guide investment decisions, and stove-piped system development have impeded the department's efforts to modernize and integrate its IT systems, networks, and capabilities.

Information Sharing

The Homeland Security Act of 2002 makes coordination of homeland security communication with state and local government authorities, the private sector, and the public a key department responsibility. However, due to time pressures, the department did not complete a number of the steps essential to effective planning and implementation of the Homeland Security Information Network (HSIN)—the “sensitive but unclassified” system it instituted to help carry out this mission. For example, the HSIN and the Homeland Security State and Local Community of

Interest systems, both developed by DHS, are not integrated. As a result, users must maintain separate accounts, and information cannot easily be shared across the systems. State and local fusion center personnel expressed concern that there were too many federal information sharing systems that were not integrated. As such, effective sharing of counter-terrorist and emergency management information critical remains an ongoing challenge for the department. Resources, legislative constraints, privacy, and cultural challenges—often beyond the control of the department—pose obstacles to the success of the department’s information sharing initiatives.

On a broader scale, the department is also challenged with incorporating data mining into its overall strategy for sharing information to help detect and prevent terrorism. Data mining aids agents, investigators, and analysts in the discovery of patterns and relationships from vast quantities of data. The Homeland Security Act authorizes the department to use data mining and tools to access, receive, and analyze information. However, the department’s data mining activities consist of various stove-piped activities that use limited data mining features. For example, CBP performs matching to target high-risk cargo. The Secret Service automates the evaluation of counterfeit documents. TSA collects tactical information on suspicious activities. ICE detects and links anomalies indicative of criminal activity to discover relationships. Without department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues remains untapped.

I understand that DHS has taken numerous steps over the past 2 years to strengthen its enterprise architecture and information security programs. However, many of these initiatives are still a “work-in-progress.” Much work remains to be done. The challenge for department from here-on-out will be sustaining the progress already made over the past few years while, at the same time, continuing to invest in improvements that are needed to strengthen its IT infrastructure.

ACQUISITION MANAGEMENT

During my tenure as the IG of the department, this was the one area that, in my opinion, improved the most. This was due, for most part, to the commitment made by the Secretary and Deputy Secretary of Homeland Security, and other senior officials, including my co-panelist, Elaine Duke, to improve the department’s acquisition management function.

Beginning with the department’s inception in 2003, the OIG and GAO identified perennial problems relating to acquisition oversight, cost growth, and schedule delays, resulting in performance problems and mission delays, as illustrated by the problems the department experienced with the Coast Guard’s Deepwater program, CBP’s SBINet program, FEMA’s flood map modernization program, and the CFO’s financial systems consolidation initiatives. Each of these efforts failed to meet capability, benefit, cost, and schedule expectations. For example, in June 2010 my former office reported that over half of the programs we reviewed awarded contracts to initiate acquisition activities without component or department approval of documents essential to planning acquisitions, such as mission need statements outlining the specific functional capabilities required to accomplish DHS’s mission and objectives; operational

requirements; and acquisition program baselines. Additionally, the OIG reported that only a small number of DHS's major acquisitions had validated cost estimates.

Since the issuance of those reports, DHS has made remarkable strides to implement, transform, and strengthen its acquisition management capabilities. At the time of my retirement on March 1, 2011, the number of procurement staff had more than doubled since 2005. In addition, participation in the Acquisition Professional Career Program, which sought to develop acquisition leaders, increased 62% from 2008 to 2010. Also, since my retirement, according to GAO and the OIG, the department developed detailed plans to address a number of other acquisition management challenges. For example, it created a Procurement Staffing Model and chartered Centers of Excellence to enhance its acquisition capabilities, and is implementing a Decision Support Tool which was developed to gauge the health of major acquisitions and facilitate the flow of information from the components to the Management Directorate. Furthermore, I think it is worth mentioning, DHS reduced its noncompetitive contracts over the past four years by 89 percent, from \$3.5 billion in 2008 to \$389 million in fiscal year 2012. In my opinion, this is a major accomplishment.

However, as both the GAO and OIG have pointed out over the past year, much work remains. The department continues to experience performance problems, cost overruns, schedule delays, and often lacks fundamental documents needed to help manage risk and measure performance. Both the GAO and OIG have recommended that the department equip the Office of the Chief Procurement Officer with additional resources to provide effective, department-wide oversight of acquisition policies and procedures, and the authority to enforce compliance with those policies and procedures. To be truly successful, the department must have an infrastructure in place that not only enables it to effectively oversee the complex and large dollar procurements critically important to achieving its mission, but also provides the transparency, accountability, and enforcement tools needed to ensure that its components are adhering to key knowledge-based acquisition practices and departmental policies and procedures.

The urgency and complexity of the department's mission will continue to demand rapid pursuit of major investment programs. Since its creation, the department spent about 40% of its budget on contracts. In fiscal year 2012, the department had approximately 160 acquisition programs with estimated life cycle costs of more than \$144 billion. Although that figure may decrease in the years ahead, the department will continue to rely heavily on contractors to accomplish its multifaceted mission and will continue to pursue high-risk, complex acquisition programs.

GRANTS MANAGEMENT

Disaster Grants Management

FEMA oversees billions of dollars in disaster grant funds each year, and, due to the environment under which these funds are administered, they are highly vulnerable to fraud, waste, and abuse. To illustrate, during fiscal year 2012, the OIG's audits of 56 disaster grants identified \$387 million in questionable costs and funds that could be put to better use. The extent of the fraud,

waste, and abuse that the OIG uncovers year after year in the disaster relief program, for the past 25 years, is unacceptable, and it needs to be vigorously addressed. Yet FEMA still has not developed a robust program to curtail fraud, waste, and abuse within its disaster relief programs.

Preparedness Grants Management

Over the past 10 years, DHS has awarded more than \$35 billion to state, local, tribal, and territorial governments to enhance their capabilities to prepare for and prevent natural and manmade disasters and acts of terrorism.

Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, requires the OIG to audit individual states' management of State Homeland Security Program and Urban Areas Security Initiatives grants and annually submit to Congress a report summarizing the results of these audits. In the audits completed to date, the OIG concluded that the states have generally done an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used.

However, according to an OIG report released this past December, the department still does not have a system in place to determine the extent its preparedness grants have enhanced the states' capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Also, the department does not require states to report progress in achieving milestones as part of the annual application process. As a result, when annual application investment justifications for individual continuing projects are being reviewed, DHS does not know whether prior year milestones for the projects have been completed. DHS also does not know the amount of funding required to achieve needed preparedness and response capabilities. Furthermore, many states have outdated strategic plans, and many do not have plans with goals and objectives that are specific, measurable, achievable, results-oriented, and time-limited. Without some form of measurable goal or objective, or a mechanism to objectively gather results-oriented data, neither DHS nor the states can demonstrate the level of effectiveness of the Nation's preparedness and response capabilities.

Finally, DHS needs to improve its grantee monitoring program to ensure the grant recipients are meeting their financial and project obligations on time and according to applicable federal and state laws and regulations. On February 14, 2013, the OIG reported that DHS either inconsistently applied or failed to apply risk indicators to determine the level of monitoring a grantee should receive. Consequently, DHS did not have a reasonable level of assurance that high-risk grantees were being monitored.

Strategic planning, performance measurement, and oversight are important management controls for DHS to ensure that federal funds are used for their intended purpose and that enhancements in preparedness capabilities are being achieved. Without a bona fide performance measurement system, it is impossible to determine whether annual investments are improving our Nation's homeland security posture. Furthermore, without clear, meaningful performance standards, the

department lacks the tools necessary to make informed funding decisions. In today's economic climate, it is critical that DHS concentrate its limited resources on those threats that pose the greatest risk to the country.

In conclusion, I believe it is important to understand that most, if not all, of the department's management support challenges were inherited from the department's legacy agencies. The department did not create them. To compound matters, the complexity and urgency of the department's mission have often exacerbated the department's ability to address them in a disciplined and effective manner.

The department's senior officials are well aware of these challenges and are attempting to remedy them, and, are making some headway. Today, ten years after its creation, the department now has in place one of the strongest management teams imaginable. The Under Secretary for Management, the Chief Information Officer, the Chief Financial Officer and the Chief Procurement Officer, all have proven that they possess the knowledge and skills needed to get the job done. Moreover, they have the full support of the Secretary and Deputy Secretary, both of whom have demonstrated a their commitment to improving the department's management functions.

The question now is does the department have the resolve and wherewithal to sustain those efforts. The ability of the department to do so is fragile, not only because of the early stage of development that the initiatives are in, but also because of the government's budget constraints and the current lack of resources to implement planned corrective actions. In today's environment of large government deficits and pending budget cuts, the new challenge will be to sustain the progress already made and at the same time continue to make the necessary improvements that are critical to the success of the department's management functions and, what is more important, to its homeland security mission. To accomplish this, they need your support.

It is important that the Congress continue to invest in the department's management improvement initiatives, and continue to provide oversight of those efforts. Unless the department and Congress stay focused on these challenges, it will be harder than ever to facilitate solutions to strengthen the department's management support functions and, ultimately, its homeland security mission.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the Members may have.

Written Statement
of
Shawn Reese
Analyst in Emergency Management and Homeland Security Policy
Before
The Senate Homeland Security and Governmental Affairs Committee
March 21, 2013
“The Department of Homeland Security at 10 Years: A Progress Report on
Management”

Chairman Carper, Ranking Member Coburn, and Members of the Committee, on behalf of the Congressional Research Service I would like to thank you for this opportunity to appear before you to discuss the Department of Homeland Security (DHS) at its tenth anniversary.

Today I will discuss the implications of the absence of a federal government-wide national homeland security strategy, the use of multiple definitions of homeland security in national strategic documents, the lack of comprehensive national homeland security priorities, and the funding of these priorities. Specifically, my statement will address how the absence of clear definition and concept of homeland security affects DHS' ability to prioritize and manage the department's missions. This written statement is drawn largely from my CRS report *Defining Homeland Security: Analysis and Congressional Considerations*.

Accordingly, my statement summarizes key portions of this report, and addresses key findings which include the absence of an agreed upon comprehensive definition and concept of homeland security. This absence, then affects how DHS, and the federal government, prioritize homeland security missions. My statement concludes with an analysis of the potential consequences stemming from the lack of a consensus homeland security definition and concept, the absence of homeland security priorities, and how this may affect the funding and execution of critical homeland security activities.

Current Homeland Security Environment

Congress and policymakers are responsible for funding homeland security priorities. Generally, these priorities need to exist and be clear in order for funding to be most effective. Presently, as DHS itself has stated,¹ the department does not prioritize its homeland security missions across DHS mission areas. Many argue, in an ideal scenario, there would be a clear and comprehensive definition and concept of homeland security, and a consensus about it; as well as prioritized missions, goals, and activities that emit from this comprehensive definition. Policymakers could then use a process to incorporate feedback and respond to new facts and situations as they develop. However, more than ten years after the 9/11 terrorist attacks, policymakers continue to grapple with a comprehensive definition and concept of homeland security. For example, the U.S. government does not have a single definition for "homeland security." Currently, different strategic documents and mission statements offer varying missions that are derived from different homeland security definitions. Of course, over time it is expected that definitions and concepts change and evolve in response to changing conditions. The question is what is the comprehensive definition of homeland security today. This is more than an issue of what words describe "homeland security," it is instead an issue of how policymakers understand what homeland security is and how it is accomplished.

¹ Alan Cohn, U.S. Department of Homeland Security, Office of Policy, statement before the House Homeland Security Committee, Subcommittee on Oversight, Investigations, and Management, "Is DHS Effectively Implementing a Strategy to Counter Emerging Threats?" hearing, 112th Cong., 2nd sess., Feb. 3, 2012.

Historically, the strategic documents framing national homeland security policy have included national strategies produced by the White House and documents developed by DHS. Prior to the 2010 *National Security Strategy*, the 2002 and 2007 *National Strategies for Homeland Security* were the guiding documents produced by the White House. In 2011, the White House issued the *National Strategy for Counterterrorism*.

In conjunction with these White House strategies, DHS has developed a series of evolving strategic documents that are based on the two national homeland security strategies and include the 2008 *Strategic Plan—One Team, One Mission, Securing the Homeland*; the 2010 *Quadrennial Homeland Security Review* and *Bottom-Up Review*; and the 2012 *Department of Homeland Security Strategic Plan*. The 2012 DHS strategic plan is the latest evolution in DHS's process of defining its mission, goals, and responsibilities. This plan, however, only addresses the department's homeland security purview and is not a document that addresses homeland security missions and responsibilities that are shared across the federal government.

Today, 30 federal entities receive annual homeland security funding excluding DHS. The Office of Management and Budget (OMB) estimates that 48% of annual homeland security funding is appropriated to these federal entities, with the Department of Defense (DOD) receiving approximately 26% of total federal homeland security funding. DHS receives approximately 52%.²

Currently, DHS is developing the 2014 *Quadrennial Homeland Security Review (QHSR)*, which is scheduled to be issued in late 2013 or early 2014. Given the anticipated issuance of this latest QHSR, this might be an ideal time to review the concept of homeland security, the definition of the term "homeland security," and how the concept and definition of homeland security affect congressional appropriations and the identification of priorities as established by DHS and the Administration.

Evolution of the Homeland Security Concept

The concept of homeland security is evolving. The evolution of the homeland security concept has been communicated in several strategic documents. Today, strategic documents provide guidance to all involved federal entities and include the 2010 *National Security Strategy* and the 2011 *National Strategy for Counterterrorism*. There are also strategic documents that provide specific guidance to DHS entities and include the 2010 *Quadrennial Homeland Security Review*, the *Bottom-Up Review*, and the 2012 *Department of Homeland Security Strategic Plan*. Prior to issuance of these documents, national and DHS homeland security strategic documents included the 2002 and 2007 *National Strategies for Homeland Security* and the 2008 *Department of Homeland Security Strategic Plan*. All of these documents have varying definitions for "homeland security" and varying missions have been derived from these definitions.

² U.S. Office of Management and Budget, *Budget of the United States Government, Fiscal Year 2013: Analytical Perspectives, February 2012*, "Appendix – Homeland Security Mission Funding by Agency and Budget Account," http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/homeland_supp.pdf.

While the definitions and missions embodied in these strategic documents have commonalities, there are significant differences. Natural disasters are specifically identified as an integral part of homeland security in five of the seven documents, and three documents—the 2008 and 2012 DHS *Strategic Plans* and the *Bottom-Up Review*—specifically include border and maritime security and immigration in their homeland security definitions. All of these mentioned issues are important and involve significant funding requests. However, the lack of consensus about the inclusion of these policy areas in a definition of homeland security may have negative or unproductive consequences for national homeland security operations. The inclusion or exclusion of a particular mission in the homeland security concept does not mean that the mission is not being funded or perhaps even being funded adequately. It means that it is more difficult for policymakers to prioritize across mission areas and answer the question of what future homeland security appropriations ought to fund. A consensus definition could be useful, but may not be sufficient. A clear prioritization of strategic missions may help focus and direct federal entities' homeland security activities. Additionally, prioritization affects Congress's authorization, appropriation, and oversight activities. Ultimately, DHS' current efforts to design and issue the forthcoming QHSR may be important in the debate on a comprehensive homeland security strategy.

The continued absence of distinct national homeland security priorities may be the result of competing or differing definitions of homeland security within national strategic documents and the evolving concept of homeland security. However, prior to 9/11 such entities as the Gilmore Commission³ and the United States Commission on National Security⁴ discussed the need to evolve the way national security policy was conceptualized due to the end of the Cold War and the rise of radicalized terrorism. After 9/11, policymakers concluded that a new approach was needed to address the large-scale terrorist attacks. A presidential council and department were established, and a series of presidential directives were issued in the name of "homeland security." These developments established that homeland security was a distinct, but undefined concept.⁵ Later, the federal, state, and local government responses to disasters such as Hurricanes Katrina and Sandy expanded the concept of homeland security to include significant disasters, major public health emergencies, and other events that threaten the United States, its economy, the rule of law, and government operations.⁶

One may argue, however, that homeland security as concept or policy might be waning as a separate and distinct policy concept. Evidence for this viewpoint can be found in the current Administration's incorporation of the homeland security staff into the national security staff and the inclusion of homeland security priorities within the 2010 *National Security Strategy*. There has not been a national homeland security strategy since 2007. Additionally, the Office of

³ For information on the Gilmore Commission, see <http://www.rand.org/nsrd/terrpanel.html>. The Gilmore Commission was established prior to 9/11; however, it released its fifth and final report in December 2003.

⁴ For information on the U.S. Commission on National Security, see <http://www.fas.org/irp/threat/nssg.pdf>. The U.S. Commission on National Security was established in 1998 and issued its final report in February 2001. The commission did reference the idea of "homeland security" in early 2001.

⁵ Harold C. Relyea, "Homeland Security and Information," *Government Information Quarterly*, vol. 19, 2002, p. 219.

⁶ Nadav Morag, "Does Homeland Security Exist Outside the United States?," *Homeland Security Affairs*, vol. 7, September 2011, p. 1.

Management and Budget (OMB) has questioned the value of federal departments and agencies identifying homeland security funding with their FY2014 budget request submissions.⁷

Definitions and Missions⁸

Definitions and missions are part of strategy development. Policymakers develop strategy by identifying national interests, prioritizing missions to achieve those national interests, and arraying instruments of national power to achieve national interests.⁹ Strategy is not developed within a vacuum. President Barack Obama's Administration's 2010 *National Security Strategy* states that strategy is meant to recognize "the world as it is" and mold it into "the world we seek."¹⁰ Developing a homeland security strategy, however, may be complicated if the key concept of homeland security is not succinctly defined, and strategic missions are not aligned and synchronized among different strategic documents and federal entities.

Some common themes among homeland security definitions in national strategic documents are:

- the homeland security enterprise encompasses a federal, state, local, and tribal government and private sector approach that requires coordination;
- homeland security can involve securing against and responding to both hazard-specific and all-hazards threats; and
- homeland security activities do not imply total protection or complete threat reduction.

Each of these documents highlights the importance of coordinating homeland security missions and activities. However, individual federal, state, local, and tribal government efforts are not identified in the documents.

The competing and varied definitions in these documents may indicate that there is no succinct and comprehensive homeland security concept. Without a succinct homeland security concept, policymakers and entities with homeland security responsibilities may have a hard time successfully coordinating or focusing on the highest prioritized or most necessary activities. Coordination is especially essential to homeland security because of the multiple federal agencies and the state and local partners with whom they interact. Coordination may be difficult if these entities do not operate with the same understanding of the homeland security concept. For example, definitions that do not specifically include immigration or natural disaster response and recovery may result in homeland security stakeholders and federal entities not adequately resourcing and focusing on these coordinated activities. Again, it is not about whether mission areas are funded or not, it is about how DHS prioritizes the funding across mission areas, and how policymakers choose between DHS priorities and the priorities of other agencies tasked

⁷ http://www.performance.gov/sites/default/files/tmp/_List_of_Reports_Required_by_P_L%20111-352.xls

⁸ A table summarizing homeland security definitions and missions can be found in CRS report *Defining Homeland Security: Analysis and Congressional Considerations*.

⁹ Terry L. Deibel, *Foreign Affairs Strategy: Logic for American Statecraft* (New York: Cambridge University Press, 2007), p. 5.

¹⁰ Executive Office of the President, *National Security Strategy*, Washington, DC, May 2010, p. 9.

with homeland security responsibilities. Additionally, an absence of a consensus definition may result in Congress funding a homeland security activity that DHS does not consider a priority. An absence of a national list of priorities could result in DHS being unable to identify where to spend future homeland security dollars.

Varied homeland security definitions, in numerous documents, result in homeland security stakeholders identifying and executing varied strategic missions. Homeland security stakeholders include federal departments and agencies, state and local governments, and non-profit and non-governmental organizations. The strategic documents mentioned earlier and listed in the CRS report identify numerous homeland security missions such as terrorism prevention; response and recovery; critical infrastructure protection and resilience; federal, state, and local emergency management and preparedness; and border security. As noted earlier, none of these documents specifically tasks a federal entity with the overall responsibility for homeland security.

These strategic documents all identify specific missions as essential to securing the nation. All of the documents state that the nation's populace, critical infrastructure, and key resources need protection from terrorism and disasters. This protection from both terrorism and disasters is a key strategic homeland security mission. Some, but not all, of the documents include missions related to border security, immigration, the economy, and general resilience. Members of Congress and congressional committees, however, have sometimes criticized these documents.

Senator Susan Collins—former ranking member of this committee—expressed disappointment in the 2010 *Quadrennial Homeland Security Review* and 2010 *Bottom-Up Review* arguing that they did not communicate priorities and did not compare favorably to the most recent *Quadrennial Defense Review*.¹¹ The *Quadrennial Defense Review* identifies national security and U.S. military priorities through a process “...from objectives to capabilities and activities to resources.”¹² Furthermore, the *Quadrennial Homeland Security Review* missions are different from the 2007 *National Strategy for Homeland Security*¹³ missions, and neither identifies priorities, or resources, for DHS, or for other federal agencies. Since the *National Strategy for Homeland Security* and the *Quadrennial Homeland Security Review* missions are differing and varied, and because the *Quadrennial Homeland Security Review* does not specifically identify a strategic process to achieve the missions, it could be assumed that this document was meant to be solely operational guidance. Additionally, some critics found the *Bottom-Up Review* lacking in detail and failing to meet its intended purpose.¹⁴

¹¹ U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Charting a Path Forward: The Homeland Security Department's Quadrennial Review and Bottom-Up Review*, 111th Cong., 2nd sess., July 21, 2010.

¹² U.S. Department of Defense, *Quadrennial Defense Review*, Washington, DC, February 2010, p. iii.

¹³ The 2007 *National Strategy for Homeland Security* is the most recent national strategy specifically on homeland security.

¹⁴ Katherine McIntire Peters, “DHS Bottom-Up Review is long on ambition, short on detail,” *GovernmentExecutive.com*, July 2010.

Further congressional criticism included an observation on the absence of a single DHS strategy. At a House Homeland Security Committee's Subcommittee on Oversight, Investigations and Management hearing, Chairman Michael McCaul stated that "...DHS needs a single strategic document which subordinate agencies can follow and make sure the strategy is effectively and efficiently implemented. This single document should conform to the National Security Strategy of the United States of America. If the agencies do not have a clearly established list of priorities, it will be difficult to complete assigned missions."¹⁵

Quadrennial Homeland Security Review

In August 2007, Congress enacted the Implementing 9/11 Commission Recommendations Act¹⁶ which required the DHS Secretary to conduct a quadrennial review of homeland security. This review was to be a comprehensive examination of the homeland security strategy of the Nation, including recommendations regarding the long-term strategy and priorities of the Nation for homeland security and guidance on the programs, assets, capabilities, budget, policies, and authorities of the Department.¹⁷

Additionally, the DHS Secretary was to consult with the "heads of other Federal agencies" and

*delineate and update, as appropriate, the national homeland security strategy, consistent with appropriate national and Departmental strategies, strategic plans, and Homeland Security Presidential Directives, including the National Strategy for Homeland Security, the National Response Plan, and the Department Security Strategic Plan.*¹⁸

These updates were to "prioritize the full range of the critical homeland security mission areas of the Nation."¹⁹ Many knowledgeable observers concluded that the 2010 *Quadrennial Homeland Security Review* did not accomplish these requirements. For example, David Maurer, Director of the Government Accountability Office's Homeland Security and Justice Team stated before the House Committee on Homeland Security's Subcommittee on Oversight, Investigations, and Management on February 3, 2013, that the 2010 QHSR identified five key DHS missions but did not prioritize them as required by the 9/11 Commission Act.²⁰ Additionally, Alan Cohn, Deputy Assistant Secretary, Office of Policy, DHS, stated, in February 2012, that the department was

¹⁵ U.S. Congress, House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management, *Is DHS Effectively Implementing a Strategy to Counter Emerging Threats?*, 112th Cong., 2nd sess., February 3, 2012.

¹⁶ P.L. 110-53.

¹⁷ 121 Stat. 544, 6 U.S.C. 347.

¹⁸ *Ibid.*

¹⁹ *Ibid.*

²⁰ David Maurer, Government Accountability Office, statement before the House Homeland Security Committee, Subcommittee on Oversight, Investigations, and Management, "Is DHS Effectively Implementing a Strategy to Counter Emerging Threats?" hearing, 112th Cong., 2nd sess., Feb. 3, 2012.

still in the process of aligning resources with priorities. However, that process was not completed for the 2010 QHSR.²¹

Congressional Considerations

Policymakers are faced with a complex and detailed list of risks, or threats to security, for which they then attempt to plan. However, some have argued that managing those risks correctly 99% of the time may not be good enough when even a single failure may lead to significant human and financial costs.²² Homeland security is essentially about managing risks. The purpose of a strategic process is to develop missions to achieve that end. Before risk management can be accurate and adequate, policymakers ideally coordinate and communicate. That work to some degree depends on developing a foundation of common definitions of key terms and concepts. It is also necessary, in order to best coordinate and communicate, to ensure stakeholders are aware of, trained for, and prepared to meet assigned missions. At the national level, many believe there is yet not an alignment of homeland security definitions and missions among disparate federal entities. DHS is, however, attempting to align its definition and missions, but does not prioritize its missions;²³ there appears to be clarity lacking in the national strategies of federal, state, and local roles and responsibilities; and, potentially, some may argue that funding is driving priorities rather than priorities driving the funding.

There is no evidence in the existing homeland security strategic documents that supports the aligning and prioritization of the varied missions, nor do any of the documents appear to convey how national, state, or local resources are to be allocated to achieve these missions. Without prioritized resource allocation to align missions, proponents of prioritization of the nation's homeland security activities and operations maintain that plans and responses may be haphazard and inconsistent. Another potential consequence of the absence of clear missions is that available funding then tends to drive the priorities.

It has been argued that homeland security, at its core, is about coordination because of the disparate stakeholders and risks.²⁴ Many observers assert that homeland security is not only about coordination of resources and actions to counter risks; it is also about the coordination of the strategic process policymakers use in determining the risks, the stakeholders and their missions, and the prioritization of those missions.

²¹ Alan Cohn, Department of Homeland Security, statement before the House Homeland Security Committee, Subcommittee on Oversight, Investigations, and Management, "Is DHS Effectively Implementing a Strategy to Counter Emerging Threats?" hearing, 112th Cong., 2nd sess., Feb. 3, 2012.

²² Donald F. Kettl, *System Under Stress: Homeland Security and American Politics*, 2nd ed., Washington, DC, CQPress, 2007, p. 82.

²³ Alan Cohn, Department of Homeland Security, statement before the House Homeland Security Committee, Subcommittee on Oversight, Investigations, and Management, "Is DHS Effectively Implementing a Strategy to Counter Emerging Threats?" hearing, 112th Cong., 2nd sess., Feb. 3, 2012.

²⁴ Ibid.

Without a general consensus on the physical and philosophical definition and missions of homeland security, achieved through a strategic process, some believe that there will continue to be the potential for disjointed and disparate approaches to securing the nation. From this perspective general consensus on the homeland security concept necessarily starts with a comprehensive consensus definition and an accepted list of prioritized missions that are constantly reevaluated to meet risks of the new paradigm that is homeland security in the 21st century. These varied definitions and missions, however, may be the result of a strategic process that has attempted to adjust federal homeland security policy to continually emerging threats and risks.

Congress may decide to address the issues associated with homeland security strategy, definitions, and missions, in light of the potential for significant events to occur similar to the 9/11 terrorist attacks and Hurricanes Katrina and Sandy. Specifically, Congress may choose to consider a number of options addressing the apparent lack of a consensus homeland security definition that prioritizes missions by requiring the development of a more succinct, and distinct, national homeland security strategy. Three options stand out for congressional consideration.

First, Congress could require a distinct national homeland security strategy which would be similar to the Bush Administration's 2002 and 2007 strategies. Second, Congress could require a refinement of the National Security Strategy that would include succinct risk based homeland security priorities. Finally, Congress may focus strictly on DHS activities. This option would entail DHS further refining its quadrennial review which it is presently doing.

**G A O**

Accountability • Integrity • Reliability

United States Government Accountability Office
Washington, DC 20548

May 8, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate

Subject: *Department of Homeland Security: Response to Post-Hearing Questions for the Record*

Dear Mr. Chairman:

This letter responds to your April 5, 2013, request that we address questions submitted for the record by Senator Mark L. Pryor, related to our statement at the March 21, 2013, hearing on management at the Department of Homeland Security (DHS).¹ At the hearing, we discussed, among other things, the progress DHS has made in transforming its original component agencies into a single department and our narrowing the scope of this high-risk area to focus on strengthening the department's management functions. Specifically, we noted that DHS needs to further strengthen its acquisition, information technology (IT), and financial and human capital management functions. The enclosure provides our responses to Senator Pryor's questions. In responding to these questions, we relied on work associated with previously issued GAO reports, as well as a review of a recent statement by the DHS Chief Information Officer.

If you have any questions about this letter or need additional information, please contact me at (202) 512-5500 or Cathleen A. Berrick, Managing Director, Homeland Security and Justice at (202) 512-3404 or berrickc@gao.gov.

Sincerely yours,

Gene L. Dodaro

Comptroller General of the United States

Enclosure

¹See GAO, *High-Risk Series: Government-wide 2013 Update and Progress Made by the Department of Homeland Security*, GAO-13-444T (Washington, D.C.: March 21, 2013).

Enclosure

**Post-Hearing Questions for the Record
Submitted to the Honorable Eugene L. Dodaro
From Senator Mark L. Pryor**

"The Department of Homeland Security at 10 Years: A Progress Report on
Management"
March 21, 2013

1. Acquisitions program management and IT project management have been difficult areas for the Department of Homeland Security (DHS) to manage. What resources are needed to make improvements in these areas?

In a number of reports issued within the last year, we have identified deficiencies in both DHS's acquisition and IT program and portfolio management. We further reported that important resources in both of these areas include sound policy, adequate workforce to implement that policy, and rigorous and institutionalized project management disciplines. We recommended actions the department can take in these areas that, if fully implemented, should lead to needed improvements.

For example, with regard to major program acquisitions, we reported in September 2012, that DHS had established a knowledge-based acquisition policy for program management that is largely consistent with key practices and would help DHS address the significant challenges we identified across its acquisition programs.² These challenges included funding instability, workforce shortfalls, and changes in planned capabilities. However, we found that DHS has not consistently met the policy's requirements, and officials explained that DHS's culture has emphasized the need to rapidly execute missions more than sound acquisition management practices. Among other things, at the time, officials told us that DHS leadership permitted programs to advance without department-approved acquisition documents because the department had an operational need for the promised capabilities, but could not approve the documents in a timely manner. Because DHS has not generally implemented its acquisition policy, senior leaders lack the critical knowledge needed to accurately track program performance. We recommended that the department ensure that all major acquisition programs fully comply with DHS acquisition policy before approving their movement through the acquisition life cycle. DHS concurred with this recommendation. We will continue to monitor the department's progress in addressing our recommendations and adhering to its program management policy.

In addition, as we reported in September 2012, DHS officials explained that, in certain instances, programs were not capable of documenting knowledge needed to support effective decision making, while in others, DHS headquarters lacked the capacity to validate the adequacy of the documented knowledge. We have previously identified that the magnitude and complexity of the DHS acquisition

²GAO, *Homeland Security: DHS Requires More Disciplined Investment Management to Help Meet Mission Needs*, GAO-12-833 (Washington, D.C.: Sept. 18, 2012).

portfolio demands a capable and properly trained workforce and that workforce shortfalls increase the risk of poor acquisition outcomes. Fifty-one of 62 program manager survey respondents reported that their programs had experienced workforce shortfalls, increasing the likelihood their programs will perform poorly in the future. DHS's acquisition policy establishes that major program offices should be staffed with personnel with appropriate qualifications and experience in key acquisition disciplines. Alternatively, DHS officials told us headquarters staffing shortfalls are less of an issue than in the past. Specifically, DHS headquarters officials told us that, as of fiscal year 2012, they had enough resources to hold oversight reviews when components requested them.

In another example, with regard to IT project management, we reported in September 2012 that approximately one-third of DHS's major IT investments—which totaled about \$1 billion in spending—had one or more subsidiary projects with cost or schedule overruns of at least 10 percent.³ Causes of these shortfalls included weaknesses in key project management disciplines such as cost and schedule estimating and defining requirements, among others. Moreover, we found that DHS often did not adequately address these shortfalls and their causes, in part because department guidance did not consistently require the documentation of corrective actions.

In a March 19, 2013, written statement submitted to the House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, DHS's Chief Information Officer (CIO) stated that the department is establishing a series of Centers of Excellence to provide guidance, training, and support from subject matter experts across DHS in program, project, and technical disciplines.⁴ To date, according to the CIO, eight centers have been established,⁵ and the department plans to review the need for additional centers in years to come.

We recommended in our September 2012 report that DHS (1) address the shortcomings in its guidance and (2) develop corrective actions for all major IT investments experiencing cost and schedule shortfalls. The department concurred and estimated that it would implement the first recommendation by the end of September 2013 and the second one immediately. In addition, if the Center of Excellence model is expanded, it could significantly increase DHS's IT project success and help address the shortcomings we have identified.

a. Are there best practices that DHS management can look to for guidance on measurable, sustainable progress in implementing its key management initiatives?

³GAO, *Information Technology: DHS Needs to Enhance Management of Cost and Schedule for Major Investments*, GAO-12-904 (Washington, D.C.: Sept. 26, 2012).

⁴DHS Management Directorate Chief Information Officer Richard Spires, written testimony for a House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency hearing titled "DHS Information Technology: How Effectively Has DHS Harnessed IT to Secure Our Borders and Uphold Immigration Laws?" (Washington, D.C.: March 19, 2013).

⁵These centers cover program management, cost estimating and analysis, enterprise architecture, systems engineering, requirements engineering, test and evaluation, privacy, and accessibility.

There are best practices that DHS management can use to guide their management improvement efforts, many of which we have cited in our prior reports on DHS management functions. GAO has also issued best practices across a range of management and other disciplines that can assist agencies in their efforts.

For example, we reported in September 2012 that DHS has developed an acquisition policy that is consistent with many key program management practices that we have previously identified.⁶ These key practices are summarized in table 1, along with our assessment of DHS's acquisition policy.

Table 1: GAO Assessment of DHS's Acquisition Policy Compared to Key Program-management Practices

GAO key practice area	Summary of key practices	GAO assessment of DHS acquisition policy
Identify and validate needs	Current capabilities should be identified to determine if there is a gap between the current and needed capabilities. A need statement should be informed by a comprehensive assessment that considers the organization's overall mission.	●
Assess alternatives to select most appropriate solution	Analyses of Alternatives should be conducted early in the acquisition process to compare key elements of competing solutions, including performance, costs, and risks. Moreover, these analyses should assess many alternatives across multiple concepts.	●
Clearly establish well-defined requirements	Requirements should be well defined and include input from operators and stakeholders. Programs should be grounded in well-understood concepts of how systems would be used and likely requirements costs.	●
Develop realistic cost estimates and schedules	A cost estimate should be well documented, comprehensive, accurate, and credible. A schedule should identify resources needed to do the work and account for how long all activities will take. Additionally, a schedule should identify relationships between sequenced activities.	●
Secure stable funding that matches resources to requirements	Programs should make trade-offs as necessary when working in a constrained budget environment.	●
Demonstrate technology, design, and manufacturing maturity	Capabilities should be demonstrated and tested prior to system development, making a production decision, and formal operator acceptance.	◐
Utilize milestones and exit criteria	Milestones and exit criteria – specific accomplishments that demonstrate progress – should be used to determine that a program has developed required and appropriate knowledge prior to a program moving forward to the next acquisition phase.	◐
Establish an adequate workforce	Acquisition personnel should have appropriate qualifications and experience. Program managers should stay on until the end of an acquisition life-cycle phase to assure accountability. Government and contractor staff should also remain consistent.	◐

Legend: ● DHS policy reflects key practices; ● DHS policy substantially reflects key practices; ◐ DHS policy partially reflects key practices.

Source: GAO analysis of DHS acquisition policy.

⁶GAO-12-833. See app. II of the report for a discussion of the key acquisition management practices.

Note: Appendixes I and II in our report, *Homeland Security: DHS Requires More Disciplined Investment Management to Help Meet Mission Needs*, GAO-12-833 (Washington, D.C.: Sept. 18, 2012), present a more detailed description of key program-management practices and how we assessed them.

As the table indicates, there are three areas where DHS could further enhance acquisition oversight: demonstrating technology, design, and manufacturing maturity; utilizing milestones and exit criteria; and establishing an adequate workforce. DHS officials generally acknowledged that DHS has opportunities to strengthen its program-management guidance and reported they are currently updating their acquisition policy. Furthermore, implementing our recommendation to ensure that all major acquisition programs fully comply with this policy, with which DHS concurred, should help the department strengthen its acquisition management activities.

In another example, with regard to IT management, we reported in July 2012, that DHS has defined a vision for a new governance process for its IT investments that includes a tiered oversight structure, among other things.⁷ We reported that this new framework and associated policies are generally consistent with Office of Management and Budget (OMB) guidance and best practices identified in our IT investment management framework.⁸ However, DHS's framework had not yet been finalized. In our report, we also identified recognized best practices for implementing the new framework, which include obtaining organizational buy-in involving all key stakeholders, establishing an implementation team and plan, and developing measures to assess progress in meeting objectives and establishing mechanisms to document lessons learned.⁹ We also reported that DHS had begun to implement aspects of its new governance process but had not fully followed these best practices in implementing the process. For example, the department had not developed an implementation plan, fully documented performance measures, or developed mechanisms for capturing lessons learned.

In his March 19 statement, the DHS CIO described elements of the department's new governance process. Among other things, the new governance structure is to provide additional oversight of certain programs or sets of related programs, particularly those rated at higher risk. According to the CIO, 16 programs that would immediately benefit from this additional oversight had already been identified. The CIO further stated that, as of March 2013, these programs have such oversight.

While these are steps in the right direction, we recommended in our July 2012 report that DHS finalize the policies and procedures associated with its new governance structure, ensuring that they fully address best practices from our IT investment management framework. We also recommended DHS fully follow best practices for implementing its new governance process. The department

⁷GAO, *Information Technology: DHS Needs to Further Define and Implement Its New Governance Process*, GAO-12-818 (Washington, D.C.: July 25, 2012).

⁸GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

⁹These practices were drawn from GAO reports, OMB guidance, and guidance from recognized experts in IT governance, including the IT Governance Institute, Gartner, IBM, and Oracle.

agreed with these recommendations, stating that it would implement them by September 30, 2013.

In addition, we reported in October 2012 that DHS had approximately 40 major IT investments that were rated as medium, moderately high, or high risk on OMB's IT Dashboard as of March 2012.¹⁰ This suggests that there are many more investments that require additional oversight. If fully and effectively implemented, DHS's new governance process should yield significant improvements in its IT investment management.

¹⁰GAO, *Information Technology Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies*, GAO-13-98 (Washington, D.C.: Oct. 16, 2012).

**Post-Hearing Questions for the Record
Submitted to the Honorable Jane Holl Lute
From Senator Thomas R. Carper**

**“The Department of Homeland Security at 10 Years: A Progress Report on
Management”
March 21, 2013**

Question#:	1
Topic:	major programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony, you indicated that DHS is beginning to change the culture regarding management and oversight of the major programs. What specifically are the next steps that the Department will be taking in improving the management of the department? GAO recommends that the Department track and independently validate the effectiveness and sustainability of the management improvements that have been made. How will you do that? What types of reports will be available to this committee so that we can monitor the progress as it is occurring?

Response: The Department has a clear plan and next steps to improve management at DHS. Since 2010, the Under Secretary for Management (USM) has focused on institutionalizing more rigor and accountability into the Department’s management culture. The Integrated Strategy for High Risk Management (2011) serves as a roadmap for continuous improvement by setting forth clear and comprehensive action plans and outcomes to improve management across the Department. As indicated in previous testimony, the first phase of the five-year plan was to standardize and strengthen the policies, processes, and systems that support the management and oversight of the Department’s major programs.

We are pleased that GAO has recently acknowledged that the Department has made substantial progress to enhance its management culture. In a recent report published in February 2013, GAO noted, “Important strides have been made to strengthen the department’s management functions and in integrating those functions across the department, particularly in recent years.” GAO added, “If implemented and sustained, the [Integrated Strategy] provides a path for DHS to be removed from the High Risk list.” (Government Accountability Office, High Risk Series, An Update)

Question#:	1
Topic:	major programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

In June 2013, the USM issued the fifth update to the Department's Integrated Strategy for High Risk Management. This report will build upon previous action plans to further enhance management across the Department.

In December 2010, the USM established several management improvement initiatives across the functional lines-of business (LOB) to address the 31 High Risk Outcomes published by GAO in September 2010. Every six months since December 2010, the Department has published a comprehensive update with detailed corrective action plans. For each update, GAO has independently validated the Department's progress to fully address each of those outcomes. As indicated earlier, GAO has acknowledged the Department's substantial progress in improving management since 2010.

Each LOB will continue to meet regularly with GAO to demonstrate the effectiveness and sustainability of their key initiatives.

We are also in the final stages of developing a Management Health Assessment (MHA) tool that will consistently and objectively track performance and capability across MGMT LOBs. This assessment of key health measures will allow leadership to diagnose performance issues before they become major challenges, as well as ensure greater integration and accountability by standardizing reporting requirements across the Department. In addition to the MHA, Chief Executive Officers within MGMT have been using specialized performance scorecards for measuring Components' performance related to the areas of efficiency, effectiveness and stakeholder satisfaction. For example, the Office of the Chief Financial Officer uses a Financial Management Health Assessment with 46 key measures across nine functional areas, and the Office of the Chief Procurement Office uses a Procurement Health Assessment with 30 measures.

The Department actively tracks and measures the performance of acquisition programs and reports status through the Comprehensive Acquisition Status Report (CASR), Quarterly Program Accountability Report (QPAR), and Exhibit 300. The CASR is an annual report required by statute and supports the President's annual budget submission to Congress. It includes information on key aspects of program management including cost, schedule, performance, funding, risks, contracts, key events, and lifecycle cost estimates. The QPAR provides senior leadership, Component Acquisition Executives, and program managers with visibility into potential issues regarding Component acquisition program performance before they escalate. Further, the Exhibit 300 captures data on the performance and management of the Department's IT investments. The data from the report is used to support the Administration's IT Dashboard initiative.

Question#:	1
Topic:	major programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Additionally, the Department ensures monitoring of management improvement efforts through various other reporting mechanisms across DHS management functions. For example, the annual Human Capital Management Report contains a summary of human capital activities and programs conducted during the fiscal year and the impact on organizational performance. DHS also uses the Federal Employee Viewpoint Survey results, reported annually to Congress and the public, to monitor human capital management, and focus on employee engagement and leadership development efforts.

DHS publishes annual performance and accountability reports, including the Annual Financial Report and the Annual Performance Report, which enable the President, Congress and the public to assess the effectiveness of the Department's mission performance and stewardship of resources. Included in the Annual Financial Report are the Independent Auditor's Report, the Financial Statements, and other accompanying information (e.g., management assurances and major management challenges).

DHS also regularly reports key performance measures such as improper payment rate, employee retention, and real property savings to OMB and the public via the www.performance.gov web page. Further, the committee can monitor DHS progress at the www.USASpending.gov web page where the Department regularly reports procurement and financial assistance obligation data to the public.

Question#:	2
Topic:	sequestration
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: With the tough fiscal environment and the impact of sequestration on the Department's management entities, will you be able to sustain and improve upon the vital management progress that has been made in the past 5 years?

Response: Since 2009, DHS has made great strides in our continued efforts to strengthen our management lines-of-business and enhance our management capabilities throughout the Department. Our priorities for FY 2013 and beyond remain focused on enhancements to financial management, acquisition, and workforce improvements. With over \$4 billion in efficiency savings and cost avoidances, DHS has made significant strides to streamline the cost of operating the Department, which has allowed us to focus our resources on improving our mission related priorities. We cite the U.S. Government Accountability Office's acknowledgement of our "significant" management progress as a testament to the men and women in the DHS management chain who have demonstrated their commitment to build an improved DHS.

The challenge for DHS under the current tough fiscal environment is ensuring that we continue to focus on and receive congressional support for sustaining the management improvements and documented progress we've made to date. Our ability to provide oversight to all of our acquisition programs has been greatly enhanced, ensuring full consideration of the investment lifecycle costs of our programmatic investments. We have established and recorded sustainable procedures to ensure that the improvements we've made in acquisition will continue to support our priority mission needs for the foreseeable future. Our record of progress in the area of financial management has been noted, most notably, by our ability to achieve qualified audit opinions and make substantial progress on reducing our improper payments rate. We are well on our way to be able to achieve an unqualified audit opinion as a result.

However, the impact of sequestration does limit our ability to address several key management areas, namely the modernization of our financial systems, the training required to maintain an effective acquisition workforce, and the ability to sustain a clean audit status by limiting our ability to properly resource the activities needed to shore up the Department's financial workforce through selected hiring and training activities. With \$4 billion in efficiencies and cost avoidances already achieved across the Department since 2009, an arbitrary additional 5 percent cut to our management accounts undermines our ability to prioritize and sustain the progress we've made.

Question#:	3
Topic:	improving management
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: Aside from budget pressures, what are the major obstacles to improving management at the Department? Are there any legislative authorities that you would recommend we change or institute for the Department that would enhance management and reduce risk?

Response: While there are budget pressures, the Department continues to sustain and enhance the progress made since 2009 to improve management. Further, no additional statutory changes are recommended at this time.

We are pleased by the February 2013 report from the Government Accountability Office (GAO) entitled "High Risk Series, An Update," which acknowledged that, "Important strides have been made to strengthen the department's management functions and in integrating those functions across the department, particularly in recent years. If implemented and sustained, [the Integrated Strategy for High Risk Management] provides a path for DHS to be removed from GAO's High Risk list."

The Management Directorate plans to publish the 5th update to its Integrated Strategy for High Risk Management in June. This update demonstrates the Department's commitment to sustaining progress in an effort to "fully address" each of GAO's recommendations and outcomes.

Question#:	4
Topic:	program cost
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: We continue to hear criticism of the department's ability to estimate program cost and prevent cost overruns. What is your management team doing to improve cost analyses, and to strengthen the oversight over major acquisitions, so that we see better results and fewer cost increases in major programs?

Response: In an effort to contain and prevent cost growth in our major acquisition programs, DHS has instituted a variety of measures to ensure efficiency and mitigate risk. In 2010, DHS implemented Acquisition Management Directive (MD) 102-01, which requires major acquisitions to demonstrate appropriate planning in order to receive approval to move through the acquisition lifecycle. To ensure program managers are executing within cost and schedule parameters and to prevent potential cost growth, every program is required to receive approval from the Acquisition Review Board (ARB) before proceeding to the next phase of the acquisition life cycle, such as moving from development to production. Part of this process includes the development of an Acquisition Program Baseline (APB). The APB documents the fundamental agreement on critical program cost, schedule, and performance objectives between the Program Manager (PM), the Component Head, and the DHS Acquisition Decision Authority (ADA). The APB's scope encompasses the entire planned execution of the program. Its cost parameters trace back to an approved Life Cycle Cost Estimate (LCCE) that documents the program's critical cost parameters in measureable, quantitative terms. The LCCE affords the Department the ability to track actual program performance against a formal baseline.

In practical terms, the APB is the "contract" between the Acquisition Decision Authority (ADA) and the Component on what will be delivered, how it will perform, when it will be delivered, and what it will cost. Should a program or project fail to meet any cost, schedule, or performance threshold in the APB the Program Manager must submit a remediation plan to the Department within 30 days explaining circumstances of the breach and proposing corrective action. Within 90 days of the breach the program should either be back within approved APB parameters; undergo a re-baseline of the breached parameters and have a new APB approved or partake in a program review with the ADA to review any proposed baseline revisions and recommendations.

In addition to ARB reviews at major milestones, DHS actively tracks and measures actual program performance via monthly reporting and oversight mechanisms such as the Comprehensive Acquisition Status Report, Quarterly Program Accountability Report, and Exhibit 300. This oversight provides an early alert to potential problems, such as cost growth or requirements creep, and, as a result, the Department can take corrective action by engaging the Component or program.

Question#:	4
Topic:	program cost
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

As a result of these oversight processes, the Under Secretary for Management (USM) is able to direct improvements to inadequate program plans before allowing them to proceed. By requiring programs to update their estimates to reflect changes in scope and schedule DHS is not only able to track program performance against a baseline but also proactively engage a program if potential problems are identified.

The Department has implemented several improvements to the quality and reliability of the cost estimating discipline across DHS. In 2011, the USM established the CE&A COE, through the Office of Program Accountability and Risk Management (PARM), to provide best practices and guidance for development of all cost estimates and cost analyses in the Department. The COE has identified and obtained best-in-class cost estimating tools and standardized operating models that have been disseminated to the Components. By providing cost estimating subject matter expertise to assist DHS Components and program managers, the number of DHS-approved LCCEs has significantly increased over the last year. This allows DHS to better articulate required funding needs and more effectively ascertain impacts to program scope should budget be changed.

The COE has developed and implemented a LCCE scorecard to systematically analyze the quality of LCCEs based on best practices identified by the GAO. The TECS Modernization system, as evidenced in their rebaselining efforts, exemplifies the value of both the scorecard and COE support to develop a reliable LCCE.

DHS has also increased the number of Level III Certified Cost Estimators by 50 percent. Level III, the highest level certification, represents a senior level mastery of the knowledge and skills associated with the complexities of cost estimating. DHS is institutionalizing the cost estimating discipline across the Department by embedding experienced certified cost estimators into major operational Components via the CE&A COE.

These cost estimators provide consistent application of GAO best practices and establish cost estimating standard operating procedures at the Component level. In addition to the added focus on accountability, risk, and oversight through the establishment of PARM, the changes have significantly enhanced the maturity of the Department, particularly in this discipline. These tools and practices provide a robust foundation upon which to build a culture of cost estimation within DHS which, in turn, increases the reliability of cost estimates across the Department.

Question#:	5
Topic:	best places to work
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: The non-profit Partnership for Public Service recently issued its 2012 Best Places to Work in the Federal Government rankings, which offers the most comprehensive assessment of how federal employees view their jobs and workplaces. The Department of Homeland Security ranked last among major federal agencies. What do you think are the root causes of that low rating and what is the Department doing to improve morale?

Response: The Department of Homeland Security (DHS) takes the assessment and rating of the 2012 Best Places to Work in the Federal Government very seriously. The Department has been working to enhance employee engagement and morale.

The DHS Management Directorate's Office of the Chief Human Capital Officer analyzed the 2012 Federal Employee Viewpoint Survey data to gain insight into root causes of decreased employee morale. This analysis determined that DHS should focus efforts to improve employee performance and recognition, leadership and supervision, communication, and work/life balance.

These findings were used to develop a three-pronged strategy to improve employee engagement, which are currently underway:

1. The Secretary appointed an Employee Engagement Executive Steering Committee (EE ESC) to oversee the DHS Employee Engagement Action Plan, which was submitted to OPM and OMB in January 2013. The EE ESC ensures that the objectives within the DHS Employee Engagement Action Plan are carried out within the Components. The Committee is focused on developing an Employee Engagement Communications Strategy, ensuring that Component employee engagement actions plans are reviewed and strengthened, ensuring that engagement issues are discussed with our union partners in Labor Management Forums, and evaluating promising internal and external solutions for adoption across the Department. In addition, the Plan also includes initiatives for leadership development, soliciting employee feedback, and encouraging work-life balance.
2. The Department-wide Leader Development Framework is a systematic and strategic approach to strengthening leadership skills throughout the DHS workforce. Accomplishments of the Leader Development Framework include: the 2012 rollout of the Cornerstone program for first line supervisors; a pilot of a Capstone program for new Senior Executives and Coast Guard admirals; the

Question#:	5
Topic:	best places to work
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

graduation of the first DHS SES Candidate Development Program; and the DHS Fellows Program, which was established in 2007 and is currently hosting its seventh cohort of GS-14 and GS-15 Department employees.

3. Developing and leading efforts related to employee communication, training, emphasis on diversity and inclusion, and employee recognition. An example of this approach is the DHS Diversity and Inclusion Strategic Plan. This strategic plan was developed through cross-Component collaboration with the objectives of securing a high-performing and diverse workforce; cultivating a culture of collaboration, flexibility and fairness; and institutionalizing diversity and inclusion through leadership commitment, accountability, and workforce engagement.

Question#:	6
Topic:	St. Elizabeths
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: What's the significance of the consolidation of headquarters at the St. Elizabeths campus to the operations of the Department – both in terms of management and mission? Do you see a path forward on St. Elizabeths through the tough fiscal environment?

Response: DHS's legacy facilities are currently scattered in over fifty locations throughout the National Capital Region (NCR), adversely impacting critical communication and coordination across DHS Components. To support the incident management and command-and- control requirements of our mission, it is vital to continue development of the DHS Consolidated Headquarters at St. Elizabeths Campus in a secure setting. Consolidation will allow the strategic realignment of the real property portfolio in the NCR to more effectively and efficiently support the DHS mission.

The collocation of the Secretary's Headquarters with Component Leadership will enhance command and control functions in the preparation for the response to natural disasters, terrorist attacks and other contingencies. This integrated approach will allow DHS to effectively communicate and engage in critical events as they occur and share such information to help secure America. In addition, consolidation will contribute to reduced facility costs and provide quality workspace to attract and retain the best professional workforce. We will optimize the real estate portfolio by increasing utilization efficiency integrating mobile workplace strategies.

The FY 2014 request continues the St. Elizabeths development with the renovation of the Center Building Complex to house the Secretary's Office and the Department's executive leadership, several hundred headquarters staff, and key leadership functions for command/control and daily operations of the Department. This request represents a revised approach to the build-out of the St. Elizabeths campus from the original plan, reflecting the realities of the current budget environment. Instead of requesting large development segments of 1 million square feet or more, the revised development plan is based on market-sized segments of approximately 300,000 square feet that are funded as a complete severable segment. There is no reliance on the uncertainty of future funding to complete work already started, as was the case with the Phase 1 project for the U.S. Coast Guard Headquarters.

Question#:	6
Topic:	St. Elizabeths
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

The revised plan acknowledges the challenges of the federal budget environment and presents a viable path to complete this critically important departmental initiative to enhance command, control, planning and response to functions of the Department.

**Post-Hearing Questions for the Record
Submitted to the Honorable Jane Holl Lute
From Senator Tom A. Coburn**

**“The Department of Homeland Security at 10 Years: A Progress Report on
Management”
March 21, 2013**

Question: In your written statement, you noted that DHS had identified more than \$4 billion in cost avoidances and implemented more than 45 efficiency initiatives as a result of the department-wide Efficiency Review. Please provide a list, by component, of all of the efficiency initiatives identified through this review, the total potential cost savings identified through each initiative, the total cost savings realized to date, and an indication of whether DHS plans to return funds to the Treasury, request fewer funds in the FY14 budget request, or has reprioritized the funding towards other uses.

Response: Since the beginning of this Administration, the Department of Homeland Security (DHS) has made an unprecedented commitment to efficiency and has implemented several initiatives to reduce costs, share resources across Components, and consolidate and streamline operations wherever possible in order to best support our frontline operations and build a culture of fiscal discipline and accountability at DHS.

With the launch of Secretary Napolitano’s Department-wide Efficiency Review (ER) in March 2009, DHS has been proactive in promoting efficiency throughout the Department. We have changed the way DHS does business, identifying over \$4 billion in cost avoidances by streamlining operations and fostering a culture of greater transparency, accountability and fiscal discipline through 46 ER initiatives and other Department-wide initiatives. DHS has redeployed these cost avoidances to mission-critical operations across the Department.

All DHS ER initiatives are implemented department-wide. A listing of the 46 DHS ER initiatives is attached.

Cost avoidances for the DHS ER initiatives, other DHS-wide initiatives, and Component-specific efficiency efforts are listed in the attached table. The initiatives are grouped by cost avoidance category. The table lists cost avoidances achieved from FY 2009 – FY 2012, as well as those that are projected through FY 2015 and outyears.



Efficiency Review Initiatives

DHS Efficiency Review					
Initiatives					
Launch Date					
April 17, 2009	Eliminate non-mission critical travel; maximize use of conference calls and web-based training and meetings	Consolidate subscriptions to professional publications and newspapers	Eliminate printing and distribution of all reports and documents that can be sent electronically or posted online	Maximize usage of government office space for meetings and conferences in place of renting facilities	
May 27, 2009	Implement an electronic tracking tool for fleet usage data to identify opportunities for alternative fuel usage; heighten vigilance for fraud, waste or abuse; and optimize fleet management	Conduct an assessment of the number of full-time and part-time employees and contractors to better manage our workforce	Utilize refurbished IT equipment and redeploy the current inventory throughout DHS	Leverage buying power to acquire software licenses for department-wide usage	Eliminate all external contracts for the design and production of new seals and logos
June 26, 2009	Develop cross-component training opportunities for employees	Develop a process for obtaining preliminary applicant security background data for candidates referred for final consideration	As replacements are needed, convert new printers/faxes/copiers into all-in-one machines	Streamline decision-making processes in headquarters offices to eliminate redundancies	Increase usage of DHS-wide blanket purchase agreements for office supplies
July 24, 2009	Establish a plan to ensure the DHS workforce has employees sufficient in number and skill to deliver our core mission	Initiate acquisition/leasing of hybrid vehicles for administrative use and alternative-fuel vehicles in cases where hybrids are not feasible	Implement energy efficiencies in all facility management projects	Standardize content for new-employee orientation and mandatory annual training modules DHS-wide	Increase coordination across all headquarters and operating Components



Efficiency Review Initiatives

DHS Efficiency Review				
Initiatives				
Launch Date	Initiatives			
April 7, 2010	Implement paperless earning and leave statements (ELS) DHS-wide			
July 8, 2010	Establish a DHS-wide sourcing vehicle for the acquisition of non-military uniforms	Establish a DHS-wide sourcing vehicle for the acquisition of tactical communications equipment and services	Establish a DHS-wide sourcing vehicle for the acquisition of wireless communication devices and services	Establish a DHS-wide sourcing vehicle for the acquisition of furniture in the National Capital Region (NCR)
August 5, 2010	Increase usage of DHS-wide contracting vehicles for background investigations	Establish a DHS-wide vehicle for purchasing bulk fuel for fleet, aircraft, and marine vessels	Reduce DHS expenditures on DHS contractor background investigations	Improve energy management in DHS by maximizing opportunities to reduce energy consumption at DHS-owned facilities
December 20, 2010	Develop and execute a customer-focused strategy for web-content management and web-hosting services for all DHS public-facing websites			
	Conduct annual optimization and validation of personal wireless communication services and devices DHS-wide			



Efficiency Review Initiatives

DHS Efficiency Review			
Initiatives			
Launch Date			
June 1, 2011	Establish a system and supporting processes for posting all notifications of seized property pending forfeiture online rather than in print media		
July 13, 2011	Establish a DHS Center of Excellence responsible for administration of alternatively financed energy savings contracts within the Department	Establish and implement a DHS Integrated Facility Assessment (IFA) Center of Excellence (COE) to develop and manage an integrated approach to facility condition assessments, systems lifecycle assessments, facility energy audits and analyses, water conservation assessments, and building and systems commissioning/recommissioning across DHS Component facilities	
February 7, 2012	Establish national negotiated discounts for the acquisition of vehicle maintenance services	Identify DHS-wide solutions for the limited availability of operational briefing, rehearsal and staging areas and use-of-force training facilities	Expand usage of the Department-wide process for transferring unused enterprise software licenses
	Implement the coordinated, enterprise-level submission of records disposition requests for common functions across the Department	Establish a DHS-wide sourcing vehicle for the acquisition of intelligence services	Implement agreements to facilitate cross-Component transfer of excess aviation equipment and establish cross-Component maintenance teaming agreements for aviation assets



Efficiency Review Initiatives

DHS Efficiency Review Initiatives	
Launch Date	Initiatives
June 20, 2012	Establish a portfolio of strategically sourced contract vehicles and other vehicles, such as Inter-Agency Agreements (IAAs) for the acquisition of language services
October 17, 2012	Maximize the usage of DHS training facilities through improved information sharing.

DHS Cost Avoidances by Category
As of September 2013

Category	FY2009	FY2010	Total FY2011	FY2012	FY2013	FY2014	FY2015	Outyears	Total
Aviation	\$0	\$0	\$0	\$962,181	\$0	\$0	\$0	\$0	\$962,181
Background Investigations Contract	\$1,600,000	\$2,360,340	\$0	\$568,970	\$63,416	\$0	\$0	\$0	\$4,592,726
Contract Management	\$798,135	\$5,064,283	\$6,543,744	\$1,490,003	\$1,000,000	\$1,000,000	\$0	\$0	\$15,897,065
Contractor Conversion	\$0	\$13,650,000	\$28,025,000	\$38,868,000	\$98,868,000	\$0	\$0	\$0	\$119,411,000
Energy Efficiencies	\$44,800	\$4,311,615	\$7,542,546	\$5,748,043	\$524,349	\$411,442	\$418,509	\$1,329,336	\$19,830,640
ER Blanket Purchase Agreements	\$15,972,006	\$66,303,379	\$101,003,787	\$201,545,020	\$49,103,332	\$14,950,000	\$14,950,000	\$26,800,000	\$496,627,524
Facilities	\$1,511,789	\$2,130,386	\$1,107,852	\$3,764,370	\$3,679,856	\$0	\$0	\$0	\$11,194,253
Fleet Management	\$294,582	\$1,066,322	\$5,848,488	\$19,830,687	\$35,534,375	\$19,829,557	\$19,829,557	\$4,972,404	\$107,205,952
Hiring/Background Investigations process	\$8,632,395	\$80,587,109	\$189,766,176	\$51,598,688	\$0	\$0	\$0	\$0	\$330,584,768
IT Equipment Management	\$3,288,871	\$2,699,311	\$10,978,737	\$6,364,337	\$5,513,809	\$0	\$0	\$0	\$28,845,585
Multi-Functional Devices (MFDs)	(\$930,798)	\$3,093,700	\$2,637,630	\$1,195,000	\$947,493	\$0	\$0	\$0	\$6,943,025
Mission/Component Specific	\$1,356,331	\$3,862,000	\$3,750,500	\$2,397,000	\$1,852,000	\$1,852,000	\$8,000,000	\$0	\$23,069,831
Non-ER Blanket Purchase Agreements	\$0	\$0	\$2,800,000	\$9,000,000	\$9,000,000	\$0	\$0	\$0	\$20,800,000
Non-IT Equipment Management	\$459,000	\$392,832	\$1,130,996	\$423,100	\$1,953,282	\$167,100	\$167,100	\$137,100	\$4,830,510
Other Identified DHS-wide Cost Avoidances (non-ER)	\$0	\$650,831,272	\$887,988,895	\$405,138,000	\$779,032,000	\$30,000	\$30,000	\$0	\$2,723,070,157
Paperless Earning and Leave Statement	\$104,763	\$260,859	\$1,476,238	\$1,466,350	\$0	\$0	\$0	\$0	\$3,308,200
Printing/Reproduction	\$5,243,878	(\$2,816,512)	\$1,050,131	\$1,489,901	\$1,177,662	\$0	\$0	\$0	\$6,145,040
Process Improvement	\$1,150,000	\$1,072,487	\$2,847,485	\$2,838,451	\$5,172,419	\$5,579,020	\$3,765,818	\$249,000	\$22,674,680
Property Management	\$7,000	\$2,509,529	\$540,539	\$523,529	\$523,529	\$523,529	\$523,529	\$5,758,836	\$10,910,000
Software License Transfers	\$0	\$0	\$0	\$169,566	\$943,748	\$0	\$0	\$0	\$1,133,414
Subscriptions	\$7,160	\$2,003,205	\$2,000,000	\$3,000,000	\$0	\$0	\$0	\$0	\$7,010,365
Training	\$1,211,945	\$333,965,056	\$212,019	\$261,493	\$98,317	\$0	\$0	\$0	\$335,768,830
Travel	\$2,490,209	(\$28,583,176)	\$19,430,604	\$1,291,301	\$2,148,702	\$0	\$0	\$0	\$16,777,690
Wireless Assets and Services	\$654,397	\$8,394,424	\$1,737,460	\$11,234,805	\$8,277,078	\$6,214	\$6,214	\$6,214	\$30,316,806
Total	\$63,896,463	\$1,151,138,451	\$1,278,418,798	\$770,730,195	\$945,413,367	\$44,348,862	\$47,690,727	\$39,252,880	\$4,344,909,743

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: At the hearing, you indicated that DHS has folded all of its existing major acquisition programs under the new acquisition policy.

Please provide a current list of all of DHS's major acquisition programs, along with an indication of where the program is in relation to the acquisition cycle.

Please indicate, for each program, whether the program has a current, DHS-approved Mission Needs Statement, Operational Requirements Document, Acquisition Program Baseline, Integrated Logistics Support Plan, and Test and Evaluation Master Plan. For instances in which the program does not have a current DHS-approved document, please provide an explanation as to why.

Response: The below list of FY 2012 Major Acquisition Oversight List Program answers the above requests. The table below provides this information. When a program has "Not required" as a response, this means that DHS waived the requirement for the documentation based on where the program was in its life cycle with DHS established MD 102-01. When a program has "Not applicable", that means the program is not at the stage where it is required or it is not required for that type of program.

Program - Project (P) - Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
1. CBP - Advance Passenger Information System (APIS)	IT	2	Support	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
2. CBP - Automated Commercial Environment (ACE) / International Trade Data System (ITDS)	IT	1	Obtain & Produce/ Deploy/ Support	Yes	No	Yes	No	No	In process of replanning. ADE-2A/B scheduled for July 27, 2013.

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOME LAND SECURITY (SENATE)

Program - Project (P) - Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
3. CBP - Automated Targeting System (ATS) Maintenance	IT	2	Support	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
4. CBP - Border Patrol Facilities	Non-IT	1	Mixed	No	No	No	No	Not Applicable	Operational Activity, currently being reviewed for removal from the major acquisition oversight list.
5. CBP - Facilities Management & Engineering Tactical Infrastructure (FM&E TI)	Non-IT	1	Mixed	No	No	No	Yes	Not Applicable	Operational Activity, currently being reviewed for removal from the major acquisition oversight list.
6. CBP - Infrastructure	IT	2	Support	No	No	No	No	Not Applicable	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
7. CBP - Integrated Fixed Towers (IFT)	IT/Mixed	2	Obtain	Yes	Yes	Yes	Yes	No	TEMP under development as of Oct 2012.
8. CBP - Land Border Integration (LBI)	IT	1	Support	Yes	Yes	Yes	Yes	Yes	Operational Activity, currently being reviewed for removal from the major acquisition oversight list.
9. CBP - OFO Facilities	Non-IT	2	Mixed	Yes	No	No	No	Not Applicable	Operational Activity, currently being reviewed for removal from the major acquisition oversight list.

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Program—Project (P)—Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
10. CBP - Mission Support Facilities	Non-IT	2	Support	No	No	No	No	Not Applicable	Recently added to Major Acquisition List.
11. CBP - Mobile Assets Program (MAP)	Non-IT	1	Support	No	No	No	No	Not Applicable	Operational Activity, being reviewed for removal from the major acquisition oversight list.
12. CBP - Non-Intrusive Inspection (NII) Systems Program	IT	1	Mixed	Yes	Yes	No	No	Not Applicable	During 2011 Program Review, program stated that APB, ILSP, and TEMP are under development.
13. CBP - SAP	IT	2	O&M	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
14. CBP - Strategic Air and Marine Plan (STAMP)	Non-IT	1	Obtain & Produce/ Deploy/ Support	Yes	No	No	No	No	The Department is working with CBP and the programs and will hold an Acquisition Review Board baseline the understanding of the programs.
15. CBP - Tactical Communication (TAC-COM) Modernization	IT	2	Mixed	Yes	Yes	No	No	No	Program is at ADE-1, so not required to provide the additional documents yet.
16. CBP - TFCS Modernization	IT	2	Mixed	Yes	Yes	Yes	Yes	Yes	
17. CBP - Transportation	Non-IT	3	Support	Yes	Yes	Yes	No	Not Applicable	

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Program – Project (P) – Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
18. DHS - A&O - Common Operational Picture (COP)	IT	2	Mixed	No	Yes	No	No	Not Applicable	The Department is working with the program to establish a baseline and create acquisition documentation.
19. DHS - CIO - Homeland Security Information Network (HSIN)	IT	2	Obtain & Produce/ Deploy/ Support	Yes	Yes	Yes	Yes	Yes	
20. DHS - CIO - Infrastructure Transformation Program (ITP)	IT	1	Mixed	Yes	Yes	Yes	Yes	Not Applicable	
21. DHS - DMO - HSPD-12	IT	2	Support	No	No	No	No	Not Applicable	Recently added to the FY12 MAOL.
22. DHS OCIO - Homeland Secure Data Network (HSDN)	IT	1	Support	Not Required	Not Required	Yes	Not Required	Not Required	
23. DHS- Next Generation Tactical Communication (NextGen TAC-COM)	IT	2	Need	Yes	Not Applicable	Not Applicable	Not Applicable	Not Applicable	
24. FEMA - Housing Inspection Services (HIS)	Non-IT	2	Support	Yes	Not Applicable	Yes	Not Applicable	Not Applicable	
25. FEMA - Infrastructure	IT	2	Mixed	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
26. FEMA - Integrated Public Alert and Warning System (IPAWS)	IT	2	Mixed	Yes	Yes	Yes	Yes	Yes	

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Program – Project (P) – Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
27. FEMA - Logistics Supply Chain Management System (LSCMS) (previously TAV)	IT	2	Mixed	Yes	Yes	Yes	Yes	Yes	
28. FEMA - Risk Mapping, Analysis and Planning (Risk Map)	Non-IT	1	Support	Yes	Not Required	Yes	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
29. FEMA - Software Application Development	IT	2	Support	No	No	No	No	No	Program is currently under review to determine whether this is a major acquisition, since acquisition is a service.
30. ICE - Air Charter Program (ACP)	Non-IT	2	Support	Not Applicable	Not Applicable	No	Not Applicable	Not Applicable	Program is a services program. The department is working with ICE and the program to develop and APB for future iterations.
31. ICE - Detention and Removal Operations (DRO)	Non-IT	2	Support	Not Applicable	Not Applicable	No	Not Applicable	Not Applicable	Program is a services program. The department is working with ICE and the program to develop and APB for future iterations.
32. ICE - Detention and Removal Operations (DROM)	IT	2	Obtain & Produce/ Deploy/ Support	Yes	No	No	No	No	Program documentation is under development at the Component level.
33. ICE - DRO Electronic Health Record (EHR) System	IT	2	Analyze/ Select	Yes	Yes	Yes	Yes	Yes	

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOME LAND SECURITY (SENATE)

Program - Project (P) - Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
34. ICE - Enforcement Information Sharing (EIS)	IT	2	Mixed	Yes	Yes	Yes	Yes	No	The Program does have a TEMP, but it was approved at the Component level. All major programs are required to have their TEMP approved by S&I.
35. ICE - Fleet Management Program (FMP)	Non-IT	2	Support	No	No	No	No	Not Applicable	Operational activity being removed from the Major Acquisition Oversight List.
36. ICE - IT Infrastructure	IT	1	Produce/ Deploy/ Support	Yes	Yes	Not Required	Yes	Not Required	MD 102-01 documentation waived, because this program was in full sustanment when policy was established.
37. ICE - Student & Exchange Visitor Information System (SEVIS I and II)	IT	2	Mixed	Yes	Yes	Yes	Yes	Yes	
38. ICE - TECS Modernization	IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
39. NPPD - Critical Infrastructure Technology & Architecture (CITA)	IT	2	Mixed Obtain & Produce/ Deploy/ Support	Yes	Yes	Yes	No	Not Applicable	CITA is not included on the FY13 MAOL. Projects that were continued in the CITA investments are now tracked as several investments.
40. NPPD - Federal Protective Services	Non-IT	2	Support	No	No	No	No	Not Applicable	Per MD-102, only AP required for an Enterprise Service Contract

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Program – Project (P) – Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
41. NPPD - National Cybersecurity & Protection System (NCPS)	IT	I	Mixed	Yes	Yes	Yes	Yes	Yes	
42. NPPD – Next Generation Network (NGN)	IT	I	Obtain	Yes	Yes	Yes	Yes	Yes	
43. NPPD - SAFECOM	Non-IT	I	Support	No	No	Yes	No	Not Applicable	Recently added to the DHS Major Acquisition Oversight List.
44. NPPD - United States Visitor and Immigrant Status Indicator Technology (US-VISIT)	IT	I	Mixed Obtain & Produce/ Deploy/ Support	Yes	Yes	Yes	Yes	Yes	
45. OHA - Bio Watch Gen-3	Non-IT	I	Obtain	Yes	Yes	No	Yes	Yes	BioWatch was required to perform an Analysis of Alternatives. A baseline cannot be established until that activity is completed.
46. S&T - National Bio and Agro-Defense Facility (NBAF)	Non-IT	I	Obtain	Yes	Yes	Yes	Yes	Not Applicable	
47. S&T - National Biodefense Analysis and Countermeasures Center (NBACC) Facility	Non-IT	I	Support	Yes	Yes	No	Yes	Not Applicable	Facility Completed ADE-3 and entered full sustainment.
48. TSA - Electronic Baggage Screening Program (EBSP)	Non-IT	I	Obtain & Produce/ Deploy/ Support	Yes	Yes	Yes	Yes	Yes	

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOME LAND SECURITY (SENATE)

Program – Project (P) – Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
49. TSA - HRAccess (P)	Non-IT	1	Support	Yes	Yes	Yes	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
50. TSA - Information Technology Infrastructure Program (ITIP)	IT	1	Support	Yes	Not Required	Yes	Not Required	Not Applicable	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
51. TSA - National Explosives Detection Canine Team Program (K9) System	Non-IT	2	Support	Yes	Not Required	Yes	Not Required	Not Applicable	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
52. TSA - Passenger Screening Program (PSP)	Non-IT	1	Obtain & Produce/ Deploy/ Support	Yes	Yes	Yes	Yes	Yes	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
53. TSA - Screening Partnership Program	Non-IT	1	Support	Yes	Not Required	Yes	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
54. TSA - Secure Flight	IT	1	Support	Yes	Yes	Yes	Yes	Yes	
55. TSA - Security Technology Integrated Program (STIP) (P)	IT	2	Mixed Obtain & Produce/ Deploy/ Support	Yes	Yes	Yes	Not Applicable	Yes	

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Program – Project (P) – Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
56. TSA - Transportation Worker Identification Credentialing (TWIC)	IT	1	Support	Yes	Not Required	Yes	Not Required	Yes	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
57. TSA - IT/AC Infrastructure Modernization Program (TIM)	IT	2	Obtain	Yes	Yes	Yes	Yes	Yes	
58. USCG - C4ISR	IT	1	Produce/Deploy	Yes	Yes	Yes	Yes	Yes	
59. USCG - CG Logistics Information Management System (CG-LIMS)	IT	2	Support	No	No	No	No	No	
60. USCG - Core Accounting System (CAS)	IT	2	Support	No	No	No	No	No	A new modernization effort is being started. The CAS system is in sustainment and will be phased out, so not cost effective to complete documentation.
61. USCG - Fast Response Cutter (FRC)	Non-IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
62. USCG - HC-130H Conversion/Sustainment Projects	Non-IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
63. USCG - HC-130J Fleet Introduction	Non-IT	2	Obtain	Yes	Yes	Yes	Yes	Yes	
64. USCG - HC-144A Maritime Patrol Aircraft (MPA)	Non-IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
65. USCG - HH-60 Conversion Projects	Non-IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Program – Project (P) – Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
66. USCG - HH-65 Conversion/Sustainment Projects	Non-IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
67. USCG - Infrastructure - CGOne	IT	2	Support	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
68. USCG - Infrastructure - SW/RS	IT	2	Support	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
69. USCG - Interagency Operations Centers (IOC)	IT	2	Analyze/Select	Yes	Yes	Yes	Yes	Yes	
70. USCG - Medium Endurance Cutter Sustainment	Non-IT	1	Produce/Deploy	No	No	Yes	No	No	Program is a sustainment program of an existing asset.
71. USCG - National Security Cutter (NSC)	Non-IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
72. USCG - Nationwide Automatic Identification System (NAIS)	IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
73. USCG - Offshore Patrol Cutter (OPC)	Non-IT	1	Obtain	Yes	Yes	Yes	Yes	Yes	
74. USCG - Rescue 21	IT	1	Support	Yes	Yes	Yes	Yes	Yes	
75. USCG - Response Boat - Medium (RB-M)	Non-IT	1	Produce/Deploy	Yes	Yes	Yes	Yes	Yes	
76. USCG - Unmanned Aircraft Systems (UAS)	Non-IT	1	Need	Yes	Not Applicable	Not Applicable	Not Applicable	Not Applicable	

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOME LAND SECURITY (SENATE)

Program - Project (P) - Service (S)	IT or Non-IT	Level	Phase	MNS	ORD	APB	ILSP	TEMP	Explanation
77. USCIS - Application Support Centers (ASC)	Non-IT	2	Produce/ Deploy/ Support	Yes	No	Yes	No	Not Applicable	Recently added to DHS Major Acquisition Oversight List
78. USCIS - Benefits Provision - Verification Information System (VIS)	IT	2	Obtain & Produce/ Deploy/ Support	Yes	No	No	No	No	Program is being combined with another program. Documentation will be established for the combined program.
79. USCIS - Infrastructure (End User Support)	IT	2	Support	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
80. USCIS - Infrastructure (Enterprise)	IT	2	Support	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.
81. USCIS - Integrated Document Production (IDP)	IT	2	Support	Yes	No	Yes	No	Not Applicable	
82. USCIS - Transformation	IT	1	Produce/ Deploy/ Support	Yes	Yes	Yes	Yes	Yes	
83. USSS - Information Integration & Transformation (IIT)	IT	2	Obtain	Yes	Yes	Yes	Yes	Yes	
84. USSS - IT Infrastructure	IT	2	Support	Not Required	Not Required	Not Required	Not Required	Not Required	MD 102-01 documentation waived, because this program was in full sustainment when policy was established.

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide a table listing the program, date and subject of each acquisition review board meeting held since implementation of the current acquisition policy, along with a summary of the decisions made at the meeting.

Response: The list of Acquisition Review Boards since the signing of the Department's Acquisition Policy Directive, MD-102 (October 2011) is provided below.

	Component	Program	ARB DATE	Summary
1	TSA	Electronic Baggage Screening Program (EBSP)	11/4/2011	Acquisition Decision Event 3
2	TSA	Passenger Screening Program (PSP)	12/12/2011	Acquisition Decision Event 2B/2C
3	CBP	Integrated Fixed Towers (IFT)	1/25/2012	Acquisition Decision Event 2B/3
4	NPPD	Next Generation Network Priority Services (NGN-PS)	2/1/2012	Acquisition Decision Event 2B
5	NPPT	National Cybersecurity and Protection System (NCPs)	2/14/2012	Acquisition Decision Event 3
6	USCIS	Transformation	2/16/2012	Program Review for approval of funding for segment release
7	USCG	Offshore Patrol Cutter (OPC)	2/28/2012	Acquisition Decision Event 2A/2B
8	NPPD	National Cybersecurity and Protection System (NCPs)	4/25/2012	Program Review - Approve strategy change
9	NPPD	National Cybersecurity and Protection System (NCPs)	6/5/2012	Program Review - Contract award
10	USCIS	Transformation	6/26/2012	Program Review - Contract option period award

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Response: The list of Acquisition Review Boards since the signing of the Department's Acquisition Policy Directive, MD-102 (October 2011) is provided below.

	Component	Program	ARB DATE	Summary
1	TSA	Electronic Baggage Screening Program (EBSF)	11/4/2011	Acquisition Decision Event 3
2	TSA	Passenger Screening Program (PSP)	12/12/2011	Acquisition Decision Event 2B/2C
3	CBP	Integrated Fixed Towers (IFT)	1/25/2012	Acquisition Decision Event 2B/3
4	NPPD	Next Generation Network Priority Services (NGN-PS)	2/1/2012	Acquisition Decision Event 2B
5	NPPT	National Cybersecurity and Protection System (NCPS)	2/14/2012	Acquisition Decision Event 3
6	USCIS	Transformation	2/16/2012	Program Review for approval of funding for segment release
7	USCG	Offshore Patrol Cutter (OPC)	2/28/2012	Acquisition Decision Event 2A/2B
8	NPPD	National Cybersecurity and Protection System (NCPS)	4/25/2012	Program Review - Approve strategy change
9	NPPD	National Cybersecurity and Protection System (NCPS)	6/5/2012	Program Review - Contract award
10	USCIS	Transformation	6/26/2012	Program Review - Contract option period award

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

11	TSA	Passenger Screening Program (PSP)	7/3/2012	Program Review - Advanced Imaging Technology (AIT) Roadmap Acquisition Decision Event 2C
12	TSA	Electronic Baggage Screening Program (EBSP)	7/30/2012	
13	OHA	BioWatch Generation 3 (GEN 3)	8/16/2012	Program review - Return program for AoA and performance testing
14	USCG	Fast Response Cutter (FRC)	8/23/2012	Removal from breach; Acquisition Decision Event 2C
15	CBP	Automated Commercial Environment (ACE)	9/14/2012	Program Review - Breach remediation
16	NPPD	Continuous Diagnostics and Mitigation (CDM) Program	9/17/2012	Acquisition Decision Event 1
17	USCG	HC-144 Maritime Patrol Aircraft (MPA)	10/3/2012	Removal from breach; Acquisition Decision Event 3
18	CBP	TECS Modernization	11/16/2012	Removal from breach; Acquisition Decision Event 2B/C
19	CBP	Arizona Technology Plan	11/16/2012	Plan Briefing / Program Review
20	CBP	Automated Commercial Environment (ACE)	12/17/2012	Program review - approval for Agile pilot
21	TSA	Passenger Screening Program (PSP)	2/15/2013	Program review

Question: Please provide a listing of all major acquisition programs that have been terminated since implementation of the current acquisition policy.

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Response: The following programs have been terminated since the implementation of the current acquisition policy.

1. Advanced Spectroscopic Portal (ASP)
2. Strategic Border Initiative Network (SBINet)
3. Risk Assessment and Management Program (RAMP)
4. Transformation and Systems Consolidation (TASC)

Question: Please provide a listing of all major acquisition programs that the department currently considers to be problematic or high-risk, and describe the risk mitigation strategies being used to ensure that taxpayer funds are used wisely.

Response:

Component	Program	Risk Mitigation	DHS Reviews
CBP	Automated Commercial Environment (ACE)	To mitigate the risks associated with ACE, DHS has convened four Acquisition Review Board meetings regarding the ACE Program. DHS established an Executive Steering Committee (ESC) to provide ongoing senior-level oversight of ACE, including regular reviews of progress and activities of the Program. As of the September 14, 2012 Acquisition Review Board, ACE has been paused, preventing it from further spending on the development of new capabilities until the program has completed the necessary planning. The program is currently undergoing a re-baseline to include the release strategy, transition plan to agile development methodology, and restructuring of the Program Management Office. The ESC is convening every two weeks to oversee progress.	July 9, 2010 (ARB) September 30, 2011 (ARB for ESC chartering) September 14, 2012 (ARB) December 17, 2012 (ARB)

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Component	Program	Risk Mitigation	DHS Reviews
CBP	TECS Modernization	To mitigate the risks associated with TECS Mod, DHS has convened two Acquisition Review Board meetings regarding the TECS Mod Program. DHS established an Executive Steering Committee to provide ongoing senior-level oversight of TECS Mod, including regular reviews of progress and activities of the Program. The ARB re-baselined the program in November 2012.	October 19, 2010 (ARB) November 16, 2012 (ARB)
ICE	Student and Exchange Visitor Information System (SEVIS)	To mitigate the risks associated with SEVIS, DHS has convened three Acquisition Review Board meetings regarding the SEVIS Program. As of the December 19, 2012 Acquisition Review Board (ARB), the SEVIS II program has been paused. The ARB also confirmed the necessity for the SEVIS II breach status to remain in effect as well as prohibition to expend SEVIS II funds without direct Department approval. The Department concluded that action was required to restructure and refocus SEVIS and SEVIS II efforts.	July 15, 2010 (ARB) February 22, 2011 (ARB) June 28, 2012 (ARB – show cause review) December 19, 2012 (ARB)
NPPD	National Cybersecurity Protection System (NCPS)	To mitigate the risks associated with NCPS, DHS has convened six Acquisition Review Board meetings regarding the NCPS Program. DHS established Executive Steering Committees (ESCs) to provide ongoing senior-level oversight of NCPS, including regular reviews of progress and activities of the Programs. As a result of the ESC oversight, the program successfully awarded a contract to the first Internet Service Provider (ISP) in March 2013.	October 26, 2010 (ARB) March 30, 2011 (ARB) February 14, 2012 (ARB) April 25, 2012 (ARB) June 5, 2012 (ARB) February 20, 2013 (ARB)

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOME LAND SECURITY (SENATE)

Component	Program	Risk Mitigation	DHS Reviews
OHA	BioWatch Gen3	To mitigate the risks associated with the BioWatch Gen-3 acquisition, DHS has convened four Acquisition Review Board meetings regarding the BioWatch Gen-3 acquisition. The acquisition was returned for additional planning, including a technology demonstrator to determine technological feasibility and an alternatives analysis. As a result of the August 16, 2012 Acquisition Review Board (ARB), BioWatch has been paused, preventing it from further spending until the program has completed an additional Analysis of Alternatives (AOA) for department approval.	July 7, 2010 (ARB) December 3, 2010 (ARB) April 25, 2011 (ARB) August 16, 2012 (ARB)
TSA	Passenger Screening Program (PSP)	To mitigate the risks associated with PSP, DHS has convened five Acquisition Review Board reviews regarding the PSP Program. Cost variance is due to the vendor's ability to provide the capabilities required by the Program to meet requirements. To mitigate this variance, PSP solicits input from industry stakeholders in the requirements development process to ensure requirements are achievable in realistic timeframes.	May 19, 2010 (ARB) August 18, 2010 (ARB) December 12, 2011 (ARB) July 3, 2012 (ARB) February 15, 2013 (ARB)
TSA	TTAC Infrastructure Modernization (TIM)	To mitigate the risks associated with TIM, DHS has convened two Acquisition Review Board meetings regarding the TIM Program. DHS established an Executive Steering Committees (ESCs) to provide ongoing senior-level oversight of TIM, including regular reviews of progress and activities of the Programs. With the oversight of the ARB and ESC, the program has the proper independent verification and validation (IV&V) in place to ensure that the new system identifies gaps and that they are resolved. Historically the program has shown a cost and schedule variance, however the contract is in place, the development contractor is now onboard and the program is on track to achieve required milestones.	September 15, 2011 (ARB) September 30, 2011 (ARB for ESC chartering)

Question#:	8
Topic:	acquisition programs
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOME LAND SECURITY (SENATE)

Component	Program	Risk Mitigation	DHS Reviews
USCIS	Transformation	To mitigate the risks associated with Transformation, DHS has conducted four Acquisition Review Board (ARB) meetings regarding the Transformation Program. DHS established an Executive Steering Committee (ESC) to provide ongoing senior-level oversight of Transformation, including regular reviews of progress and activities of the Programs. At the Direction of the ARB, the Program has implemented agile development methodologies to assist with cost and schedule management.	June 21, 2011 (ARB) September 30, 2011 (ARB for ESC chartering) February 16, 2012 (ARB) June 26, 2012 (ARB)
TSA	Electronic Baggage Screening Program (EBSP)	To mitigate the risks associated with EBSP, DHS has convened 4 Acquisition Review Board meetings regarding EBSP. To mitigate risks, the Program coordinates with stakeholders to ensure testing and procurements run smoothly and meet airport checked baggage screening needs. The Program has also developed a Qualified Vendor Communication Plan to improve the communication and interaction of EBSP and the industry. Finally, the Program continues to meet the Congressional mandate to screen 100% of checked baggage.	May 19, 2010 (ARB) February 25, 2011 (ARB) November 4, 2011 (ARB) July 30, 2012 (ARB) April 20, 2012 (ADA Review)

Question#:	9
Topic:	US-VISIT program
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In an August 2012 report on the US-VISIT program, the DHS Inspector General found 825,000 instances in which the biographic data in the identification system did not match the associated fingerprints. The report stated that the program could not determine whether those instances indicated fraud. What actions has DHS taken to respond to the findings and recommendations included in this report?

Response: The Department of Homeland Security (DHS) Office of the Inspector General's (OIG) review identified 825,000 instances where the same fingerprints were associated with different biographic data within the Automated Biometric Information System (IDENT) managed by the DHS National Protection and Programs Directorate's (NPPD) Office of Biographic Identity Management (OBIM), formerly named the United States Visitor and Immigrant Status Indicator Technology Program. NPPD/OBIM concurred with the recommendation to review the data inconsistencies to determine if biographic fraud exists in this data set. While the OIG found most of the discrepancies were likely attributable to data collection errors, the OIG stated there were instances where it appeared individuals had supplied fraudulent biographic data at a port of entry.

NPPD/OBIM's analysis of the 825,000 instances found the number of potential fraud cases were lower than previously reported due to additional information received from OIG. NPPD/OBIM used an automated process to reduce the original 825,000 instances provided by OIG to a more targeted set of 10,791 potential fraud instances. The OIG auditors agreed with NPPD/OBIM's criteria to reduce the number of potential fraud instances. This reduction leaves a small percentage to be manually investigated for potential fraud, and these cases will be forwarded to appropriate law enforcement entities for investigation. Although it is difficult to estimate how long the different law enforcement entities will need to manually research their share of the 10,791 instances, OBIM should be able to provide a report showing the number of fraud cases based on this research and resulting actions in 3-4 months.

Question#:	10
Topic:	9/11 commission
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: A number of recommendations made by the 9/11 commission have not yet been implemented. For example, TSA is still struggling to implement an effective explosives detection capability. What is the current status of TSA's efforts to develop this capability and implement the 9/11 commission recommendation?

Response: The Department of Homeland Security (DHS) and its many partners within the Federal government, public and private sectors, and communities across the country have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds. Together, these efforts have provided a strong foundation to protect our communities while safeguarding the fundamental rights of all Americans and allowing the American way of life to thrive. See below for a chronology of the events that took place on September 11, 2001 and how DHS has addressed recommendations made by the 9/11 Commission:

September 11 Chronology

September 11, 2001	Today
In early 1999, Osama Bin Laden summoned operatives to Afghanistan to discuss using commercial aircraft as weapons and developed a list of potential targets in the United States.	Today, in concert with public and private sector partners as well as international allies, this Administration has developed a multi-layered information sharing security strategy to target and identify both known and unknown individuals that may pose a threat to the United States wherever the operational planning might occur with the goal of preventing such persons from entering the country.
In April of 1999, the hijackers began to obtain passports and visas for travel to the United States.	DHS and other federal partners have built a capacity to more extensively vet those individuals applying for visas or travel to the U.S. For example, through the Visa Security Program, which did not exist on 9/11 and is now operational at 20 posts in 20 countries, Immigration and Customs Enforcement, in conjunction with the State Department, deploys trained special agents overseas to high-risk visa activity posts to conduct targeted, in-depth reviews of particular visa applications and applicants before they reach the United States.
Between 1999 and 2001, many of the hijackers prepared for the 9/11 attack while living in Germany.	The Department of Homeland Security (DHS), in collaboration with the Departments of Justice and State, has signed Preventing and Combating Serious Crime Agreements with 39 countries, including Germany, to share information about terrorists and criminals.

Question#:	10
Topic:	9/11 commission
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

The hijackers began arriving in the U.S. in late April 2001 on tourist visas with cash and travelers checks acquired in the Middle East.	DHS partners with the Terrorist Screening Center, the National Counterterrorism Center and other federal entities to analyze travel-related data in order to better understand and anticipate the travel patterns of known or suspected terrorists. Today's travel related databases along with threat-related intelligence have been essential in identifying, targeting, and interdicting known and suspected terrorists as well as suspicious cargo before it enters the United States.
Prior to 9/11, the hijackers enrolled in flight schools and conducted cross-country surveillance flights in order to identify aircraft that would produce their desired impact.	The Transportation Security Administration (TSA) has responsibility for ensuring that foreign students seeking training at flight schools do not pose a threat to aviation or national security. TSA performs background checks, including government watchlist matching, a criminal history check, and an immigration status check.
During the spring and summer of 2001, several of the hijackers were apprehended by U.S. law enforcement for various traffic violations.	Today, 78 recognized fusion centers throughout the country serve as focal points at the state and local level for the receipt, analysis, gathering, and sharing of threat and vulnerability-related information. In addition, the Nationwide Suspicious Activity Reporting Initiative helps to train state and local law enforcement to recognize behaviors and indicators related to terrorism, crime and other threats while standardizing how those observations are analyzed and disseminated. Finally, state and local law enforcement officers can determine whether an individual is on a watchlist through the National Crime Information Center.
On the morning of 9/11, hijackers passed through security checkpoints at four U.S. airports, allegedly carrying knives, box cutters and concealed weapons on their person or in carry-on luggage.	Multilayered security measures are now in place to enhance aviation security including the prescreening of passengers; the deployment of new technologies; and training of airport security and law enforcement personnel to better detect behaviors associated with terrorism. Since 9/11, the capacity of frontline security personnel and new technologies has significantly expanded. Through Secure Flight, DHS now prescreens 100% of the approximately 14 million passengers flying weekly to, from, and within the U.S. against government watchlists. In addition, all checked and carry-on baggage is now screened for metallic and non-metallic threats by new technologies as well as over 52,000 transportation security officers at more than 450 airports across the country.
Although eight of the hijackers were randomly selected for additional screening and a gate agent flagged two as suspicious, none were prevented from boarding their flights on 9/11.	Today, TSA's Behavior Detection Officers utilize non-intrusive behavior observation and analysis techniques to identify potentially high-risk passengers who exhibit behaviors that indicate they may be a threat to aviation and/or transportation security and refer them for additional screening. TSA also conducts screening of passengers at boarding gates based on current intelligence and passengers of interest.

Question#:	10
Topic:	9/11 commission
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

At 8:19 AM, flight attendants and passengers began reporting hijackings of the aircraft via airphone.	Following 9/11, all commercial aircraft have been secured through the hardening of cockpit doors. In addition, the risk-based deployment of Federal Air Marshals, the Federal Flight Deck Officer program, in which eligible flight crewmembers are authorized by TSA to use firearms to defend against violence, and the crewmember behavior recognition and response training program, all provide additional layers of aviation security.
Throughout the morning of September 11, 2011, air traffic control operators, military personnel and first responders on the ground lacked situational awareness of what other agencies were doing to address the developing crisis.	Through the use of mobile and fixed site technologies, voice radio systems used by first responders are more interoperable than ever before. Since 9/11, the federal government has made significant organizational changes and investments in training and technical assistance to improve emergency communications capabilities. Moreover, the National Emergency Communications Plan and Incident Command System have established standardized plans, protocols, and procedures to improve command, control, and communications.

With respect to those recommendations addressed by the Transportation Security Administration (TSA), DHS has accelerated the deployment of new passenger and baggage screening technologies to detect the next generation of threats, including Advanced Imaging Technology (AIT) units, Explosives Detection Systems (EDS), Explosives Trace Detection (ETD) units, Advanced Technology (AT) X-Ray systems, and Bottled Liquids Scanners (BLS). Prior to 9/11, limited federal security requirements existed for cargo and baggage screening. Today, 100 percent of all checked and carry-on baggage is screened for explosives and TSA continually assesses intelligence to develop countermeasures in order to enhance its multiple layers of security at airports and onboard aircraft. In addition, while TSA does not conduct passenger screening abroad, it requires airports that serve as the last point of departure to the U.S. to meet stringent security standards.

Enhanced Screening Technologies

Advanced Imaging Technology

TSA began deploying AIT units in 2008, leading to the detection of hundreds of prohibited, illegal or dangerous items at checkpoints nationwide. AIT safely screens passengers for metallic and nonmetallic threats, including weapons, explosives and other objects concealed under layers of clothing. AIT has been evaluated and determined to be safe for all passengers by the Food and Drug Administration, National Institute for Standards and Technology, and Johns Hopkins University Applied Physics Laboratory. TSA ensures passenger privacy through Automated Target Recognition (ATR) software on millimeter wave AIT units, which automatically detects potential threats using a

Question#:	10
Topic:	9/11 commission
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

generic outline of a person for all passengers. AIT units without the ATR capability were removed from airports by June 1, 2013 in order to comply with the Federal Aviation Administration Modernization and Reform Act of 2012 mandate. ATR will be installed on all future procurements of AIT units.

Explosives Trace Detection

ETD units are used by TSOs to screen carry-on articles, checked baggage, and passengers for explosive residue. A swab is used to collect samples, which are electronically analyzed for traces of explosive residue or vapor.

Advanced Technology X-Ray

AT X-Ray machines scan carry-on baggage from multiple angles, providing the operator with a clear image regardless of the bag's orientation within the machine.

Bottled Liquid Scanners

BLS are hand-held or bench-top devices which are capable of detecting explosives and flammable liquids.

Explosives Detection Systems

TSA screens 100 percent of all checked baggage for explosives. Through a sophisticated analysis of each checked bag, EDS can quickly and effectively determine if a bag contains a potential threat.

Canines

TSA's National Explosives Detection Canine Team Program (NEDCTP) deploys canine teams to screen air cargo at the nation's highest cargo volume airports. All of the original 120 Agency-Led Cargo Canine Teams have been allocated and deployed and the NEDCTP is currently training teams to account for 19 vacancies resulting from attrition. Additionally, the NEDCTP provides explosives detection canine capabilities in the aviation, mass transit, and maritime transportation sectors. The NEDCTP has grown from 200 explosives detection canine teams in 2001 to 921 in 2013. TSA has also developed a Passenger Screening Canine program to utilize a canine's ability to detect explosive odors emanating from items worn or carried by a person.

Cargo Security

Prior to 9/11, no federal security requirements existed for cargo screening. Now, 100 percent of all cargo transported on passenger aircraft that depart U.S. airports is screened commensurate with screening of passenger checked baggage. This was accomplished

Question#:	10
Topic:	9/11 commission
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

largely through the Certified Cargo Screening Program, which permits entities that have undergone rigorous inspection and certification processes throughout the air cargo supply chain, to use qualified explosive detection technologies to screen cargo prior to it being tendered for transport on passenger aircraft. In December 2012, TSA implemented requirements for 100 percent screening of international inbound cargo transported on passenger aircraft. TSA also requires 100 percent screening of any cargo shipments identified as high-risk cargo transported on all-cargo aircraft international flights inbound to the United States. As part of this effort, TSA works with industry to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process, which certifies foreign aviation security programs that are commensurate with TSA standards. As of September 2013, TSA has recognized the NCSPs of 38 countries. TSA also works jointly with U.S. Customs and Border Protection on the Air Cargo Advanced Screening (ACAS) Pilot initiative, which is a partnership with industry to identify and mitigate, through risk assessment, high risk air cargo shipments prior to loading inbound to the United States.

Question#:	11
Topic:	grants
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: With regard to DHS' preparedness grants, you stated that DHS is improving in its ability to track what federal funds are spent on.

Please describe the current status of the department's efforts to track what preparedness grant funds are spent on, and measure the effectiveness of those grants.

Response: FEMA's Grant Programs Directorate has several mechanisms to track grant spending and programmatic implementation of the grants. FEMA requires grantees to submit quarterly financial reports for each grant. These reports provide information on funding expended, funding remaining, and financial obligations of the grant. In addition, FEMA requires grantees to submit semi-annual progress reports on how they are implementing their grants. The semi-annual reports also contain data on grant expenditures. Federal program analysts review the semi-annual progress reports to determine if the grantee is having any challenges in implementing their grant program. Finally, Federal program analysts monitor grantees. Both desk reviews and on-site monitoring include reviews of financial and programmatic data to ensure that grantees are making sufficient progress in implementing their grant programs.

FEMA has made substantial progress over the past year in measuring the effectiveness of DHS preparedness grants. The National Preparedness Goal (the Goal) and the National Preparedness System serve as the framework for assessing grant effectiveness.

FEMA's strategy for developing metrics and assessing grant performance begins with the Goal. The Goal defines the core capabilities necessary to prepare for the threats and hazards that pose the greatest risk to the security of the Nation, and it includes concrete, measurable objectives to manage that risk. The Goal's capability targets provide concrete statements of the Nation's requirements in each core capability.

As part of the National Preparedness System, FEMA has developed or is leveraging performance assessments that measure progress toward achieving the Goal. FEMA's strategy is to base assessments on the principles that the Nation needs to understand the risks it faces, use those risks to determine the capabilities it needs, assess its current capability levels against those requirements, and track its progress in closing capability gaps.

Question#:	11
Topic:	grants
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

In 2012 FEMA released a consistent methodology for determining risks in the *Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment (THIRA) Guide (CPG-201)*. CPG-201 details the five-step process jurisdictions can use to generate desired outcomes and capability targets for each of the core capabilities. Diverging from past efforts to establish measures and metrics for a capability that would be applied uniformly, this approach allows a jurisdiction to establish its own capability targets based on the risks it faces.

Question: In October 2011, the National Academy of Public Administration released a congressionally mandated report on developing more meaningful grant performance measures. The report included a list of recommended performance measures. Does DHS and FEMA plan to implement the recommended measures included in this report?

Response: To support the measurement of the effectiveness of the Homeland Security Grant Program (HSGP), in 2011 the National Academy of Public Administration (NAPA) assisted FEMA in studying, developing, and implementing quantitative performance measures and metrics. NAPA developed 16 performance measures for the State Homeland Security Program (SHSP) and the Urban Areas Security Initiative (UASI) programs, and offered 30 additional recommendations, many of which are related to the implementation of the measures. As FEMA pointed out in the *Redundancy Elimination and Enhanced Performance for Preparedness Grants Act (Public Law 111-271): Report on the Grants Program Measurement Study*, NAPA's recommendations broadly validate FEMA's current approaches to increasing preparedness and conducting performance assessments. The underlying themes of NAPA's proposed performance measures and recommendations align with current FEMA initiatives and policies, and in several cases NAPA's recommended measures are either already in place or in the process of being implemented. In other cases the recommended measures present a variety of implementation challenges, as NAPA acknowledged in its report.

In August 2011, FEMA reported its progress in measuring the effectiveness of preparedness grants to Congress in the *Redundancy Elimination and Enhanced Performance for Preparedness Grants Act (Public Law 111-271): 2012 Biennial Report to Congress (REEPPG Biennial Report)*. The report included measurements for 10 of NAPA's 16 recommended metrics, and also included measurements for 16 metrics that FEMA developed independently. For the performance measures and metrics that FEMA could not yet quantify, FEMA is considering ways of managing the implementation challenges of these new measures.

Question#:	12
Topic:	GAO recommendations
Hearing:	The Department of Homeland Security at 10 Years: A Progress Report on Management
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide a current list of all outstanding GAO recommendations that have not yet been implemented by DHS. For each recommendation, please indicate whether the department agrees or disagrees with the recommendation, the steps the department plans to take to implement the recommendation, and when implementation will be complete.

Response: Attached is a listing identifying all open GAO recommendations to DHS as of May 17, 2013, excluding those that have been closed as of October 25, 2013. The spreadsheet identifies 394 open recommendations, by Component, the associated report number, report received date, and report title. Also included for each recommendation is the Department position – whether DHS concurred (agreed) or non-concurred (disagreed) with the recommendation, actions taken or planned to implement the recommendation, and projected completion dates.

Audit follow-up is an integral part of good management and is a shared responsibility between DHS management and the auditors. DHS recognizes that corrective action taken by management on resolved findings and recommendations is essential to improving the effectiveness and efficiency of Government operations. We agree with 97 percent of the GAO recommendations shown on the listing. During 2011 to 2013 (to date), GAO issued a total of 444 recommendations, and DHS closed 852 recommendations (including some from prior years). We are grateful for the level of coordination and professionalism GAO has displayed in our work together. We are currently working with GAO to close 104 (26%) of the 394 open recommendations.

Open GAO Recommendations
(As of 05/17/2013)

[illegible]

[illegible]

#	Comp	Report Number	Report Title	Rec #	Recommendation	Department/Program	Action/Recommendations	Proposed Completion Date
13	CBP	GAC-09-024	Border Patrol: Checkpoints Contribute to Consistent Data Collection and Improved Efficiency	3	To improve the reliability and accountability of checkpoints, the Department of Customs and Border Protection should improve the quality of the information that is collected from checkpoints. This information should be made available in the field, state, or federal level, and developing support of these materials.	Customs	In December 2012, UTIP and IAP produced an integrated report intended to aid the Border Patrol in addressing the concerns raised in GAC-09-024. In January 2013, the Executive Governance Board (EGB) created the Checkpoint Working Group to evaluate the GAC-09-024. In June 2013, a grant was awarded to a third management plan approved on November 17, 2013. Using the later date as a starting point, this grant is intended to be completed by June 30, 2015. Therefore, CBP had to adjust their deadlines on the recommendations. CBP intended to complete the grant by June 30, 2015.	6/30/2015
14	CBP	GAC-09-024	Border Patrol: Checkpoints Contribute to Consistent Data Collection and Improved Efficiency	4	To improve the reliability and accountability of checkpoints, the Department of Customs and Border Protection should use the information that is collected from checkpoints to make decisions on where to place checkpoints and other relevant factors in order to improve the efficiency and effectiveness of these materials.	Customs	In December 2012, UTIP and IAP produced an integrated report intended to aid the Border Patrol in addressing the concerns raised in GAC-09-024. In January 2013, the Executive Governance Board (EGB) created the Checkpoint Working Group to evaluate the GAC-09-024. In June 2013, a grant was awarded to a third management plan approved on November 17, 2013. Using the later date as a starting point, this grant is intended to be completed by June 30, 2015. Therefore, CBP had to adjust their deadlines on the recommendations. CBP intended to complete the grant by June 30, 2015.	6/30/2015
15	CBP	GAC-09-024	Border Patrol: Checkpoints Contribute to Consistent Data Collection and Improved Efficiency	6	To ensure that the checkpoint design process results in a more efficient and effective process, the Department of Customs and Border Protection should use the information that is collected from checkpoints to make decisions on where to place checkpoints and other relevant factors in order to improve the efficiency and effectiveness of these materials.	Customs	In December 2012, UTIP and IAP produced an integrated report intended to aid the Border Patrol in addressing the concerns raised in GAC-09-024. In January 2013, the Executive Governance Board (EGB) created the Checkpoint Working Group to evaluate the GAC-09-024. In June 2013, a grant was awarded to a third management plan approved on November 17, 2013. Using the later date as a starting point, this grant is intended to be completed by June 30, 2015. Therefore, CBP had to adjust their deadlines on the recommendations. CBP intended to complete the grant by June 30, 2015.	6/30/2015
16	CBP	GAC-09-024	Border Patrol: Checkpoints Contribute to Consistent Data Collection and Improved Efficiency	1	The CBP Commissioner ensures that CBP's new training program is effective and efficient.	Customs	On October 10, 2012, UTIP and IAP produced an integrated report intended to aid the Border Patrol in addressing the concerns raised in GAC-09-024. In January 2013, the Executive Governance Board (EGB) created the Checkpoint Working Group to evaluate the GAC-09-024. In June 2013, a grant was awarded to a third management plan approved on November 17, 2013. Using the later date as a starting point, this grant is intended to be completed by June 30, 2015. Therefore, CBP had to adjust their deadlines on the recommendations. CBP intended to complete the grant by June 30, 2015.	6/30/2015
17	CBP	GAC-09-024	Border Patrol: Checkpoints Contribute to Consistent Data Collection and Improved Efficiency	1	The CBP Commissioner ensures that CBP's new training program is effective and efficient.	Customs	On October 10, 2012, UTIP and IAP produced an integrated report intended to aid the Border Patrol in addressing the concerns raised in GAC-09-024. In January 2013, the Executive Governance Board (EGB) created the Checkpoint Working Group to evaluate the GAC-09-024. In June 2013, a grant was awarded to a third management plan approved on November 17, 2013. Using the later date as a starting point, this grant is intended to be completed by June 30, 2015. Therefore, CBP had to adjust their deadlines on the recommendations. CBP intended to complete the grant by June 30, 2015.	6/30/2015
18	CBP	GAC-09-024	Border Patrol: Checkpoints Contribute to Consistent Data Collection and Improved Efficiency	1	The CBP Commissioner ensures that CBP's new training program is effective and efficient.	Customs	On October 10, 2012, UTIP and IAP produced an integrated report intended to aid the Border Patrol in addressing the concerns raised in GAC-09-024. In January 2013, the Executive Governance Board (EGB) created the Checkpoint Working Group to evaluate the GAC-09-024. In June 2013, a grant was awarded to a third management plan approved on November 17, 2013. Using the later date as a starting point, this grant is intended to be completed by June 30, 2015. Therefore, CBP had to adjust their deadlines on the recommendations. CBP intended to complete the grant by June 30, 2015.	6/30/2015

[illegible]

#	Comp.	Report Number	Report Title	Report Received Date	Rec #	Recommendation	Comment/Response	Actions Taken/Remarks	Proposed Completion Date
26	CIP	GAO-10-341	Supply Chain Security: CIPs Has Made Progress in Assessing Risks, but Needs to Improve in Identifying and Responding to New Risks Challenges Remain: Public Version Only	9/30/2010	1	1. CIPs submit to Regulatory Assessment and Final Report (RAF) to the Department of Homeland Security (DHS) and the Department of Defense (DoD) for review. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. 2. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment.	Concur	These related activities to the Regulatory Assessment and Final Report (RAF) are part of a larger effort to improve the security of the supply chain. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment.	7/31/2013
27	CIP	GAO-11-38	IDENTIFYING BORDER: More Time Needed to Assess Risks and Improve Security Operations and Mutual Assistance Challenges Remain: Public Version	10/19/2011	1	1. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. 2. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment.	Concur	On July 27, 2011, CIPs published the Final Narrative Report: Programmatic Environmental Impact Statement (PEIS) and Draft Record of Decision (ROD). CIPs were still in the process of reviewing the PEIS and ROD. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment.	4/30/2015
28	CIP	GAO-11-73	Moving Risk: Prospects, Challenges Remain in the Federal Government's Effort to Assess and Manage Risk Challenges Remain: Public Version	10/25/2011	1	1. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. 2. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment.	Concur	As of January 3, 2013, CIPs CIPs report, CIPs has conducted a broad survey of nearly every business leader nationwide and has been working on developing a cost benefit analysis. The CIPs report has been submitted and is pending review by the Department of Homeland Security.	12/31/2012
29	CIP	GAO-11-73	Moving Risk: Prospects, Challenges Remain in the Federal Government's Effort to Assess and Manage Risk Challenges Remain: Public Version	10/25/2011	2	1. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. 2. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment. The review process is a multi-step process that includes a preliminary assessment, a detailed assessment, and a final assessment.	Concur	As of January 3, 2013, CIPs CIPs report, CIPs has conducted a broad survey of nearly every business leader nationwide and has been working on developing a cost benefit analysis. The CIPs report has been submitted and is pending review by the Department of Homeland Security.	12/31/2012

#	Comp.	Report Number	Report Title	Rec #	Recommendation	Overseer Position	Action Taken/Remarks	Prepared By	Completion Date
38	CSP	GAO-11-190	Maritime Security: Federal Agencies Have Taken Action to Improve Maritime Security, But Three Elements Can Be Strengthened	2	GAO recommends that the Secretary of Homeland Security direct the Commissioner of the Coast Guard and Commissioner of Customs and Border Protection to conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. The assessment is critical necessary to address any variance	Colonel	In order to perform a comprehensive analysis of all relevant CSP data, CSP will analyze all available data and direct the data reported to the relevant agencies. CSP will also conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year. CSP will also conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year.		12/1/2010
39	CSP	GAO-11-195	Maritime Security: Federal Agencies Have Taken Action to Improve Maritime Security, But Three Elements Can Be Strengthened	3	GAO recommends that the Secretary of Homeland Security direct the Commissioner of the Coast Guard and Commissioner of Customs and Border Protection to conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. The assessment is critical necessary to address any variance	Colonel	In order to perform a comprehensive analysis of all relevant CSP data, CSP will analyze all available data and direct the data reported to the relevant agencies. CSP will also conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year. CSP will also conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year.		11/30/2010
41	CSP	GAO-11-91	Border Security: Enhanced DHS Interagency Coordination is Needed for the Northern Border		Direct CSP to develop policy and guidance necessary to ensure that all relevant agencies are aware of the problem and are working to address it. The assessment is critical necessary to address any variance	Colonel	On January 25, 2011, the Deputy Commissioner signed the U.S. Customs and Border Protection (CBP) Integrated Planning and Reporting (IPR) report. The report identified the problem and the need for a joint assessment of CSP. The report also identified the need for a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year.		10/12/2010
42	CSP	GAO-11-335	Border Security: Enhanced DHS Interagency Coordination is Needed for the Northern Border		GAO recommends that the Secretary of Homeland Security direct the Commissioner of the Coast Guard and Commissioner of Customs and Border Protection to conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. The assessment is critical necessary to address any variance	Colonel	On March 1, 2011, the Deputy Commissioner signed the U.S. Customs and Border Protection (CBP) Integrated Planning and Reporting (IPR) report. The report identified the problem and the need for a joint assessment of CSP. The report also identified the need for a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year.		5/1/2011
43	CSP	GAO-11-68	SECURE BORDER: RELATIVE CONSTRAINTS TO THE CBP Technology Component Need		GAO recommends that the Secretary of Homeland Security direct the Commissioner of the Coast Guard and Commissioner of Customs and Border Protection to conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. The assessment is critical necessary to address any variance	Colonel	On March 1, 2011, the Deputy Commissioner signed the U.S. Customs and Border Protection (CBP) Integrated Planning and Reporting (IPR) report. The report identified the problem and the need for a joint assessment of CSP. The report also identified the need for a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year.		6/30/2010
44	CSP	GAO-11-68	SECURE BORDER: RELATIVE CONSTRAINTS TO THE CBP Technology Component Need		GAO recommends that the Secretary of Homeland Security direct the Commissioner of the Coast Guard and Commissioner of Customs and Border Protection to conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. The assessment is critical necessary to address any variance	Colonel	On March 1, 2011, the Deputy Commissioner signed the U.S. Customs and Border Protection (CBP) Integrated Planning and Reporting (IPR) report. The report identified the problem and the need for a joint assessment of CSP. The report also identified the need for a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year.		10/12/2010
45	CSP	GAO-11-62	Data Mining: CBP Needs to Improve Data Mining Capabilities to Support Border Security		GAO recommends that the Secretary of Homeland Security direct the Commissioner of the Coast Guard and Commissioner of Customs and Border Protection to conduct a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. The assessment is critical necessary to address any variance	Colonel	On March 1, 2011, the Deputy Commissioner signed the U.S. Customs and Border Protection (CBP) Integrated Planning and Reporting (IPR) report. The report identified the problem and the need for a joint assessment of CSP. The report also identified the need for a joint assessment of CSP to determine the extent and nature of the problem and identify ways to address the problem. This effort is in progress and will be completed by the end of the fiscal year.		7/1/2010

[illegible]

[illegible]

[illegible]

#	Comp.	Report Number	Report Received Date	Report Title	Rec #	Recommendation	Department / Division	Action/Task/Requirement	Projected Completion Date
67	CBP	GAO-13-59	1/20/2014	Border Security: Additional Actions Needed to Strengthen CBP Efforts to Monitor Risk of Employee Corruption and Misconduct	2	Assess the feasibility of expanding the integrity program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location. This includes assessing the feasibility of expanding the program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location.	U.S. Customs and Border Protection (CBP) Internal Affairs (IA) will work with the Department of Homeland Security (DHS) Office of the Inspector General (OIG) to develop a plan to expand the integrity program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location. This includes assessing the feasibility of expanding the program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location.	U.S. Customs and Border Protection (CBP) Internal Affairs (IA) will work with the Department of Homeland Security (DHS) Office of the Inspector General (OIG) to develop a plan to expand the integrity program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location. This includes assessing the feasibility of expanding the program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location.	9/30/2013
68	CBP	GAO-13-59	1/20/2014	Border Security: Additional Actions Needed to Strengthen CBP Efforts to Monitor Risk of Employee Corruption and Misconduct	3	Conduct quality assurance reviews of CBP IA investigations requested by HIEFA's quality assurance program.	U.S. Customs and Border Protection (CBP) Internal Affairs (IA) will work with the Department of Homeland Security (DHS) Office of the Inspector General (OIG) to develop a plan to expand the integrity program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location. This includes assessing the feasibility of expanding the program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location.	The U.S. Customs and Border Protection (CBP) Office of Internal Affairs (IA) Personnel Security Division (PSD) will work with the current Quality Assurance program to verify the accuracy of the data collected, when warranted. CBP IA, in turn, will work to ensure that the data collected is accurate and that the data is used to identify and address any issues. CBP IA will also work to ensure that the data is used to identify and address any issues. CBP IA will also work to ensure that the data is used to identify and address any issues.	9/30/2013
69	CBP	GAO-13-59	1/20/2014	Border Security: Additional Actions Needed to Strengthen CBP Efforts to Monitor Risk of Employee Corruption and Misconduct	4	Establish a process to log document, as required, any information received from HIEFA's quality assurance program.	U.S. Customs and Border Protection (CBP) Internal Affairs (IA) will work with the Department of Homeland Security (DHS) Office of the Inspector General (OIG) to develop a plan to expand the integrity program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location. This includes assessing the feasibility of expanding the program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location.	The U.S. Customs and Border Protection (CBP) Office of Internal Affairs (IA) Personnel Security Division (PSD) will develop a process to log document, as required, any information received from HIEFA's quality assurance program. The PSD will develop a process to log document, as required, any information received from HIEFA's quality assurance program. The PSD will develop a process to log document, as required, any information received from HIEFA's quality assurance program.	9/30/2013
70	CBP	GAO-13-59	1/20/2014	Border Security: Additional Actions Needed to Strengthen CBP Efforts to Monitor Risk of Employee Corruption and Misconduct	5	Develop guidance for CBP offices on the use and implementation of the integrity program.	U.S. Customs and Border Protection (CBP) Internal Affairs (IA) will work with the Department of Homeland Security (DHS) Office of the Inspector General (OIG) to develop a plan to expand the integrity program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location. This includes assessing the feasibility of expanding the program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location.	The U.S. Customs and Border Protection (CBP) Office of Internal Affairs (IA) Personnel Security Division (PSD) will develop a process to log document, as required, any information received from HIEFA's quality assurance program. The PSD will develop a process to log document, as required, any information received from HIEFA's quality assurance program. The PSD will develop a process to log document, as required, any information received from HIEFA's quality assurance program.	9/30/2013
71	CBP	GAO-13-59	1/20/2014	Border Security: Additional Actions Needed to Strengthen CBP Efforts to Monitor Risk of Employee Corruption and Misconduct	6	Set target timelines for completing and implementing a comprehensive integrity strategy.	U.S. Customs and Border Protection (CBP) Internal Affairs (IA) will work with the Department of Homeland Security (DHS) Office of the Inspector General (OIG) to develop a plan to expand the integrity program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location. This includes assessing the feasibility of expanding the program to include all CBP employees, regardless of position, and to include all CBP offices, regardless of location.	The U.S. Customs and Border Protection (CBP) Office of Internal Affairs (IA) Personnel Security Division (PSD) will develop a process to log document, as required, any information received from HIEFA's quality assurance program. The PSD will develop a process to log document, as required, any information received from HIEFA's quality assurance program. The PSD will develop a process to log document, as required, any information received from HIEFA's quality assurance program.	9/30/2013

[illegible]

[illegible]

#	Comp.	Report Number	Report Received Date	Report Title	Rec #	Recommendation	Department Action	Actions Taken/Status	Project Completion Date
80	FEMA	GAO-06-106	11/16/2005	Hurricane Katrina: Ineffective FEMA Response to Evacuation Needs of Millions of Citizens of Orleans and Mississippi	3	For the current MO and GSA contracts in Mississippi and for Orleans Parish, FEMA should design and implement internal control systems to ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed.	Concur	FEMA provided an updated Corrective Action Plan (CAP) to satisfy issues of the recommendations.	4/18/2013
81	FEMA	GAO-06-106	11/16/2005	Hurricane Katrina: Ineffective FEMA Response to Evacuation Needs of Millions of Citizens of Orleans and Mississippi	4	For the current MO and GSA contracts in Mississippi and for Orleans Parish, FEMA should design and implement internal control systems to ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed.	Concur	FEMA provided an updated Corrective Action Plan (CAP) to satisfy issues of the recommendations.	4/18/2013
82	FEMA	GAO-06-106	11/16/2005	Hurricane Katrina: Ineffective FEMA Response to Evacuation Needs of Millions of Citizens of Orleans and Mississippi	5	To address the extensive costs associated with evacuating citizens, FEMA should design and implement internal control systems to ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed.	Concur	FEMA provided an updated Corrective Action Plan (CAP) to satisfy issues of the recommendations.	4/18/2013
83	FEMA	GAO-06-106	11/16/2005	Hurricane Katrina: Ineffective FEMA Response to Evacuation Needs of Millions of Citizens of Orleans and Mississippi	6	With regard to the 10 transportation and destination (MO) and for Orleans Parish, FEMA should design and implement internal control systems to ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed. FEMA should also ensure that the evacuation of citizens is properly planned and executed.	Concur	FEMA provided an updated Corrective Action Plan (CAP) to satisfy issues of the recommendations.	4/18/2013
84	FEMA	GAO-06-106	2/15/2006	Emergency Travel Assistance: Federal Options for the States	1	To ensure timely and effective disaster assistance to public transit, the Secretary of Homeland Security should direct the FEMA to work with the states to develop guidelines or regulations for public transit to ensure that the states are able to receive the assistance they need. FEMA will work with the states to develop guidelines or regulations for public transit to ensure that the states are able to receive the assistance they need.	Concur	FEMA updated the response to the Final Report 06-243 to satisfy recommendations at § 42. This was sent to GAO on March 12, 2013. FEMA is working on the response.	4/18/2013
85	FEMA	GAO-06-243	2/15/2006	Emergency Travel Assistance: Federal Options for the States	2	To provide timely and effective disaster assistance to public transit, the Secretary of Homeland Security should direct the FEMA to work with the states to develop guidelines or regulations for public transit to ensure that the states are able to receive the assistance they need. FEMA will work with the states to develop guidelines or regulations for public transit to ensure that the states are able to receive the assistance they need.	Concur	FEMA updated the response to the Final Report 06-243 to satisfy recommendations at § 42. This was sent to GAO on March 12, 2013. FEMA is working on the response.	4/18/2013
86	FEMA	GAO-06-12	10/1/2006	Flood Insurance: FEMA's Rate Setting Process Warrants Attention	1	The Secretary of the Department of Homeland Security should ensure that FEMA's rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable.	Concur	FEMA provided the GAO with the report regarding methodologies for gathering flood probability data as a result of the data from the rating. FEMA's rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable.	4/18/2013
87	FEMA	GAO-06-12	10/1/2006	Flood Insurance: FEMA's Rate Setting Process Warrants Attention	2	The Secretary of the Department of Homeland Security should ensure that FEMA's rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable.	Concur	FEMA provided the GAO with the report regarding methodologies for gathering flood probability data as a result of the data from the rating. FEMA's rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable. FEMA should also ensure that the rate setting process is fair and equitable.	4/18/2013
88	FEMA	GAO-06-12	12/1/2006	Disaster Preparedness: FEMA's Public Assistance Grant Program Encountered Challenges with Cost Overruns	1	To help DOD improve the operation of the PA grant program and build on some of the actions taken to date, the Secretary of Homeland Security should ensure that FEMA's public assistance grant program is fair and equitable. FEMA should also ensure that the public assistance grant program is fair and equitable. FEMA should also ensure that the public assistance grant program is fair and equitable.	Concur	The GAO informed the ALD that they will review the documents received from FEMA and inform the ALD if anything else is needed. A report is required for the recommendations for the final report to GAO on August 11, 2017. FEMA is working on the report.	4/18/2013

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

#	Comp	Report Number	Report Date	Report Title	Rec'd	Recommendation	Department Action	Action Taken/Remarks	Progress Completion Date
148	FEMA	CAO-11-009	7/25/2011	FEMA and the Corps view that FEMA has not assessed the Corps' role in disaster response and recovery. FEMA has not assessed the Corps' role in disaster response and recovery. FEMA has not assessed the Corps' role in disaster response and recovery.	1	To assist in improving disaster response, FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery.	Concur	On February 27, 2013, FEMA provided additional information to CAO in early course of the recommendation. The CAO advised FEMA that they had requested the documents and are in the process of updating the recommendation reporting system to note that the issue is closed.	6/30/2013
149	FEMA	CAO-11-002	9/13/2011	HOME LAND SECURITY: Active FEMA has not assessed the Corps' role in disaster response and recovery. FEMA has not assessed the Corps' role in disaster response and recovery. FEMA has not assessed the Corps' role in disaster response and recovery.	8	To improve disaster response and recovery, FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery.	Concur	FEMA has the authority and capability to leverage the National Response Coordination Center (NRCC) to help prepare for response to disasters. FEMA has the authority and capability to leverage the NRCC to help prepare for response to disasters. FEMA has the authority and capability to leverage the NRCC to help prepare for response to disasters.	TBD
150	FEMA	CAO-12-047	12/19/2011	Post-Disaster Grant Program: Risk Management and Mitigation Measures Could Be Strengthened	1	The FEMA Administration to review the accounts for how widely FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts. FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts. FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts.	Concur	As of March 22, 2013, FEMA provided an update to the reporting to support closure of the recommendation. It is currently awaiting clearance from GPO leadership.	4/15/2013
151	FEMA	CAO-12-047	12/19/2011	Post-Disaster Grant Program: Risk Management and Mitigation Measures Could Be Strengthened	2	The FEMA Administration to review the accounts for how widely FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts. FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts. FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts.	Concur	As of March 22, 2013, FEMA provided an update to the reporting to support closure of the recommendation. It is currently awaiting clearance from GPO leadership.	4/15/2013
152	FEMA	CAO-12-047	12/19/2011	Post-Disaster Grant Program: Risk Management and Mitigation Measures Could Be Strengthened	4	The FEMA Administration to review the accounts for how widely FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts. FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts. FEMA's disaster response and recovery efforts are coordinated with FEMA's disaster response and recovery efforts.	Concur	As of March 22, 2013, FEMA provided an update to the reporting to support closure of the recommendation. It is currently awaiting clearance from GPO leadership.	4/15/2013
153	FEMA	CAO-12-053	3/20/2012	Increased Security DHS Needs Better Project Information and Coordination with Other Overlapping Grant Programs	1	To better identify and reduce the risk of duplication through FEMA's disaster response and recovery efforts, FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery.	Concur	On February 15, 2013, FEMA provided an update to the reporting to support closure of the recommendation. It is currently awaiting clearance from GPO leadership.	6/30/2013
154	FEMA	CAO-12-053	3/20/2012	Increased Security DHS Needs Better Project Information and Coordination with Other Overlapping Grant Programs	2	To better identify and reduce the risk of duplication through FEMA's disaster response and recovery efforts, FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery.	Concur	On February 15, 2013, FEMA provided an update to the reporting to support closure of the recommendation. It is currently awaiting clearance from GPO leadership.	6/30/2013
155	FEMA	CAO-12-053	3/20/2012	Increased Security DHS Needs Better Project Information and Coordination with Other Overlapping Grant Programs	3	To better identify and reduce the risk of duplication through FEMA's disaster response and recovery efforts, FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery.	Concur	On February 15, 2013, FEMA provided an update to the reporting to support closure of the recommendation. It is currently awaiting clearance from GPO leadership.	6/30/2013
156	FEMA	CAO-13-047	4/25/2012	Increased Security DHS Needs Better Project Information and Coordination with Other Overlapping Grant Programs	1	To better identify and reduce the risk of duplication through FEMA's disaster response and recovery efforts, FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery. FEMA should conduct a study to determine the Corps' role in disaster response and recovery.	Concur	The action was developed by FEMA in close consultation with GAO's Disaster FEMA. FEMA is currently working on a second response to properly close out the recommendation.	4/25/2013

#	Comp	Report Reference	Report Received Date	Report Title	Rec #	Recommendation	Department Position	Action Taken/Remarks	Proposed Completion Date
153	FEMA	GAO-12-487	4/26/2012	Resilient Emergency Management Agency Workforce Planning and Training: Incorporating Strategic Management Principles	2	To help ensure that FEMA's agencywide workforce planning and training efforts are coordinated in a strategic manner, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	The update was developed by FEMA in direct consultation with GAO's Dan Vukobratovic. FEMA is currently working on a second response to helpfully close out the recommendation.	4/26/2012
158	FEMA	GAO-12-487	4/26/2012	Resilient Emergency Management Agency Workforce Planning and Training: Incorporating Strategic Management Principles	3	To help ensure that FEMA's agencywide workforce planning and training efforts are coordinated in a strategic manner, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	The update was developed by FEMA in direct consultation with GAO's Dan Vukobratovic. FEMA is currently working on a second response to helpfully close out the recommendation.	4/26/2012
159	FEMA	GAO-12-487	4/26/2012	Resilient Emergency Management Agency Workforce Planning and Training: Incorporating Strategic Management Principles	4	To help ensure that FEMA's agencywide workforce planning and training efforts are coordinated in a strategic manner, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	The update was developed by FEMA in direct consultation with GAO's Dan Vukobratovic. FEMA is currently working on a second response to helpfully close out the recommendation.	4/26/2012
160	FEMA	GAO-12-538	6/1/2012	DISASTER ASSISTANCE PROGRAMS: FEMA Could Enhance Training for Disaster Assistance Program Staff	1	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	FEMA provided the response to the 80-Char Letter on August 13, 2012. On February 22, 2013, FEMA requested closure of the recommendation. Additional information was forwarded to GAO on April 12 to support closing the recommendation including the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs. The OIG's review of the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs.	5/24/2012
161	FEMA	GAO-12-538	6/1/2012	DISASTER ASSISTANCE PROGRAMS: FEMA Could Enhance Training for Disaster Assistance Program Staff	2	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	FEMA provided the response to the 80-Char Letter on August 13, 2012. On February 22, 2013, FEMA requested closure of the recommendation. Additional information was forwarded to GAO on April 12 to support closing the recommendation including the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs. The OIG's review of the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs.	5/24/2012
162	FEMA	GAO-12-538	6/1/2012	DISASTER ASSISTANCE PROGRAMS: FEMA Could Enhance Training for Disaster Assistance Program Staff	3	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	FEMA provided the response to the 80-Char Letter on August 13, 2012. On February 22, 2013, FEMA requested closure of the recommendation. Additional information was forwarded to GAO on April 12 to support closing the recommendation including the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs. The OIG's review of the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs.	5/24/2012
163	FEMA	GAO-12-538	6/1/2012	DISASTER ASSISTANCE PROGRAMS: FEMA Could Enhance Training for Disaster Assistance Program Staff	4	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	FEMA provided the response to the 80-Char Letter on August 13, 2012. On February 22, 2013, FEMA requested closure of the recommendation. Additional information was forwarded to GAO on April 12 to support closing the recommendation including the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs. The OIG's review of the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs.	5/24/2012
164	FEMA	GAO-12-538	6/1/2012	DISASTER ASSISTANCE PROGRAMS: FEMA Could Enhance Training for Disaster Assistance Program Staff	5	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	FEMA provided the response to the 80-Char Letter on August 13, 2012. On February 22, 2013, FEMA requested closure of the recommendation. Additional information was forwarded to GAO on April 12 to support closing the recommendation including the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs. The OIG's review of the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs.	5/24/2012
165	FEMA	GAO-12-538	6/1/2012	DISASTER ASSISTANCE PROGRAMS: FEMA Could Enhance Training for Disaster Assistance Program Staff	6	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	FEMA provided the response to the 80-Char Letter on August 13, 2012. On February 22, 2013, FEMA requested closure of the recommendation. Additional information was forwarded to GAO on April 12 to support closing the recommendation including the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs. The OIG's review of the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs.	5/24/2012
166	FEMA	GAO-12-538	6/1/2012	DISASTER ASSISTANCE PROGRAMS: FEMA Could Enhance Training for Disaster Assistance Program Staff	7	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	FEMA provided the response to the 80-Char Letter on August 13, 2012. On February 22, 2013, FEMA requested closure of the recommendation. Additional information was forwarded to GAO on April 12 to support closing the recommendation including the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs. The OIG's review of the draft agencywide policy for the administration implementation oversight of the FEMA disaster programs.	5/24/2012
167	FEMA	GAO-12-748	7/25/2012	Enhance Pandemic Preparedness: Agencywide Report on Pandemic Preparedness: Incorporating Strategic Management Principles	1	To help DHS improve the management of FEMA's disaster assistance programs, we recommended that the FEMA Administrator develop a strategic workforce planning and training strategy that incorporates FEMA's mission, vision, and strategic goals, and that the strategy be approved by FEMA's senior leadership.	Concur	As of September 2012, FEMA needed the draft Federal Continuity Plan (FCP). FEMA requested and approved the draft FCP. FEMA is currently working on a second response to helpfully close out the recommendation.	4/26/2012

[illegible]

[illegible]

#	Comp.	Report Number	Report Title	Rec'd/Response Date	Recommendation	Department/Program	Action/Task/Remarks	Proposed Completion Date
187	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	As indicated above, the ISGCB has initiated a Department-wide effort to draft an Implementation Plan and has convened a Department-wide meeting to discuss the plan. The plan is currently under review and will be submitted to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
188	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
189	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
190	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
191	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
192	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
193	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
194	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
195	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
196	IA	GAO-12-889	INFORMATION SHARING: DHS Has Communicated Leadership and Program Information to the Active Border Controls Initiative and Strengthened Efforts	9/18/2012	To address information-sharing gaps and risks, direct the Secretary to develop and implement a plan to improve information sharing among DHS components, including the Active Border Controls Initiative, and to ensure that the plan is consistent with the law, as well as determine whether other information sharing initiatives are needed to address the information sharing gaps.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	6/30/2013
197	ICL	GAO-10-228	DHS Needs to Better Leverage Program Performance along the Document Border	7/22/2010	To determine whether ICE could better leverage its resources to address the document border, the Department should conduct a study to determine whether ICE could better leverage its resources to address the document border.	Control	The ISGCB is currently reviewing the plan and will submit it to the President for signature. The plan will be implemented by the end of the second quarter of fiscal year 2013.	4/1/2011

[illegible]

[illegible]

[illegible]

[illegible]

#	Comp.	Report Number	Report Received Date	Report Title	Rec #	Recommendation	Department / Division	Action/Task/Remarks	Report Completion Date
237	MMMT-CDO	GAO-11-362	3/16/2011	GAO-11-362: Information Technology: The Department of Homeland Security Should Speed the CDO's Information Technology Modernization Efforts to Improve Data Accuracy	3	To help ensure that the Department provides accurate and timely information to the public, the Department should speed the CDO's information technology modernization efforts to improve data accuracy at least monthly.	GAO-11-362	On March 28, 2013, DHS OIG sent CDO an update and request for information 3. DHS provided detailed information on the progress of the CDO's information technology modernization efforts. DHS OIG will follow up with DHS OIG in August 2013 to ensure that DHS OIG is making progress.	3/31/2013
238	MMMT-CDO	GAO-11-368	7/26/2011	DATA CENTER CONSOLIDATION: DHS Should Accelerate the Consolidation of Data Centers to Reduce Costs and Improve Data Accuracy	1	We are recommending that the Secretary and agency heads direct their component agencies and their data center program managers to complete the existing requests in their respective data center consolidation initiatives and plans.	GAO-11-368	DHS is preparing to issue new OIG guidance that will affect documentation of the approach in order to speed the recommendation. DHS OIG will follow up with DHS OIG in August 2013 to ensure that DHS OIG is making progress.	12/31/2013
239	MMMT-CDO	GAO-11-381	7/26/2011	Information Technology: DHS Needs to Improve Its Information Technology Modernization Efforts	1	To help guide consistent and effective execution of IT/IT at DHS, the Secretary should direct the CDO to develop a plan for the Department's information technology modernization efforts, including when major and other high-risk IT modernization efforts are required, and to ensure that the CDO is taking steps to ensure that plans and significant findings from DHS OIG are being addressed.	GAO-11-381	60-Day letter was sent to Congress/OMB on January 4, 2013. DHS OIG EMOJ letter met with GAO on March 21 to discuss the progress of the CDO's information technology modernization efforts. DHS OIG will follow up with DHS OIG in August 2013 to ensure that DHS OIG is making progress.	12/31/2013
240	MMMT-CDO	GAO-11-391	7/26/2011	Information Technology: DHS Needs to Improve Its Information Technology Modernization Efforts	2	To help guide consistent and effective execution of IT/IT at DHS, the Secretary should direct the CDO to develop a plan for the Department's information technology modernization efforts, including when major and other high-risk IT modernization efforts are required, and to ensure that the CDO is taking steps to ensure that plans and significant findings from DHS OIG are being addressed.	GAO-11-391	The 60-day letter was sent to Congress/OMB on January 4, 2013. The DHS OIG EMOJ letter met with GAO on March 21 to discuss the progress of the CDO's information technology modernization efforts. DHS OIG will follow up with DHS OIG in August 2013 to ensure that DHS OIG is making progress.	12/31/2013
241	MMMT-CDO	GAO-11-391	7/26/2011	Information Technology: DHS Needs to Improve Its Information Technology Modernization Efforts	3	To help guide consistent and effective execution of IT/IT at DHS, the Secretary should direct the CDO to develop a plan for the Department's information technology modernization efforts, including when major and other high-risk IT modernization efforts are required, and to ensure that the CDO is taking steps to ensure that plans and significant findings from DHS OIG are being addressed.	GAO-11-391	The 60-day letter was sent to Congress/OMB on January 4, 2013. The DHS OIG EMOJ letter met with GAO on March 21 to discuss the progress of the CDO's information technology modernization efforts. DHS OIG will follow up with DHS OIG in August 2013 to ensure that DHS OIG is making progress.	9/30/2014
242	MMMT-CDO	GAO-11-398	7/26/2011	FOIA: DHS Needs to Improve Its Information Technology Modernization Efforts	1	To help guide consistent and effective execution of IT/IT at DHS, the Secretary should direct the CDO to develop a plan for the Department's information technology modernization efforts, including when major and other high-risk IT modernization efforts are required, and to ensure that the CDO is taking steps to ensure that plans and significant findings from DHS OIG are being addressed.	GAO-11-398	On June 20, 2013, DHS OIG sent a 60-day letter which requested closure of the recommendation, along with attached supporting documentation. DHS OIG will follow up with DHS OIG in August 2013 to ensure that DHS OIG is making progress.	4/20/2013
243	MMMT-CDO	GAO-11-412	10/17/2011	GAO-11-412: DHS Needs to Improve Its Information Technology Modernization Efforts	1	To help guide consistent and effective execution of IT/IT at DHS, the Secretary should direct the CDO to develop a plan for the Department's information technology modernization efforts, including when major and other high-risk IT modernization efforts are required, and to ensure that the CDO is taking steps to ensure that plans and significant findings from DHS OIG are being addressed.	GAO-11-412	The 60-day letter was sent to Congress/OMB on January 15, 2013. The DHS OIG EMOJ letter met with GAO on March 21 to discuss the progress of the CDO's information technology modernization efforts. DHS OIG will follow up with DHS OIG in August 2013 to ensure that DHS OIG is making progress.	9/30/2013

#	Comp.	Report Number	Report Title	Report Recd. Date	Rec #	Recommendation	Department/Program	Action/Task/Remarks	Progress/Completion Date
244	MOBMT-CIO	GAO-11-742	Data Mining: DHS Needs to Improve Analytical Capabilities of Systems Supporting Counterterrorism	10/20/2011	2	In order to improve DHS's policies and practices for analyzing and processing data, DHS should: (1) develop a strategy for data mining that includes the necessary primary functions, the necessary secondary functions, and the necessary tertiary functions; (2) develop a strategy for data mining that includes the necessary primary functions, the necessary secondary functions, and the necessary tertiary functions; and (3) develop a strategy for data mining that includes the necessary primary functions, the necessary secondary functions, and the necessary tertiary functions.	CISAC	The EO Data Letter was sent to Congress/DHS on January 15, 2012. DHS OIG is awaiting approval of Operational Analysis (OA) Guidelines. DHS OA Guidelines were included in the Comments for action.	6/30/2013
245	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On April 8, 2013, a condition was included from GAO that the recommendation has been closed as implemented. No further action is necessary.	4/30/2013
246	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
247	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
248	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
249	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
250	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
251	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
252	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
253	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013
254	MOBMT-CIO	GAO-12-244	Information Technology: Department of Homeland Security Needs to Address Information Technology Vulnerabilities	2/1/2012	1	The Secretary of Homeland Security should direct the CIO to: (1) identify and prioritize the most critical information technology vulnerabilities; (2) develop a strategy for addressing the most critical information technology vulnerabilities; and (3) develop a strategy for addressing the most critical information technology vulnerabilities.	CISAC	On December 21, 2012, DHS OIG sent an update to DHS regarding the recommendation. The recommendation was not implemented. DHS OIG is awaiting DHS's response.	4/30/2013

[illegible]

[illegible]

#	Comp	Report Number	Report Received Date	Report Title	Rec #	Recommendation	Department Response	Action Taken/Remarks	Progress Completion Date
261	MDMT-PAIRM	GAO-12-831	9/18/2012	HOME AND SECURITY DHS Requires More Effective Management to Help Meet Mission Needs	2	Modify DHS acquisition policy to more fully reflect the requirements of the Federal Acquisition Regulation (FAR). 1. Ensure portfolio manager is located from next to invest in a dedicated process. 2. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 3. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 4. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy.	Concur	This recommendation will be addressed in the new Integrated Readiness Life Cycle Model (ILCM) process instead of through portfolio review.	18ED
262	MDMT-PAIRM	GAO-12-833	9/18/2012	HOME AND SECURITY DHS Requires More Effective Management to Help Meet Mission Needs	3	Ensure all major acquisition programs fully comply with DHS acquisition policy. 1. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 2. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 3. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy.	Concur	GAO described DHS' progress in doing the recommendations as referenced in the original report. In the new ILCM process, GAO requires programs that were in violation of the ILCM 102 was required to comply with an updated document rather than the ILCM 102. The ILCM is being revised to address this.	9/30/2013
263	MDMT-PAIRM	GAO-12-833	9/18/2012	HOME AND SECURITY DHS Requires More Effective Management to Help Meet Mission Needs	4	Ensure all major acquisition programs fully comply with DHS acquisition policy. 1. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 2. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 3. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy.	Concur	GAO recognizes that this is a long-term objective and is directly tied to recommendation #2 of this same report. That recommendation is to ensure that DHS is fully compliant with the ILCM process that addresses the weaknesses during the consideration of the ILCM process.	12/31/2015
264	MDMT-PAIRM	GAO-12-833	9/18/2012	HOME AND SECURITY DHS Requires More Effective Management to Help Meet Mission Needs	5	Ensure all major acquisition programs fully comply with DHS acquisition policy. 1. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 2. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy. 3. Review the acquisition policy to ensure it is consistent with the mission goals and (2) the investment strategy policy.	Concur	GAO described DHS' request to close the recommendations as referenced in the original report and the 60-day letter. GAO Note that the ILCM process is being revised to address this. The Office of Program Accountability and Risk Management (PARM) will have more discussions with GAO to determine how to carry this recommendation.	9/30/2013
265	NPPD	GAO-09-904	6/26/2009	Emergency Communications: Federal Protective Service Should Improve Planning, Coordination and Monitoring Through Federal Efforts	3	To improve federal agencies' collaboration and working in efforts related to emergency communications and in help emergency communications, the Federal Protective Service (FPS) should provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans.	Concur	Since 2007, FPS has worked with FEMA, DHS, and other federal agencies to develop guidance and technical assistance to federal agencies in developing broad emergency communications plans. FPS has provided guidance and technical assistance to federal agencies in developing broad emergency communications plans. FPS has provided guidance and technical assistance to federal agencies in developing broad emergency communications plans.	18ED
266	NPPD	GAO-09-604	6/26/2009	Emergency Communications: Federal Protective Service Should Improve Planning, Coordination and Monitoring Through Federal Efforts	4	To improve federal agencies' collaboration and working in efforts related to emergency communications and in help emergency communications, the Federal Protective Service (FPS) should provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans.	Concur	Since the issuance of the report, DHS, through the Office of Emergency Communications (OEC), has worked with the EOPC members to develop a plan to improve emergency communications. To achieve this result, OEC has worked with EOPC members to develop a plan to improve emergency communications. To achieve this result, OEC has worked with EOPC members to develop a plan to improve emergency communications.	18ED
267	NPPD	GAO-09-104	7/2/2009	Homeland Security: Federal Protective Service Should Improve Planning, Coordination and Monitoring Through Federal Efforts	1	To improve federal agencies' collaboration and working in efforts related to emergency communications and in help emergency communications, the Federal Protective Service (FPS) should provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans.	Concur	As of March 5, 2013, FPS provided a plan to improve emergency communications. As of March 5, 2013, FPS provided a plan to improve emergency communications. As of March 5, 2013, FPS provided a plan to improve emergency communications. As of March 5, 2013, FPS provided a plan to improve emergency communications.	9/30/2013
268	NPPD	GAO-09-104	7/2/2009	Homeland Security: Federal Protective Service Should Improve Planning, Coordination and Monitoring Through Federal Efforts	2	To improve federal agencies' collaboration and working in efforts related to emergency communications and in help emergency communications, the Federal Protective Service (FPS) should provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans. The FPS should also provide guidance and technical assistance to federal agencies in developing broad emergency communications plans.	Concur	As of March 5, 2013, FPS provided a plan to improve emergency communications. As of March 5, 2013, FPS provided a plan to improve emergency communications. As of March 5, 2013, FPS provided a plan to improve emergency communications. As of March 5, 2013, FPS provided a plan to improve emergency communications.	9/30/2013

[illegible]

[illegible]

[illegible]

[illegible]

#	Comp	Report Received Date	Report Title	Rec #	Recommendation	Department Response	Action/Task/Remarks	Prepared Completion Date
319	HPFD 2014	QAO-11-2014	Federal Protective Services Program Hesitant to Resolve Delays and Exhaust Member to Complete Transition	2	Given the challenges FPS faced with developing a Ramp down plan, and the need to ensure the safety of the border, the Department should continue to work with the Department of Homeland Security to ensure the smooth transition of the program. The Department should also continue to work with the Department of Justice to ensure the program is properly managed. The Department should also continue to work with the Department of State to ensure the program is properly managed.	Concur	As of October 20, 2014, HPFD received a 602-City letter response. With respect to the Ramp down plan, HPFD is currently working with the Department of Homeland Security to ensure the smooth transition of the program. The Department is also working with the Department of Justice to ensure the program is properly managed. The Department is also working with the Department of State to ensure the program is properly managed.	9/30/2015
320	HPFD 2014	QAO-11-2014	Federal Protective Services Program Hesitant to Resolve Delays and Exhaust Member to Complete Transition	1	Given the challenges FPS faced with developing a Ramp down plan, and the need to ensure the safety of the border, the Department should continue to work with the Department of Homeland Security to ensure the smooth transition of the program. The Department should also continue to work with the Department of Justice to ensure the program is properly managed. The Department should also continue to work with the Department of State to ensure the program is properly managed.	Concur	As of October 20, 2014, HPFD received a 602-City letter response. At the same time, congressional requesters initiated a new Ramp down plan. HPFD is currently working with the Department of Homeland Security to ensure the smooth transition of the program. The Department is also working with the Department of Justice to ensure the program is properly managed. The Department is also working with the Department of State to ensure the program is properly managed.	9/30/2015
321	HPFD 2014	QAO-11-2014	Federal Protective Services Program Hesitant to Resolve Delays and Exhaust Member to Complete Transition	2	Given the challenges FPS faced with developing a Ramp down plan, and the need to ensure the safety of the border, the Department should continue to work with the Department of Homeland Security to ensure the smooth transition of the program. The Department should also continue to work with the Department of Justice to ensure the program is properly managed. The Department should also continue to work with the Department of State to ensure the program is properly managed.	Concur	As of October 20, 2014, HPFD received a 602-City letter response. At the same time, congressional requesters initiated a new Ramp down plan. HPFD is currently working with the Department of Homeland Security to ensure the smooth transition of the program. The Department is also working with the Department of Justice to ensure the program is properly managed. The Department is also working with the Department of State to ensure the program is properly managed.	9/30/2015
322	HPFD 2014	QAO-11-2014	Federal Protective Services Program Hesitant to Resolve Delays and Exhaust Member to Complete Transition	3	Given the challenges FPS faced with developing a Ramp down plan, and the need to ensure the safety of the border, the Department should continue to work with the Department of Homeland Security to ensure the smooth transition of the program. The Department should also continue to work with the Department of Justice to ensure the program is properly managed. The Department should also continue to work with the Department of State to ensure the program is properly managed.	Concur	As of October 20, 2014, HPFD received a 602-City letter response. At the same time, congressional requesters initiated a new Ramp down plan. HPFD is currently working with the Department of Homeland Security to ensure the smooth transition of the program. The Department is also working with the Department of Justice to ensure the program is properly managed. The Department is also working with the Department of State to ensure the program is properly managed.	9/30/2015
323	HPFD 2014	QAO-11-2014	Federal Protective Services Program Hesitant to Resolve Delays and Exhaust Member to Complete Transition	4	Given the challenges FPS faced with developing a Ramp down plan, and the need to ensure the safety of the border, the Department should continue to work with the Department of Homeland Security to ensure the smooth transition of the program. The Department should also continue to work with the Department of Justice to ensure the program is properly managed. The Department should also continue to work with the Department of State to ensure the program is properly managed.	Concur	As of October 20, 2014, HPFD received a 602-City letter response. At the same time, congressional requesters initiated a new Ramp down plan. HPFD is currently working with the Department of Homeland Security to ensure the smooth transition of the program. The Department is also working with the Department of Justice to ensure the program is properly managed. The Department is also working with the Department of State to ensure the program is properly managed.	9/30/2015

#	Comp.	Report Number	Report Number	Report Title	Doc #	Recommendation	Department Function	Action Taken/Remarks	Responsible Officer
324	NPTD	GMO-11-001	11/20/2011	FEDERAL COURTHOUSES Improved Community Healed to Meet the Needs of a Complex Security Environment	1	The Secretary of Homeland Security and the Director of the Federal Bureau of Investigation (FBI) shall conduct a joint review of the March 2010 report, "Improving the Security of Federal Courthouses: A Study of the Security of Federal Courthouses," to identify areas for improvement. The Secretary shall coordinate with the FBI to ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans.	Concur	As of March 2012, DHS established a dedicated working group in coordination with the National Security Council to review and assess the current DHS and identify needed changes as noted in the recommendation. GAO requires DHS to work in consultation with the US Marshals to modify plans, and implement a revised plan to meet all the recommendations.	9/26/2012
325	NPTD	GMO-11-001	11/20/2011	FEDERAL COURTHOUSES Improved Community Healed to Meet the Needs of a Complex Security Environment	2	To the extent that DHS is unable to respond to the Secretary of Homeland Security's request for information, the Secretary shall ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans.	Concur	As of March 2012, DHS agrees that continued collaboration and further review of the plan ongoing results will enhance security at DHS facilities. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans.	9/26/2012
326	NPTD	GMO-12-8	11/20/2011	Community Human Capital Initiative: Human Resource Planning and Coordination	1	To ensure that the Department's cybersecurity workforce remains in better coordinated and planned, such as to better address the needs of the Department's cybersecurity workforce, the Secretary shall ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans.	Concur	GAO provided GAO with all completed component plans and the NICE integrated program plan was completed and is with the results of the study. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans.	12/10/2012
327	NPTD	GMO-12-8	11/20/2011	Community Human Capital Initiative: Human Resource Planning and Coordination	2	To ensure that the Department's cybersecurity workforce remains in better coordinated and planned, such as to better address the needs of the Department's cybersecurity workforce, the Secretary shall ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans.	Concur	GAO provided GAO with all completed component plans and the NICE integrated program plan was completed and is with the results of the study. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans.	12/10/2012
328	NPTD	GMO-12-8	11/20/2011	Community Human Capital Initiative: Human Resource Planning and Coordination	3	To ensure that the Department's cybersecurity workforce remains in better coordinated and planned, such as to better address the needs of the Department's cybersecurity workforce, the Secretary shall ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans.	Concur	GAO provided GAO with all completed component plans and the NICE integrated program plan was completed and is with the results of the study. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans.	12/10/2012
329	NPTD	GMO-12-8	11/20/2011	Community Human Capital Initiative: Human Resource Planning and Coordination	4	To ensure that the Department's cybersecurity workforce remains in better coordinated and planned, such as to better address the needs of the Department's cybersecurity workforce, the Secretary shall ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans. The Secretary shall also ensure that the results of the study are incorporated into the FBI's security plans.	Concur	GAO provided GAO with all completed component plans and the NICE integrated program plan was completed and is with the results of the study. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans. DHS agrees that it will continue to work with the FBI to ensure that the results of the study are incorporated into the FBI's security plans.	12/10/2012

#	Comp.	Report Number	Report Title	Rec #	Recommendation	Department / Priority	Action Items/Remarks	Projected Completion Date
329	NPPD	GAO-12-8	Cybersecurity Incident Capable: Initiatives to Enhance Training and Coordination	5	To ensure that governmentwide cybersecurity workforce initiatives are better coordinated and planned, and to better understand the needs of the workforce, the Secretary of Homeland Security should direct the Secretary of the Department of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	DHS provided GAO with a completed component program plan and the NICE integrated program plan was completed and is with NIST for approval. In addition to the program plan, the initiative addressed the NICE Strategic Plan and the NICE Framework to ensure that the program plan is aligned with the NICE Framework. In GAO in October, December 2012, GAO is currently reviewing all documentation for details.	12/1/2012
331	NPPD	GAO-12-82	Critical Infrastructure Protection: Cybersecurity Capabilities: Guidance is Available, but More Can Be Done to Promote Its Use	1	We recommend that the Secretary of Homeland Security, in consultation with the Secretary of Defense, should direct the Secretary of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	DHS briefed the Critical Sector Cyber Security Working on the group back on June 18, 2012, requesting that CSECWG members conduct a study of the NICE Framework to ensure that the program plan is aligned with the NICE Framework. In GAO in October, December 2012, GAO is currently reviewing all documentation for details.	TBD
332	NPPD	GAO-12-83	Cybersecurity Capabilities: Guidance is Available, but More Can Be Done to Promote Its Use	1	To help ensure that public safety agencies are not overlooking for homeland communication elements, the Secretary of Homeland Security should direct the Secretary of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	In March 2013, DHS, OGC provided GAO with a status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter.	TBD
333	NPPD	GAO-12-84	Cybersecurity Capabilities: Guidance is Available, but More Can Be Done to Promote Its Use	1	To help ensure that public safety agencies are not overlooking for homeland communication elements, the Secretary of Homeland Security should direct the Secretary of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	In March 2013, DHS, OGC provided GAO with a status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter.	TBD
334	NPPD	GAO-12-85	Cybersecurity Capabilities: Guidance is Available, but More Can Be Done to Promote Its Use	1	To help ensure that public safety agencies are not overlooking for homeland communication elements, the Secretary of Homeland Security should direct the Secretary of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	In March 2013, DHS, OGC provided GAO with a status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter.	4/20/2012
335	NPPD	GAO-12-86	Cybersecurity Capabilities: Guidance is Available, but More Can Be Done to Promote Its Use	1	To help ensure that public safety agencies are not overlooking for homeland communication elements, the Secretary of Homeland Security should direct the Secretary of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	In March 2013, DHS, OGC provided GAO with a status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter.	12/1/2012
336	NPPD	GAO-12-87	Cybersecurity Capabilities: Guidance is Available, but More Can Be Done to Promote Its Use	1	To help ensure that public safety agencies are not overlooking for homeland communication elements, the Secretary of Homeland Security should direct the Secretary of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	In March 2013, DHS, OGC provided GAO with a status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter.	5/1/2013
337	NPPD	GAO-12-88	Cybersecurity Capabilities: Guidance is Available, but More Can Be Done to Promote Its Use	1	To help ensure that public safety agencies are not overlooking for homeland communication elements, the Secretary of Homeland Security should direct the Secretary of Homeland Security to conduct a study of the National Institute for Cybersecurity Education (NICE) to identify the personnel divisions for NICE to specify the personnel divisions to be provided for planning and implementing of personnel activities.	Continues	In March 2013, DHS, OGC provided GAO with a status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter. To date, OGC had provided the status of the milestones stated in the Status Letter.	12/1/2013

[illegible]

#	Comp	Report Number	Report Received Date	Report Title	Rec #	Recommendation	Department/Agency	Action/Remarks	Anticipated Completion Date
302	PLCY	GAO-08-987	9/15/2008	Visa Waiver Program: Actions Are Needed to Improve Management of the Program, Expedite Processing, and to Address and Mitigate Program Risks	3	To improve management of the Visa Waiver Program and ensure that the program is properly managed, the Secretary of Homeland Security should direct the Visa Waiver Program's management to: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	On April 15, 2010, DHS issued a letter stating that there is a ongoing management backlog in DHS's systems to improve and enhance the program's management. After this meeting, GAO will close the recommendation based on the evidence presented by DHS at that time.	9/15/2010
303	PLCY	GAO-08-987	9/15/2008	Visa Waiver Program: Actions Are Needed to Improve Management of the Program, Expedite Processing, and to Address and Mitigate Program Risks	4	To improve management of the Visa Waiver Program and ensure that the program is properly managed, the Secretary of Homeland Security should direct the Visa Waiver Program's management to: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	DHS sent a letter to GAO dated October 4, 2010, to provide an update on the actions taken for the recommendation. It was reported that DHS's Visa Waiver Program Office (VWPO) had received a letter from the Secretary of Homeland Security to improve and enhance the program's management. DHS is currently working on the recommendation. GAO will close the recommendation based on the evidence presented by DHS at that time.	9/15/2010
304	PLCY	GAO-09-037	1/25/2009	Northern Border Security: DHS's Report on the Status of the Program's Management and to Address and Mitigate Program Risks	1	To provide Congress with information that will facilitate policy development and implementation, the Secretary of Homeland Security should: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	On April 15, 2010, DHS provided a response to this recommendation. On April 29, 2010, DHS sent GAO additional information on the program's management. GAO will close the recommendation based on the evidence presented by DHS at that time.	1/25/2010
305	PLCY	GAO-10-028	7/1/2010	REDEFINING THE ASSESSMENT OF THE NORTHERN BORDER: DHS's Report on the Status of the Program's Management and to Address and Mitigate Program Risks	1	To improve management of the Visa Waiver Program and ensure that the program is properly managed, the Secretary of Homeland Security should direct the Visa Waiver Program's management to: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	DHS Office of Policy was assigned to review the recommendation in the last few months. DHS Office of Policy is currently working on the recommendation. GAO will close the recommendation based on the evidence presented by DHS at that time.	7/1/2010
306	PLCY	GAO-11-148	5/1/2011	REDEFINING THE ASSESSMENT OF THE NORTHERN BORDER: DHS's Report on the Status of the Program's Management and to Address and Mitigate Program Risks	4	To improve management of the Visa Waiver Program and ensure that the program is properly managed, the Secretary of Homeland Security should direct the Visa Waiver Program's management to: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	The DHS Office of Policy, Information, and Communications (OIC) provided a response to this recommendation. OIC is currently working on the recommendation. GAO will close the recommendation based on the evidence presented by DHS at that time.	5/1/2011
307	PLCY	GAO-11-037	2/1/2011	REDEFINING THE ASSESSMENT OF THE NORTHERN BORDER: DHS's Report on the Status of the Program's Management and to Address and Mitigate Program Risks	1	To improve management of the Visa Waiver Program and ensure that the program is properly managed, the Secretary of Homeland Security should direct the Visa Waiver Program's management to: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	DHS provided a response to this recommendation in GAO's last year. DHS has met with GAO and seeks to find a way to address the recommendation in the future.	2/1/2011
308	PLCY	GAO-11-037	2/1/2011	REDEFINING THE ASSESSMENT OF THE NORTHERN BORDER: DHS's Report on the Status of the Program's Management and to Address and Mitigate Program Risks	2	To improve management of the Visa Waiver Program and ensure that the program is properly managed, the Secretary of Homeland Security should direct the Visa Waiver Program's management to: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	DHS provided a response to this recommendation in GAO's last year. DHS has met with GAO and seeks to find a way to address the recommendation in the future.	2/1/2011
309	PLCY	GAO-11-037	2/1/2011	REDEFINING THE ASSESSMENT OF THE NORTHERN BORDER: DHS's Report on the Status of the Program's Management and to Address and Mitigate Program Risks	2	To improve management of the Visa Waiver Program and ensure that the program is properly managed, the Secretary of Homeland Security should direct the Visa Waiver Program's management to: (1) develop a plan to improve the program's management, including a timeline for implementation; (2) develop a plan to expedite processing of the program; and (3) develop a plan to address and mitigate program risks.	Consent	On April 15, 2010, DHS provided a response to this recommendation. On April 29, 2010, DHS sent GAO additional information on the program's management. GAO will close the recommendation based on the evidence presented by DHS at that time.	2/1/2011

[illegible]

[illegible]

[illegible]

#	Comp	Report Number	Report Date	Report Title	Ref #	Recommendation	Department Response	Action Item/Remarks	Responsible Completion Date
397	18-T-154	GAO-13-340	1/14/13	OVERLAP AND DUPLICATION: Federal Security Agency's (FSA) Security Program	1	In order to eliminate overlapping and potentially duplicative investigations, as well as ensure the success of such investigations, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) should coordinate their efforts to ensure that the same information is not being collected by multiple agencies, and that the same information is not being collected by multiple agencies.	Concur	The recommendations in this report are being addressed by DHS and FBI. DHS is currently reviewing the report and will provide a response by the end of the year. FBI is currently reviewing the report and will provide a response by the end of the year. DHS and FBI are currently working to ensure that the same information is not being collected by multiple agencies, and that the same information is not being collected by multiple agencies.	7/1/13
398	18-T-154	GAO-13-340	1/14/13	OVERLAP AND DUPLICATION: Federal Security Agency's (FSA) Security Program	2	In order to eliminate overlapping and potentially duplicative investigations, as well as ensure the success of such investigations, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) should coordinate their efforts to ensure that the same information is not being collected by multiple agencies, and that the same information is not being collected by multiple agencies.	Concur	The recommendations in this report are being addressed by DHS and FBI. DHS is currently reviewing the report and will provide a response by the end of the year. FBI is currently reviewing the report and will provide a response by the end of the year. DHS and FBI are currently working to ensure that the same information is not being collected by multiple agencies, and that the same information is not being collected by multiple agencies.	7/1/13
399	11-A	GAO-08-86	2/27/09	Commercial Vehicle Security: Risk Assessment and Mitigation Strategies	3	To ensure that TSA is able to more effectively assess the security of commercial vehicles in the United States, TSA should develop a risk assessment strategy that takes into account the unique characteristics of commercial vehicles, the threat to commercial vehicles, and the potential consequences of a security breach.	Concur	As of April 15, 2013, TSA is working closely with DHS and DHS is working closely with TSA to ensure that the same information is not being collected by multiple agencies, and that the same information is not being collected by multiple agencies.	7/1/13
400	15-A	GAO-09-043	4/27/09	Flight Bag Security: Actions Have Been Taken to Enhance Security, but the Program Needs Further Improvement	3	To ensure that TSA is able to more effectively assess the security of commercial vehicles in the United States, TSA should develop a risk assessment strategy that takes into account the unique characteristics of commercial vehicles, the threat to commercial vehicles, and the potential consequences of a security breach.	Concur	On September 17, 2012, GAO was all subject data submitted to address recommendations. On April 1, 2013, additional data was submitted to GAO to allow for a final recommendation.	7/1/13
401	11-A	GAO-09-043	4/27/09	Flight Bag Security: Actions Have Been Taken to Enhance Security, but the Program Needs Further Improvement	5	To ensure that TSA is able to more effectively assess the security of commercial vehicles in the United States, TSA should develop a risk assessment strategy that takes into account the unique characteristics of commercial vehicles, the threat to commercial vehicles, and the potential consequences of a security breach.	Concur	On June 20, 2013, a meeting was held with GAO to discuss what was needed to close the recommendations. Following the meeting, TSA will provide additional information on the flight bag security program and will make a final recommendation on closing the recommendations. On April 1, 2013, additional data was submitted to GAO to allow for a final recommendation.	7/1/13

#	Comp	Report Number	Report Rec'd Date	Report Title	Ref #	Recommendation	Department Response	Actions Taken/Remarks	Expected Completion Date
437	TSA	GAO-09-389	10/20/09	AVIATION SECURITY: A National Strategy and Other Actions Would Strengthen TSA's Ability to Address Commercial Airport Perimeters and Access Controls	1	To help ensure that TSA's actions in enhancing airport security are guided by a systematic risk management approach that identifies and addresses the most serious threats to the nation's aviation system, TSA should develop a risk management strategy that identifies the most serious threats to the nation's aviation system and the most effective ways to address them. TSA should also consider using information from other agencies to help inform its risk management strategy. TSA should also consider using information from other agencies to help inform its risk management strategy. TSA should also consider using information from other agencies to help inform its risk management strategy.	Concur	As of April 12, 2013, GAO has closed the recommendation on its website.	6/30/2013
438	TSA	GAO-09-389	10/20/09	AVIATION SECURITY: A National Strategy and Other Actions Would Strengthen TSA's Ability to Address Commercial Airport Perimeters and Access Controls	5	To help ensure that TSA's actions in enhancing airport security are guided by a systematic risk management approach that identifies and addresses the most serious threats to the nation's aviation system, TSA should develop a risk management strategy that identifies the most serious threats to the nation's aviation system and the most effective ways to address them. TSA should also consider using information from other agencies to help inform its risk management strategy. TSA should also consider using information from other agencies to help inform its risk management strategy.	Concur	As of April 12, 2013, GAO has closed the recommendation on its website.	6/30/2013
439	TSA	GAO-10-128	10/20/09	AVIATION SECURITY: TSA's New Research, Development, and Rapid Deploying Technologies, but Continue to Face Challenges	2	To help ensure that DHS's Science and Technology Directorate (S&TD) and Transportation Security Administration (TSA) are working together to develop and deploy new technologies that will enhance the nation's aviation security, TSA should develop a strategy to identify and address the most serious threats to the nation's aviation system and the most effective ways to address them. TSA should also consider using information from other agencies to help inform its risk management strategy. TSA should also consider using information from other agencies to help inform its risk management strategy.	Concur	TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy. TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy. TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy.	9/30/2013
440	TSA	GAO-10-128	10/20/09	AVIATION SECURITY: TSA's New Research, Development, and Rapid Deploying Technologies, but Continue to Face Challenges	3	To help ensure that DHS's Science and Technology Directorate (S&TD) and Transportation Security Administration (TSA) are working together to develop and deploy new technologies that will enhance the nation's aviation security, TSA should develop a strategy to identify and address the most serious threats to the nation's aviation system and the most effective ways to address them. TSA should also consider using information from other agencies to help inform its risk management strategy. TSA should also consider using information from other agencies to help inform its risk management strategy.	Concur	TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy. TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy. TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy.	2/28/2014
441	TSA	GAO-10-128	10/20/09	AVIATION SECURITY: TSA's New Research, Development, and Rapid Deploying Technologies, but Continue to Face Challenges	4	To help ensure that DHS's Science and Technology Directorate (S&TD) and Transportation Security Administration (TSA) are working together to develop and deploy new technologies that will enhance the nation's aviation security, TSA should develop a strategy to identify and address the most serious threats to the nation's aviation system and the most effective ways to address them. TSA should also consider using information from other agencies to help inform its risk management strategy. TSA should also consider using information from other agencies to help inform its risk management strategy.	Concur	TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy. TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy. TSA is developing a CSA and plans to complete it by August 2013. Previously, TSA provided GAO with the overall program LCSE and TSA's strategy.	2/28/2014

[illegible]

#	Comp	Report Number	Report Title	Rec #	Recommendation	Department Response	Action/Task/Remarks	Proposed Completion Date
432	TSB	GAO-12-44	Transportation Security Information Sharing: Stakeholders Generally Agree on Need for Improved Information Sharing, but Disagree on How to Improve It	4	To help strengthen information sharing with transportation stakeholders and ensure that stakeholders receive security information in a timely and useful manner, TSA should direct the Assistant Secretary for Information Systems to conduct a study to assess the current information sharing environment, identify information sharing-related performance measures to help assess the effectiveness of the current environment, and develop a security information sharing strategy.	Concur	On February 23, 2012, TSA provided DHS with the 60-day update to the report. DHS signed the 60-day update to the HLE on June 26, 2012.	12/31/2013
433	TSB	GAO-12-46	Transportation Security Information Sharing: Stakeholders Generally Agree on Need for Improved Information Sharing, but Disagree on How to Improve It	5	To help strengthen information sharing with transportation stakeholders and ensure that stakeholders receive security information in a timely and useful manner, TSA should direct the Assistant Secretary for Information Systems to conduct a study to assess the current information sharing environment, identify information sharing-related performance measures to help assess the effectiveness of the current environment, and develop a security information sharing strategy.	Concur	On February 23, 2012, TSA provided DHS with the 60-day update to the report. DHS signed the 60-day update to the HLE on June 26, 2012.	12/31/2013
434	TSB	GAO-12-46	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	1	The Secretary of Homeland Security should direct the TSA Administrator to develop a workforce staffing plan with the Assistant Secretary for Information Systems to ensure that TSA has the personnel and resources needed to conduct threat assessments, including the use of contractors, and ensure the timely completion of existing and future threat assessments.	Concur	GAO-2012-01-3802012 TSA provided DHS with the 60-day update to the recommendation. As of 4/20, the letter has not been signed by DHS and sent to the HLE. Pending status update from DHS.	12/31/2013
435	TSB	GAO-12-46	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	2	The Secretary of Homeland Security should direct the TSA Administrator to conduct an assessment of the state of the threat assessment process, including the use of contractors, and ensure the timely completion of existing and future threat assessments.	Concur	GAO-2012-01-3802012 TSA provided DHS with the 60-day update to the recommendation. As of 4/20, the letter has not been signed by DHS and sent to the HLE. Pending status update from DHS.	4/30/2013
436	TSB	GAO-12-49	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	3	The Secretary of Homeland Security should direct the TSA Administrator to develop a workforce staffing plan with the Assistant Secretary for Information Systems to ensure that TSA has the personnel and resources needed to conduct threat assessments, including the use of contractors, and ensure the timely completion of existing and future threat assessments.	Concur	GAO-2012-01-3802012 TSA provided DHS with the 60-day update to the recommendation. As of 4/20, the letter has not been signed by DHS and sent to the HLE. Pending status update from DHS.	12/31/2013
437	TSB	GAO-12-140	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	1	Recommendation is classified.	Concur	Remarks available upon request under a separate cover.	
438	TSB	GAO-12-140	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	2	Recommendation is classified.	Concur	Remarks available upon request under a separate cover.	
439	TSB	GAO-12-140	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	3	Recommendation is classified.	Non-Concur	Remarks available upon request under a separate cover.	
440	TSB	GAO-12-140	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	4	Recommendation is classified.	Concur	Remarks available upon request under a separate cover.	
441	TSB	GAO-12-140	Transportation Security: Actions Needed to Address Limitations in TSA's Threat Assessments and Growing Workload	1	To help DHS address challenges in meeting the cargo security needs of the transportation system, TSA should direct the Assistant Secretary for Information Systems to conduct a study to assess the current information sharing environment, identify information sharing-related performance measures to help assess the effectiveness of the current environment, and develop a security information sharing strategy.	Concur	As of April 8, 2013, additional information was submitted to GAO to review. TSA believes the recommendation has been fully implemented and closed its review of T-4.	12/31/2013

#	Comp	Report Number	Report Received Date	Report Title	Ref #	Recommendation	Department Response	Action Items/Remarks	Anticipated Completion Date
440	TSA	GAO-12-2835U	5/23/2012	Aviation Security: Actions Needed to Address Challenges and Potential Threats to U.S. Airports (GAO-12-2835U)	2	To help DHS address challenges in meeting the air cargo screening requirements, TSA should: (1) conduct a comprehensive review of TSA's current cargo screening policies and procedures to ensure they are effective and efficient; and (2) develop and implement a plan to improve cargo screening efficiency and effectiveness.	GAO-12-2835U	As of April 9, 2013, additional information was submitted to GAO for review. TSA delivers the recommendation has been fully implemented and should be closed by GAO.	10/20/2012
441	TSA	GAO-12-286	4/27/2012	Aviation Security: TSA Has Not Fully Implemented the Requirements of the Registered Air Carrier Security Program in the United States (GAO-12-286)	1	To ensure TSA's current estimates and related savings of TSA's estimate that its cost estimates conform to cost estimating best practices.	GAO-12-286	The DHS signed EO-day update to the law and on August 17, 2012, Recommendation implementation is expected by September 30, 2013.	9/30/2013
442	TSA	GAO-12-4085U	6/1/2012	General Aviation Security: Weaknesses in TSA's Program to Monitor and Respond to Security Threats	1	To better ensure that TSA is able to develop effective and efficient security programs for general aviation operators, GAO recommends that the Administrator of TSA take the following actions: (1) conduct a comprehensive review of TSA's current security programs for general aviation operators; (2) develop and implement a plan to improve TSA's current security programs for general aviation operators; and (3) conduct a comprehensive review of TSA's current security programs for general aviation operators.	GAO-12-4085U	TSA is working with data received from the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs.	9/30/2013
443	TSA	GAO-12-4085U	6/1/2012	General Aviation Security: Weaknesses in TSA's Program to Monitor and Respond to Security Threats	2	To better ensure that TSA is able to develop effective and efficient security programs for general aviation operators, GAO recommends that the Administrator of TSA take the following actions: (1) conduct a comprehensive review of TSA's current security programs for general aviation operators; (2) develop and implement a plan to improve TSA's current security programs for general aviation operators; and (3) conduct a comprehensive review of TSA's current security programs for general aviation operators.	GAO-12-4085U	As of April 12, 2013, the authorized system for tracking the Department of Defense (DOD) requirements letters granted to foreign operators seeking flight training in the United States is operational and in use. In December 2012, TSA provided GAO with supporting documentation to ensure GAO has accurate history of and data on the recommendations.	6/30/2013
444	TSA	GAO-12-4085U	6/1/2012	General Aviation Security: Weaknesses in TSA's Program to Monitor and Respond to Security Threats	3	To better ensure that TSA is able to develop effective and efficient security programs for general aviation operators, GAO recommends that the Administrator of TSA take the following actions: (1) conduct a comprehensive review of TSA's current security programs for general aviation operators; (2) develop and implement a plan to improve TSA's current security programs for general aviation operators; and (3) conduct a comprehensive review of TSA's current security programs for general aviation operators.	GAO-12-4085U	TSA is working with data received from the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs.	7/1/2013
445	TSA	GAO-12-4085U	6/1/2012	General Aviation Security: Weaknesses in TSA's Program to Monitor and Respond to Security Threats	4	To better ensure that TSA is able to develop effective and efficient security programs for general aviation operators, GAO recommends that the Administrator of TSA take the following actions: (1) conduct a comprehensive review of TSA's current security programs for general aviation operators; (2) develop and implement a plan to improve TSA's current security programs for general aviation operators; and (3) conduct a comprehensive review of TSA's current security programs for general aviation operators.	GAO-12-4085U	TSA and DHS, Communications and Criminal Exploitation Unit (CCEU) have completed the pilot program identified in the original report. TSA is working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs.	11/1/2013
446	TSA	GAO-12-4085U	7/1/2012	Aviation Security: TSA Has Not Fully Implemented the Requirements of the Registered Air Carrier Security Program in the United States (GAO-12-4085U)	1	To ensure TSA's current estimates and related savings of TSA's estimate that its cost estimates conform to cost estimating best practices.	GAO-12-4085U	Remarks available upon request under a separate cover.	
447	TSA	GAO-12-4085U	7/1/2012	Aviation Security: TSA Has Not Fully Implemented the Requirements of the Registered Air Carrier Security Program in the United States (GAO-12-4085U)	2	To ensure TSA's current estimates and related savings of TSA's estimate that its cost estimates conform to cost estimating best practices.	GAO-12-4085U	Remarks available upon request under a separate cover.	
448	TSA	GAO-13-423	11/1/2012	Transportation Security Administration: Review of TSA's Current Security Programs	1	TSA Administrator should establish a consistent policy to ensure agency-wide efforts for reviewing, tracking, and reporting recommendations from GAO and other sources.	GAO-13-423	TSA is developing a new TSA Management Directive (MD) which will describe the roles and responsibilities of an involved office in implementing recommendations from GAO and other sources. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs. TSA is also working with the FAA to determine if foreign operators are being trained by authorized FAA Certified Flight Instructor (CFI) programs.	11/30/2013

[illegible]

#	Comp. Category	Report Number	Report Title	Recommendation	Department Function	Action/Implementation	Project Completion Date
468	USCIS	GAO-13-26	Passenger and Security Constraints for Airline Program Operations	3	Continued a process for updating the business when incidents occur and for identifying and addressing the associated security compliance activities.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	6/30/2013
469	TSA	GAO-13-30	Passenger and Security Constraints for Airline Program Operations	4	Developing guidance for TSA's research that involves interviews of TSA's staff to identify and address issues resulting from data entry errors.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	3/31/2013
470	USCIS	GAO-13-30	Passenger and Security Constraints for Airline Program Operations	5	Establishing a security process for reporting and addressing security incidents that could lead to the agency misbehavior or non-compliance with TSA's security requirements.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	6/30/2013
471	TSA	GAO-13-30	Passenger and Security Constraints for Airline Program Operations	6	Establishing a security process for reporting and addressing security incidents that could lead to the agency misbehavior or non-compliance with TSA's security requirements.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	6/30/2013
472	USCIS	GAO-13-30	Passenger and Security Constraints for Airline Program Operations	7	Establishing a security process for reporting and addressing security incidents that could lead to the agency misbehavior or non-compliance with TSA's security requirements.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	6/30/2013
473	USCIS	GAO-13-30	Passenger and Security Constraints for Airline Program Operations	8	Establishing a security process for reporting and addressing security incidents that could lead to the agency misbehavior or non-compliance with TSA's security requirements.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	6/30/2013
474	USCIS	GAO-13-30	Passenger and Security Constraints for Airline Program Operations	9	Establishing a security process for reporting and addressing security incidents that could lead to the agency misbehavior or non-compliance with TSA's security requirements.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	6/30/2013
475	USCIS	GAO-13-30	Passenger and Security Constraints for Airline Program Operations	10	Establishing a security process for reporting and addressing security incidents that could lead to the agency misbehavior or non-compliance with TSA's security requirements.	On 12/19/13, DHS updated the TSA's new software agreement in place for USDO Compliance to update the TSA's of an unreported security misbehavior of the conclusion of an audit or inspection activity of the TSA. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review. The TSA's new software agreement in place for USDO Compliance is currently under review.	6/30/2013

[illegible]

#	Comp.	Report Number	Report Title	Report Due	Rec #	Recommendation	Department	Action Items/Remarks	Project Completion Date
476	USCG	GAO-11-670	Efforts to Identify Active Requirements for Air Pollution Monitoring Equipment	8/1/2011	1	To achieve effective communication and relationship with stakeholders, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	Coast Guard plans to communicate with these stakeholders in the process and progress of the active planning efforts. GAO has identified under audit an 180,000-ton oil tanker (Oscar) that is scheduled to be replaced by a new ship in the next few years. The new ship will have the same tonnage as the Oscar.	12/1/2013
477	USCG	GAO-11-207	Maritime Security: Ferry Security	12/22/2010	1	To ensure that the Coast Guard conducts its known risks for securing the ferry transportation system and is not missing any risks, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	The Coast Guard established a governmentwide working group in Spring 2011. In other administrative work on the studies and their findings, the Coast Guard is working with the Department of Justice to develop a plan to address the security of ferries. Current and future work will be determined by the findings and no further changes were recommended or underway. USCG is working closely with GAO.	8/1/2013
478	USCG	GAO-11-207	Maritime Security: Ferry Security	12/22/2010	2	To ensure that the Coast Guard conducts its known risks for securing the ferry transportation system and is not missing any risks, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	The Coast Guard established a governmentwide working group in Spring 2011. In other administrative work on the studies and their findings, the Coast Guard is working with the Department of Justice to develop a plan to address the security of ferries. Current and future work will be determined by the findings and no further changes were recommended or underway. USCG is working closely with GAO.	8/1/2013
479	USCG	GAO-11-319	Efforts to Identify Active Requirements for Air Pollution Monitoring Equipment	8/1/2011	1	To achieve effective communication and relationship with stakeholders, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	Coast Guard plans to communicate with these stakeholders in the process and progress of the active planning efforts. GAO has identified under audit an 180,000-ton oil tanker (Oscar) that is scheduled to be replaced by a new ship in the next few years. The new ship will have the same tonnage as the Oscar.	12/1/2013
480	USCG	GAO-11-319	Efforts to Identify Active Requirements for Air Pollution Monitoring Equipment	8/1/2011	2	To ensure that the Coast Guard conducts its known risks for securing the ferry transportation system and is not missing any risks, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	The Coast Guard established a governmentwide working group in Spring 2011. In other administrative work on the studies and their findings, the Coast Guard is working with the Department of Justice to develop a plan to address the security of ferries. Current and future work will be determined by the findings and no further changes were recommended or underway. USCG is working closely with GAO.	12/1/2013
481	USCG	GAO-11-319	Efforts to Identify Active Requirements for Air Pollution Monitoring Equipment	8/1/2011	3	To ensure that the Coast Guard conducts its known risks for securing the ferry transportation system and is not missing any risks, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	The Coast Guard established a governmentwide working group in Spring 2011. In other administrative work on the studies and their findings, the Coast Guard is working with the Department of Justice to develop a plan to address the security of ferries. Current and future work will be determined by the findings and no further changes were recommended or underway. USCG is working closely with GAO.	12/1/2013
482	USCG	GAO-11-319	Efforts to Identify Active Requirements for Air Pollution Monitoring Equipment	8/1/2011	4	To ensure that the Coast Guard conducts its known risks for securing the ferry transportation system and is not missing any risks, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	The Coast Guard established a governmentwide working group in Spring 2011. In other administrative work on the studies and their findings, the Coast Guard is working with the Department of Justice to develop a plan to address the security of ferries. Current and future work will be determined by the findings and no further changes were recommended or underway. USCG is working closely with GAO.	12/1/2013
483	USCG	GAO-11-319	Efforts to Identify Active Requirements for Air Pollution Monitoring Equipment	8/1/2011	5	To ensure that the Coast Guard conducts its known risks for securing the ferry transportation system and is not missing any risks, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	The Coast Guard established a governmentwide working group in Spring 2011. In other administrative work on the studies and their findings, the Coast Guard is working with the Department of Justice to develop a plan to address the security of ferries. Current and future work will be determined by the findings and no further changes were recommended or underway. USCG is working closely with GAO.	12/1/2013
484	USCG	GAO-11-319	Efforts to Identify Active Requirements for Air Pollution Monitoring Equipment	8/1/2011	6	To ensure that the Coast Guard conducts its known risks for securing the ferry transportation system and is not missing any risks, the Coast Guard should include information on the progress and progress of Air Pollution Monitoring Equipment on the progress and progress of Air Pollution Monitoring Equipment.	OSCAR	The Coast Guard established a governmentwide working group in Spring 2011. In other administrative work on the studies and their findings, the Coast Guard is working with the Department of Justice to develop a plan to address the security of ferries. Current and future work will be determined by the findings and no further changes were recommended or underway. USCG is working closely with GAO.	12/1/2013

[illegible]

[illegible]

#	Comp.	Report Number	Report Title	Report Received Date	Report #	Recommendation	Department Action	Actions Taken/Remarks	Reported Completion Date
529	USCIS	GAO-11-26	Measuring the impact of the I-10 visa cap on U.S. employers.	1/14/2011	1	To help ensure that the number of new I-10 visas is not subject to the cap with entering the United States and that the cap is not applied to the I-10 visas that are already in the United States, USCIS should take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States.	Non-Courier	USCIS did not discuss with this recommendation because it has been working with DHS, and collaborating with the Dept. of State, to track the I-10 visas that are already in the United States. USCIS did not discuss with this recommendation because it has been working with DHS, and collaborating with the Dept. of State, to track the I-10 visas that are already in the United States. USCIS did not discuss with this recommendation because it has been working with DHS, and collaborating with the Dept. of State, to track the I-10 visas that are already in the United States.	10/10/14
530	USCIS	GAO-11-26	Measuring the impact of the I-10 visa cap on U.S. employers.	1/14/2011	2	To address business concerns without undermining program integrity, USCIS should take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States.	Non-Courier	USCIS did not discuss with this recommendation for a variety of reasons, including that the technology existing process could make it difficult to track the I-10 visas that are already in the United States. USCIS did not discuss with this recommendation because it has been working with DHS, and collaborating with the Dept. of State, to track the I-10 visas that are already in the United States. USCIS did not discuss with this recommendation because it has been working with DHS, and collaborating with the Dept. of State, to track the I-10 visas that are already in the United States.	10/10/14
531	USCIS	GAO-11-14	Employment Verification: Federal Agencies Have Taken Steps to Improve Tracking of Employment Challenges	1/15/2011	3	To ensure that employees have the ability to access and use their employment verification information, USCIS should take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States.	Courier	In March 2013, USCIS Verification officials conferred with GAO to provide a program report and to discuss recommendation requirements. USCIS officials reported actions addressing USCIS personnel, reporting approaches to ensure the consistency of data, and the use of the USCIS Verification system. USCIS officials reported actions addressing USCIS personnel, reporting approaches to ensure the consistency of data, and the use of the USCIS Verification system. USCIS officials reported actions addressing USCIS personnel, reporting approaches to ensure the consistency of data, and the use of the USCIS Verification system.	9/8/2013
532	USCIS	GAO-11-148	Employment Verification: Federal Agencies Have Taken Steps to Improve Tracking of Employment Challenges	1/15/2011	7	To ensure that USCIS has a clear plan for meeting business needs, USCIS should take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States.	Courier	USCIS Verification officials conferred with GAO in March 2013 to provide a program report. The USCIS Verification officials reported actions addressing USCIS personnel, reporting approaches to ensure the consistency of data, and the use of the USCIS Verification system. USCIS officials reported actions addressing USCIS personnel, reporting approaches to ensure the consistency of data, and the use of the USCIS Verification system.	6/20/2013
533	USCIS	GAO-12-66	Immigration Benefits: Consistent Adherence to DHS's Acquisition Policy Could Help Improve Transformation Program Outcomes	11/22/2011	1	To help ensure that USCIS takes a comprehensive and consistent approach to the development and implementation of its immigration benefits programs, USCIS should take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States.	Courier	USCIS continues to take steps to ensure program activities are consistent with the new staffing best practices. USCIS also continues to provide quarterly updates to GAO regarding its progress relative to the new best practices. The full implementation of USCIS's electronic migration system (ELS) is not expected until FY 2015.	9/30/2015
534	USCIS	GAO-13-66	Immigration Benefits: Consistent Adherence to DHS's Acquisition Policy Could Help Improve Transformation Program Outcomes	11/22/2011	2	To help ensure that USCIS takes a comprehensive and consistent approach to the development and implementation of its immigration benefits programs, USCIS should take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States.	Courier	Applying to the Office of Transformation Coordination's (OTC) implementation of ALE, software development, Rolling Wave Approach has been implemented into the acquisition process. The technique enables progressive elaboration in planning. The OTC has been working with USCIS to ensure that the OTC's implementation of ALE is consistent with the new staffing best practices. The OTC has been working with USCIS to ensure that the OTC's implementation of ALE is consistent with the new staffing best practices.	9/30/2013
535	USCIS	GAO-13-66	Immigration Benefits: Consistent Adherence to DHS's Acquisition Policy Could Help Improve Transformation Program Outcomes	11/22/2011	3	To help ensure that USCIS takes a comprehensive and consistent approach to the development and implementation of its immigration benefits programs, USCIS should take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States. USCIS should also take steps to improve its tracking of the I-10 visas that are already in the United States.	Courier	The Office of Transformation Coordination (OTC) has been working with USCIS to ensure that the OTC's implementation of ALE is consistent with the new staffing best practices. The OTC has been working with USCIS to ensure that the OTC's implementation of ALE is consistent with the new staffing best practices.	5/31/2013

#	Entity	Report Number	Report Review Date	Report Title	Rec #	Recommendation	Disputed Position	Action Taken/Results	Projected Completion Date
538	USCIS	OAD-12-274	12/16/2017	Immigrant Integration U.S. Citizenship and Naturalization Service (CNS) Grant Program	1	The program is currently being evaluated by the Citizenship and Naturalization Service (CNS) and the results of the evaluation will be reported to the USCIS by the end of 2017. The results of the evaluation will be used to determine if the program should be continued, modified, or terminated. We recommend that the Secretary of Homeland Security take the following action: The program should be continued with the following modifications: - The program should be expanded to include the following states: [list of states] - The program should be expanded to include the following types of grants: [list of grant types] - The program should be expanded to include the following types of activities: [list of activities]	Concur	On November 16, 2017, DHS submitted a Federal Register Notice, as recommended by USCIS, regarding how the allocation methodology for the grant program will be determined. The notice states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register.	5/1/2019
539	USCIS	OAD-13-875	9/27/2017	Commonwealth of the Northern Mariana Islands (CNMI) Additional Employment Program	1	We recommend that the Secretary of Homeland Security take the following action: The program should be continued with the following modifications: - The program should be expanded to include the following states: [list of states] - The program should be expanded to include the following types of grants: [list of grant types] - The program should be expanded to include the following types of activities: [list of activities]	Concur	In November 2012, DHS submitted a Federal Register Notice, as recommended by USCIS, regarding how the allocation methodology for the grant program will be determined. The notice states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register.	11/30/2017
539	USCIS	OAD-13-875	9/27/2017	Commonwealth of the Northern Mariana Islands (CNMI) Additional Employment Program	2	We recommend that the Secretary of Homeland Security take the following action: The program should be continued with the following modifications: - The program should be expanded to include the following states: [list of states] - The program should be expanded to include the following types of grants: [list of grant types] - The program should be expanded to include the following types of activities: [list of activities]	Non-Concur	On November 16, 2017, DHS submitted a Federal Register Notice, as recommended by USCIS, regarding how the allocation methodology for the grant program will be determined. The notice states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register.	6/30/2019
539	USCIS	OAD-13-108	10/1/2017	U.S. Visa Program: Manufacturing and High-Tech Occupations Pilot Program	1	The program is currently being evaluated by the Citizenship and Naturalization Service (CNS) and the results of the evaluation will be reported to the USCIS by the end of 2017. The results of the evaluation will be used to determine if the program should be continued, modified, or terminated. We recommend that the Secretary of Homeland Security take the following action: The program should be continued with the following modifications: - The program should be expanded to include the following states: [list of states] - The program should be expanded to include the following types of grants: [list of grant types] - The program should be expanded to include the following types of activities: [list of activities]	Concur	On November 16, 2017, DHS submitted a Federal Register Notice, as recommended by USCIS, regarding how the allocation methodology for the grant program will be determined. The notice states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register. The notice also states that the allocation methodology will be determined by the Secretary of Homeland Security, in consultation with the USCIS, and will be published in the Federal Register.	12/31/2019

**Post-Hearing Questions for the Record
Submitted to the Honorable Elaine C. Duke
From Senator Thomas R. Carper**

**“The Department of Homeland Security at 10 Years: A Progress Report on Management”
March 21, 2013**

1. I have concerns in the context of this fiscal climate about the ability of the Department to sustain the management improvements that have been made over the years. Many of these initiatives commenced during your tenure as the Under Secretary for Management. What area or areas of progress are most at risk if there are funding reductions to management functions, and what will be the impact in the next 5-10 years?

DHS Management is integral to the continuing integration of the Department. A significant amount of progress has been made in maturing DHS under the functional authority of the business chiefs, especially in the areas of procurement, acquisition, information technology, and budget and finance. Cuts to the USM offices will reduce its ability to drive these integration functions. Integration of management (doing business in a way that drives effectiveness and efficiency) will stall as the remaining staff must focus on keeping daily activities moving instead of continuing to drive maturity.

Additionally, I do not think the Integrated Investment Lifecycle Model (IILCM) will be implemented if there are significant funding reductions to USM. The components of this model are essential for the continued maturation of the Department. The IILCM will take the pillars, or building blocks, currently in place and use them in an integrated manner to drive effectiveness. Establishing the policy council is essential as DHS begins its second quadrennial homeland security review (QHSR). Used in the IILCM, the QHSR will drive capabilities and requirements discussions, which will in turn drive investments. The capacities and requirements council will institute the much needed joint look at mission. That jointness is critical for both more effective mission operations – seamless delivery of homeland security, but also better management – eliminated duplications and driving efficiency.

2. The final enacted Fiscal Year 2013 Continuing Appropriation reduced DHS management by \$17 million. Additionally, DHS was further reduced by the 5% required under “sequestration”. What are your concerns about these reductions? And if you were still the Under Secretary for Management, what types of choices do you think you would have to make to absorb that cut?

The majority of employees under the Under Secretary for Management (USM) work in the six business lines, or “chiefs”. In each of these areas, Chief Financial Officer, Chief Procurement Officer, Chief Information Officer, Chief Readiness and Logistics Support Officer, Chief Security Officer, and Chief Human Capital Officer, the employees perform two critical functions. First, they provide governance and oversight of their respective functional areas. Without that governance and oversight, the first line of defense against inefficiencies, ineffectiveness, and inappropriateness is outside oversight bodies such as the Inspector General and General Accountability Office. While their oversight is valuable, it is neither comprehensive nor timely enough to manage the risk of the \$52B+ DHS enterprise. The second function is

more operational. The USM personnel award contracts, manage acquisition programs, grant security clearances, hire personnel, and run information technology systems. These functions are integral to the operations of DHS, and if these necessary indirect costs are not funded, it will have negative impact on the direct mission programs. They will not be managed from an acquisition perspective adequately, there will be gaps in hiring, longer cycle times for clearances, space, and other support necessary to accomplish the DHS missions.

As USM, likely the first cuts would have to be to oversight and governance. Initially, any improvements and enhancements would be stalled, then oversight and governance would be reduced. That would be necessary because the operational functions provided are critical to the day-to-day operations of DHS, and could not be reduced.

3. In your testimony, you emphasized that “management and mission are not separate events”, and that “management delivers the mission” of DHS. How important is a collocated and centralized DHS management and mission leadership team to continued improvement at the Department?

My testimony did emphasize that management and mission (or operations) must work together to deliver homeland security, and I think collocated and centralized DHS management and mission leadership team contributes greatly to that effectiveness. Within DHS headquarters, it is critical. Mission must inform management, and vice versa. The collocation and centralization helps facilitate that happening in a cohesive manner. DHS was formed to eliminate redundancies and fill gaps in homeland security, and a disparate organizational structure and geographic locations make that goal difficult to achieve. For the component leadership, I believe they must wear two hats. They must be an integral part of the DHS leadership team. If there is a DHS headquarters campus, I believe they must have some presences at that location. They should serve, in their headquarters hat, as part of a board of directors. Operating component heads also must lead their mission components, and therefore also need a collocation with that entity. In making the collocating and centralizing decisions, I believe it is important to consider an “optimization” concept. Either too much centralization or too little centralization will impair operations. The amount should be optimized to facilitate a cohesive Department, while also facilitating the unique operations of the components.

4. Are there any legislative authorities that you would recommend we change or institute for the Department that would enhance management and reduce risk?

I recommend that you consider an acquisition model that facilitates industry infusion of capital into DHS investments, such as private/public partnerships and share in savings. These models have been used effectively in special cases throughout the federal government, but legislative and regulatory restrictions limit their applicability. These types of acquisition arrangements have two major benefits. First, it allows DHS to continue its integration initiatives without the need for 100% funding in the initial years. It balances the federal government’s investment over a reasonable business cycle. Second, it provides an allocation of business risk that is more even across industry and the government. Industry must assume more of the business risk for cost, performance, and schedule risk than in a traditional contract where the business is reimbursed for all costs and profit up front. The government also has appropriate cost, schedule and performance risk through a longer, program based contract with defined results. There are successful models in both the federal and commercial sectors to pursue this, and if the Committee does want to consider this recommendation, I would be pleased to meet with the staff and discuss in more detail.

**Post-Hearing Questions for the Record
Submitted to the Honorable Richard L. Skinner
From Senator Thomas R. Carper**

**“The Department of Homeland Security at 10 Years: A Progress Report On Management”
March 21, 2013**

1. Are there any legislative authorities that you would recommend we change or institute for the Department that would enhance management and reduce risk?

I do not believe that new legislative authorities or changes are needed to enhance management and reduce risk within the department. Management improvements and risk reduction initiatives should be priorities of the Secretary and her executive team, and can be implemented without new legislative mandates or authorities. What is needed, however, is strong Congressional oversight and support to ensure that the Department: does not short change its management support functions when it formulates its annual budgets; articulates clear and attainable goals and objectives, with performance metrics, for its management support initiatives; and, holds its leadership team accountable for attaining those initiatives.

2. In your testimony you point out a number of problems that the Department still has with respect to its information technology systems – for example, the need to modernize information technology in FEMA and Customs and Border Protection. What do you think are the underlying causes of these problems? Is it a lack of funds, or a scarcity of skilled personnel to oversee these projects, or something else?

I do not believe a "lack of funds" is the underlying cause. Within FEMA, I believe the problems can be traced to a lack of sustained IT leadership, management support, and in-house resistance to change, particularly within the Response and Recovery Directorate. Consequently, FEMA has not completed its efforts to establish an enterprise architecture and an IT strategic plan to coordinate and prioritize its modernization initiatives and IT projects. To be successful, FEMA needs strong IT leadership, equipped with the authority to make improvements, and, most importantly, the backing of the DHS CIO, FEMA Administrator, and Secretary. Within CBP, I believe it set its expectations too high, tried to do too much too fast, and lacked the skilled personnel to manage and oversee its projects. This is understandable given its mandate and the pressures placed on it by the Congress and the public after the 9/11 terrorist attacks. Because of this, unfortunately, many of its IT initiatives failed or proved to be wasteful. In my opinion, the public would be better served if CBP would take a more disciplined, phased approach to modernizing its IT systems, recognizing its limited ability to manage and oversee complex, highly expensive projects.

3. GAO, in its High Risk update, gives good marks to the Department for strengthening the governance structure over information technology, which is led by the Department's Chief Information Officer. Do you agree with GAO's assessment on this point, and if so,

are there promising reforms that Congress could help push that would address the type of problems you detail in your testimony?

Yes, I agree with GAO's assessment, but I do not believe the CIO has been given sufficient authority over the IT budgets of the DHS components. While the CIO plays a bigger role in the governance structure over information technology within the department, the CIO has little oversight or control over component IT budgets - at least during my tenure. Budget submissions and IT proposals are generally reviewed and approved independently of one another. Oftentimes, DHS component budgets are reviewed and approved prior to the submission of a component's IT proposal - too late for the CIO to weigh in on the merits of the proposal, or too late to stop or curtail funding for a project that may not comply with the department's enterprise architecture.

HARNESSING SCIENCE AND TECHNOLOGY TO PROTECT NATIONAL SECURITY AND ENHANCE GOVERNMENT EFFICIENCY

WEDNESDAY, JULY 17, 2013

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:10 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Thomas R. Carper, presiding.

Present: Senators Carper, Pryor, McCaskill, and Coburn.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. Good morning, everyone. The hearing will come to order.

Welcome, one and all. Secretary O'Toole, Mr. Maurer, happy to see you. Is there a baseball player in the American league, a catcher named Maurer?

Mr. MAURER. Yes, there is, although he spells his last name incorrectly.

Chairman CARPER. Yes.

Mr. MAURER. He drops that first "r."

Chairman CARPER. Yes, he only has one "r." [Laughter.]

Even without that second "r," he still is a great player.

Mr. MAURER. Oh, he is an amazing ballplayer, absolutely.

Chairman CARPER. Yes. What was the final score last night of the All-Star Game, do you have any idea?

Mr. MAURER. It was three-nothing.

Chairman CARPER. Was it National League or American League?

Mr. MAURER. American League.

Chairman CARPER. I thought it was the American. I was in a meeting this morning—I am an American League fan, a huge Tigers fan, and the Tigers had about six players last night plus the manager—and I think Rivera, the Yankees pitcher, was on the front page of the New York Times and won Most Valuable Player (MVP) at the age of 42, I think. Pretty amazing. It said under the picture—great picture of him coming out and taking the curtain call—that the American League won, three-to-nothing.

And I went to a meeting this morning and I was very proud as an American League fan to tell everybody how we had won, and even though a Yankee—I am not a big Yankees fan—had been the MVP, what a good night it was for baseball and for folks on our

side of the aisle. And everybody said, no, the National League won. So thank you. [Laughter.]

Thank you for setting the record straight. We worry here about nuclear options and trying to make sure the place does not have a meltdown, but the really important stuff is going on in baseball stadiums around the country, including guys named Mauer. So we welcome both of you.

On a more serious note, earlier this year, as we all know, the Department of Homeland Security (DHS) turned 10 years old, not a baby anymore, not a toddler, not an infant, but a young strapping 10-year-old. To mark that anniversary, Dr. Coburn, and I announced that this Committee would hold a series of hearings examining whether the Department of Homeland Security is effectively and efficiently accomplishing its core missions.

Today's hearing is the second in a series. Actually, it is, I think, more than the second in a series, but it is one of a series of hearings that is going to focus on the role of the Science and Technology (S&T) Directorate.

The threats, as we all know, to our national security evolve constantly. So, too, then, must the strategies and technologies we use to combat them.

I am an old Navy guy, about 23 years as a Naval Flight Officer (NFO), and I have often said, as have others before me, that the military are pretty good at fighting the last war. We are not as good at anticipating what the next one is. That is where the Science and Technology Directorate comes in, to help us to fight the next war and the next. The threat that we face today is a whole lot different than the one we faced when I was on active duty as a Reserve Naval Flight Officer.

The work performed by the men and women at the Directorate cut across all the various components and missions of the Department, and that work involves the harnessing of cutting-edge technology and research and development (R&D) projects from the private sector, from universities, national labs, to deploy what I call force multipliers that can make us more effective in the effort we have embarked on after September 11, 2001, to prevent and respond to terrorist attacks and natural disasters.

In essence, the Science and Technology Directorate functions as a problem solver when it is at its best. For example, the Science and Technology Directorate works closely with the Transportation Security Administration (TSA) and the Defense Advanced Research Projects Agency (DARPA), to develop a better x-ray system for checked baggage. As a result of that work, a 10-percent reduction in false alarms rate is expected. This is projected to save millions of dollars in efficiencies each year through the reallocation of staffing costs.

As another example, the Directorate examined agent operations at two stations along the Southwestern border in Texas that processed, and apprehended illegal immigrants. They recommended improvements to their operations that enable the two border stations to significantly reduce their processing time, saving up to 2 hours per illegal immigrant processed. This enabled an additional officer to remain in the field rather than be stuck in the office processing paperwork.

In its early days, the Directorate was the subject of criticism as it carved out its own role in the Department. It focused, then, on basic research, which in some instances could not be quickly put to use. Today, we are told that the Directorate has proven itself to be more effective, more often than it has been at least in the past, and it has a laser focus on development of critically needed products that can be used immediately.

As we all know, the fiscal environment in our Federal Government has been very challenging over the past couple of years, and this underscores the urgent need for agencies across government to spend our taxpayer dollars more wisely. The Science and Technology Directorate can and has been a key part of the Department of Homeland Security's efforts in that regard. It is critical that it continue, that this Directorate continue to work aggressively and effectively with the components of the Department and with first responders to find solutions that allow the Department of Homeland Security and its partners across the country to operate more effectively and more efficiently.

We thank the witnesses for coming today. We look forward to your testimony, especially about how we can continue to use the Science and Technology Directorate to get better results for less money. That is the recurring theme of this Committee and the oversight work that we do. It is something that I am determined to use my Chairmanship of this Committee, in partnership with Dr. Coburn and our colleagues here, to push throughout our Federal Government.

And when Dr. Coburn arrives—we have a vote underway and I got there right at the beginning of the vote. He is probably voting and will come here and join us shortly, and when he does, he is welcome to make any comments that he wishes to do at that time.

And with that having been done, let me just briefly introduce our witnesses. This is a small panel, so I will be fairly brief.

Our first witness is Dr. Tara O'Toole, Under Secretary for Science and Technology at the Department of Homeland Security since November 2009. Prior to this appointment, Dr. O'Toole served as Chief Executive Officer (CEO) and Director of the Center for Biosecurity at the University of Pittsburgh Medical Center and was a Professor of Medicine and Public Health at the University—are they the Panthers? University of Pittsburgh Panthers. You did not go to school there. You were not a Panther in college, were you? Where did you go to school?

Dr. O'TOOLE. I went to Vassar College.

Chairman CARPER. Vassar, OK. There we go. All right.

In addition, Dr. O'Toole previously served as Assistant Secretary of Energy for Environment, Safety, and Health at the Department of Energy (DOE). When did you serve in that capacity?

Dr. O'TOOLE. Ninety-three to 1997.

Chairman CARPER. OK. We thank you for joining us today and for your leadership at the Department. We look forward to your testimony.

Our next witness is Mr. David Maurer, Director of the U.S. Government Accountability Office's (GAOs) Homeland Security and Justice Team. Mr. Maurer began his career with the Government Accountability Office in the 1990s and worked in several key areas,

such as GAO's International Affairs and Trade Team, where he led the review of the United States' effort to combat several international issues, including terrorism and weapons of mass destruction.

We thank you for joining us, Mr. Maurer. We really thank our friends at GAO, great partners with us, and we relish our partnership and hope we can continue to have it for a long time.

Your full statements will be made part of the record. You are welcome to abbreviate if you like. Sometimes we say, use our guidelines. It should be about a 5-minute statement. If you go a little bit beyond that, that is OK. If you go way beyond that, we will have to rein you in, all right. If it is noon and you are still giving your opening statement, that is probably too long. [Laughter.]

Welcome. We are glad you are all here. Please proceed.

Dr. O'TOOLE. Shall I go first, Mr. Chairman?

Chairman CARPER. We had a flip of the coin earlier and you lost—

Dr. O'TOOLE. I won?

Chairman CARPER [continuing]. So you get to go first.

TESTIMONY OF HON. TARA J. O'TOOLE, M.D.,¹ MPH, UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY, U.S. DEPARTMENT OF HOMELAND SECURITY

Dr. O'TOOLE. OK. Well, first of all, thank you very much for this opportunity to talk about the Directorate of Science and Technology in the Department of Homeland Security and where we have come from and what we are doing now and how we make the operational missions of Homeland Security and the work of first responders more effective, more efficient, and safer.

What I am going to do is give a very brief history of the Department and then talk about how we do our work today and illustrate that work with a few examples of projects that we have engaged in.

From the beginning in 2003, Congress charged S&T with very broad and ambitious responsibilities for conducting R&D, for overseeing testing and evaluation of DHS missions in the first responder community. The Directorate is also responsible for assessing biological, chemical, and emerging threats to the United States and with operation of five National Laboratories. S&T also manages nine university-based Centers of Excellence (COEs), which collectively represent consortia of over 275—

Chairman CARPER. Let me just interrupt. I said earlier roughly 5 minutes for your opening statement. Feel free to go as long as 10 minutes, OK.

Dr. O'TOOLE. Thank you very much.

So, nine COEs, 275 colleges. We also have international agreements with 13 countries bilaterally, and all of this greatly augments our ability to engage out into the dynamic global R&D community.

Senator. Shall I pause and let Senator Coburn make his remarks?

Senator COBURN. I do not have any remarks.

¹The prepared statement of Ms. O'Toole appears in the Appendix on page 309.

Dr. O'TOOLE. OK.

Chairman CARPER. Yes, he does. [Laughter.]

And we will hear them later, I hope. All right. Please proceed. Thanks. Welcome, Tom.

Dr. O'TOOLE. The first Under Secretary of Science and Technology, Dr. Charles McQueary, undertook the heroic task of standing up the Directorate even as the Department itself was getting underway. When he began, S&T was housed in another government building where meetings were held in the cafeteria and staff had to share chairs.

Understandably, the R&D efforts of that era were less connected to the immediate operational needs of the Department, which was just getting underway, than is the case today, and there was a much stronger emphasis on basic scientific research.

The second Under Secretary, Admiral James Cohen, did the country a great service by emphasizing the importance of linking S&T's research more directly to the customers, that is, the DHS operational components and first responders, and he moved the Directorate toward more applied research.

As you said, I became Under Secretary in November 2009. Although only 6 years had passed since Congress created the Department and the Directorate, it was clear very quickly that the Homeland Security missions confront a constantly evolving landscape of adaptive adversaries, evolving threats, critical infrastructure vulnerabilities, and growing operational challenges.

The wars in Iraq and Afghanistan have brought us Improvised Explosive Devices (IEDs) using homemade explosives, requiring different detection strategies. Cybersecurity has become a top concern, as has the need to cope with huge amounts of data in order to find and intercept the illicit cargo or discover would-be terrorists within the global airline system.

My first year at DHS included the H1N1 influenza pandemic, the Haitian earthquake, the airline bombing by Abdulmutallab, and the Deepwater oil spill. We were also in the middle of the economic downturn.

Moreover, the Department now faces the need to cope with inexorable increases in commerce and travel in a setting of flat or declining Federal budgets. So to maintain service and security and the flow of trade essential to our economic well-being, we have to find better, more efficient ways of carrying out DHS missions.

New technologies, better analytical approaches are critical to successfully countering new and enduring threats and to meeting these growing operational demands. Science, technology, and analytics are the keys to doing more with less.

To better address such challenges, S&T has over the past 5 years made significant changes in the way we do research and development. Let me briefly describe how S&T does its work today.

To deliver new technologies or knowledge products to DHS components and the first responders with significant operational impact, that is, create new capabilities or improvements in effectiveness and efficiency or safety, S&T had to transition new products to use in the field over much shorter timeframes than the typical decade or more of R&D efforts. And because of the wide spectrum of Homeland Security missions and our limited budgets, we had to

achieve a very high return on those R&D investments that we did make.

To achieve these three goals—high operational impact, rapid transition to use, and high return on investment—we reshaped our R&D efforts in three major ways.

First, we now focus the majority of our R&D work on late-stage development and we actively seek technologies in which others have already invested and which S&T can adapt, evolve, or apply to DHS and first responder needs. This approach speeds transition and drives down cost to S&T. Every S&T project we do must undergo what we call technology foraging, which is a culture, not a thing, but involves a review of existing technologies or research that may be a full or partial solution or contribute in some way to the project under contemplation. Technology foraging and very strong R&D collaborations with other R&D organizations in Federal agencies and universities, in the private sector and abroad, have become part of the way we do our work, and it already had an impact on our ability to deliver a high return on investment.

Now, we also realize that not all problems are amenable to technology solutions. Process changes and systems integration can also improve performance and increase efficiency. We have established a group within S&T to apply our scientific and engineering expertise to help components conduct operational analysis, integrate system engineering principles, and to provide assistance with complex acquisitions, all of which increases efficiencies in mission execution.

The second thing we did is to develop closer, much more robust partnerships with our customers in the DHS components and the first responder communities to ensure that our R&D efforts reflect, first of all, priority needs—if we develop something that works, they will buy it and use it—and, secondly, to make sure we understand the problem we are trying to solve in all of its operational complexity.

Third, we established the R&D Portfolio Review Process as the main mechanism of evaluating and selecting projects and ensuring they are aligned with our top priorities. The Portfolio Review process that we used was originally developed by industry and is now widely used in the private sector and by some Department of Defense (DOD) laboratories. It establishes our top goals—as I mentioned, operational impact, transition to use, scientific feasibility, et cetera—as metrics against which all R&D projects are weighed. Each R&D project is treated as a separate investment and evaluated by panels of outside experts, senior people from the component partners we are trying to serve, and S&T leadership.

Over 3 years, we have driven our R&D portfolio toward our top priorities. We have had three Portfolio Reviews thus far between 2010 and 2012, and the percent of projects likely to transition to use in the field within 2 to 5 years has gone from 25 to 49 percent. The percent of—

Chairman CARPER. Just repeat that again, just that whole last sentence.

Dr. O'TOOLE. The percent of R&D projects judged likely to transition to use in 2 to 5 years has gone from 25 to 49 percent. The percent of investment targeting, what is judged to be high impact, high feasibility outcomes, has gone from 38 to 45 percent. And the

percent of projects benefiting from non-S&T funds has gone from 12 percent to 55 percent. This is cash coming from either the components or industrial partners. An additional 35 percent of these projects receive in-kind support that is at least 10 percent or more of the project costs. So, 92 percent of our projects are receiving some kind of support from the customers, which I think is a vote of confidence that we are doing useful work.

One might ask why those numbers are not even higher, but R&D is inherently risky and this performance actually places us in benchmark status compared to other R&D organizations evaluated by this process.

I would like to illustrate our work with a few examples to give you a sense of the Directorate's impact on Homeland Security and the first responder community.

First of all, we have developed a commercially available multi-band radio. You will recall that one of the top priorities of the 9/11 Commission was this problem of lack of interoperability amongst first responders. The fire department, the police department, they were using different radio bands and they could not talk to each other.

S&T took technology that had been invested in and, to some extent, developed by DOD. We used our money to help industry develop a commercially viable unit that was small enough and light enough and cheap enough to be comparable to legacy systems. And then we hooked the manufacturers up with our partnerships with first responders in the field and we did field testing of the prototype units.

What resulted is the development of a robust commercial multi-band radio market and competition from multiple vendors. There are three radios on the market today and they have been bought by the Marine Corps, by the Department of the Interior (DOI), by State and local responders in multiple States, and by the U.S. Capitol Police (USCP). So this is a success.

Another example in another area is our Resilient Electric Grid (REG) Project, which is aimed at addressing a critical vulnerability that we saw highlighted in Hurricane Sandy and many other times in the past few years. That is, how do we keep the grid operating?

The grid today is separated into isolated subsections called substations to prevent rolling power failure from taking down an entire region. Especially in dense urban areas, this technological characteristic prevents power sharing during emergencies. You cannot ship power from one substation to the other. So it prolongs outages and leads to slow and costly restoration.

What we have done is partner with DOE and with industry, who co-paid on this project, to develop a superconducting power cable that allows you to connect different substations and overcomes the previous technical limitations. This permits faster and more efficient restoration of power in emergencies. This technology is now in operational demonstration by Con Edison in New York City, in Yonkers, and we are exploring a scale-up partnership with NSTAR in Boston, which they would pay 60 percent of, to lower the cable production cost and move toward wider implementation.

Moving to cybersecurity, yet another critical infrastructure that is vulnerable to breakdown and attack, S&T won a very prestigious

prize for creating the Domain Name System Security Extensions (DNSSEC) protocol. This is one of several S&T cyber projects that is aiming at reducing the vulnerabilities of the Internet itself, and what it does is it makes it much harder for criminals to hijack the message you are sending to your bank, thinking that you are going to get your own money out, and instead having it diverted to the criminals' site. More than 30 percent of all the top-level domains—dot-us, dot-uk, dot-com, et cetera—now utilize this protocol, and it has been mandated that all second generation domain names will use it, as well.

You spoke of our work with TSA, Mr. Chairman. We all know that there is a need to improve passenger comfort in the flying public. But due to increases—

Chairman CARPER. Let me interrupt just for a moment.

Dr. O'TOOLE. Sure.

Chairman CARPER. You have been speaking for almost 15 minutes, and frankly, I think it is fascinating. But I want to make sure we hear from Dr. Maurer and have a chance to have a good conversation—

Dr. O'TOOLE. I apologize. My things say 4 minutes remaining.

Chairman CARPER. Go ahead. Just wrap it up in about the next minute, summarize, and then we will—

Dr. O'TOOLE. Of course.

Chairman CARPER [continuing]. Do the rest. Thank you.

Dr. O'TOOLE. OK. I apologize. I have 4 minutes remaining here, but sure. I will wrap it up.

I could go on and on with projects, but I think you get a sense of the breadth of work that we do and the direction that we are trying to take. I hope these few examples of our work illustrate what we are trying to accomplish.

I am very honored to be Under Secretary and to work with the extraordinary colleagues in S&T, and I am happy to answer your questions.

Chairman CARPER. Are any of your colleagues here today?

Dr. O'TOOLE. Yes.

Chairman CARPER. If they are, would you raise your hand? All right. Repeat after me— [Laughter.]

We have been joined by our colleague, Senator Pryor from Arkansas. Tom, I was giving Mark a hard time. He only serves on six Committees. I serve on three. I am not sure how many Dr. Coburn serves on, but I do not know anybody who serves on six Committees, so he is a busy guy. But I have been giving him a hard time about being the prodigal—not the prodigal son, but the prodigal brother, and I am happy to welcome him back into the fold today.

Senator PRYOR. Thank you.

Chairman CARPER. Great to see you, Mark.

Senator PRYOR. Thank you.

Chairman CARPER. All right. Mr. Maurer, you are on.

TESTIMONY OF DAVID C. MAURER,¹ DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. MAURER. Great. Thank you, Mr. Chairman.

Chairman CARPER. Would you tell me again who won the All-Star Game last night?

Mr. MAURER. It was the American League, three-to-nothing.

Chairman CARPER. Thanks so much. [Laughter.]

Mr. MAURER. GAO is glad to serve the public and the Congress. I am pleased to be here this morning, Chairman Carper, Dr. Coburn, Senator Pryor, to discuss the findings from some of our recent work looking at research and development at the Department of Homeland Security.

But before I talk about our work, I think it is important to stress a couple points about why R&D is important and why it really matters, and first and foremost is the fact that R&D is really the bridge between the scientific and engineering expertise that exists within the United States and the ability to address a wide variety of homeland security threats. To put it simply, good R&D helps make the country safer. So it is important that it is managed and implemented effectively and efficiently.

The second reason why R&D matters is because the government and the country at large is facing some pretty significant fiscal constraints right now, and depending on how you add it up, DHS spends well over a billion dollars a year annually on R&D activities, and it is really important that the taxpayers are getting the most out of every single one of those dollars.

It is also important to emphasize that good R&D is difficult to do. There is always a balancing act. You want to actually have some R&D projects fail because you want to push the boundaries of science. At the same time, you want to have enough R&D activity that transitions into real world use by operators—people are using it in the field someday to help secure the country. So appropriate management will find a way to balance the need to fail as well as the need to succeed.

Within DHS, the Science and Technology Directorate has the lead responsibility for overseeing and coordinating R&D activities across all of DHS as well as playing a leading role in coordinating with its other Federal partners on homeland security R&D. I think it is also important to underscore the fact that from GAO's perspective, we have seen that S&T has made really important progress over the last few years, and some of the points that Under Secretary O'Toole has pointed out, I think, are important to underscore, as well.

I think the reorganization that S&T undertook a few years ago was helpful. The fact that S&T now has a strategic plan that it is operating from. The Portfolio Review is helping provide a more strategic perspective on R&D investments within the Department. But I think, most critically, the fact that S&T is focused on working more closely with the various components within DHS is helping produce better R&D outcomes and also pursuing the broader

¹The prepared statement of Mr. Maurer appears in the Appendix on page 326.

goal of developing a “One DHS” vision for the Department. That is all very good.

At the same time, I am also from GAO, so clearly, we want to talk about some of the challenges and the work remaining, because, clearly, there are some significant challenges on the R&D front.

In our recently issued report, we focused on three issues. The first was, how is R&D actually defined at the Department? The second is, how much resources are devoted to R&D activities within DHS? And the third is, how is the Department overseeing and coordinating R&D?

On the first issue, we found that DHS currently does not have a standard definition for R&D across all of the Department and that is a significant problem. We looked at other large agencies or departments that handle R&D work and they do have R&D definitions that are tailored to their specific missions. So, for example, National Aeronautics and Space Administration (NASA), DOD, and other organizations that spend a great deal more on R&D have developed a common definition. And that is important because having a common definition for such a large organization as DHS will help enable gaining better strategic visibility over R&D activities and also, frankly, allow the components to understand what some other activities—whether some fall into the R&D realm and whether some fall under the acquisition realm.

Now, we will be the first to recognize that coming up with this definition at DHS is not going to be an easy thing to do. There is a wide array of missions and there is this whole spectrum of R&D and acquisition and there is a broad gray area. But we think it is important to do going forward.

This lack of definition partially explains our second finding, which is, it is really unclear at this point how much DHS actually spends on R&D activities. When you look at the budget information that DHS provides annually through the budget process, you will see line items for the Science and Technology Directorate, the Domestic Nuclear Detection Office (DNDO), and the Coast Guard, and there is money there for R&D activities.

In our work, we found that there were also R&D activities being implemented across a variety of other components. And, in fact, in fiscal year 2011, we identified an additional \$255 million in R&D activity that was not captured in the sort of standard R&D roll-up provided to the Congress. We feel that is a concern because it is hard to be strategic, it is hard to have a good perspective over what you are spending your money on if you do not have good visibility of who is doing what. So we think that is an issue that needs to be addressed.

This lack of visibility also underscores our third finding, that DHS needs to improve the overall coordination and oversight of R&D activities, and that is at the Department level, not necessarily just at S&T. We found specific to S&T that it has improved its coordination with components. There have been a variety of mechanisms, a variety of forums that S&T has implemented in partnership with various operational components with DHS. This helped improve coordination. But it is a big task and we found that R&D is inherently fragmented across DHS. It is going on in a number

of different components. Some of it is being conducted under the aegis of acquisition programs. It does not have good visibility. We think it is important to gain that visibility.

So as part of our work, we looked at the potential for overlap and duplication among R&D projects within the Department. Our concern was that if there was not visibility over all the different activities and all the money, there could be unintentional duplication of effort.

We found 35 instances involving \$66 million of different R&D projects where there was overlap, and what that means is that different parts of the Department were working on similar aspects of R&D without necessarily being informed of one another's ongoing efforts. That is overlap. Now, when—

Chairman CARPER. A quick question.

Mr. MAURER. Yes.

Chairman CARPER. Was GAO just looking within the Department for overlap and duplication, or did you look outside the Department for overlap and duplication?

Mr. MAURER. For this review, we looked just within the Department of Homeland Security. We reviewed thousands of different contracts. Now, we dug in very deeply into those contracts to see if there was actual duplication. Duplication is when two different parts of DHS were working on exactly the same thing. We did not find any examples of duplication, but we found overlap.

So, for example, we found cases where two different components were working on five separate contracts to review similar aspects of explosive detection technology. That is not necessarily bad if it is done by design. I will be the first to say, I want as many scientists as possible looking at explosive detection technology and looking at biothreats and other things. The problem occurs when it is not done strategically and when it is not done intentionally, and when that happens, it raises a potential risk of unnecessary duplication, and that is a problem because you can end up essentially wasting money.

The reason why this has happened is because DHS lacks policies to have this effective oversight, to have this effective coordination across the entire Department, and we think that, going forward, there are a few things that S&T and, more broadly, the Department needs to address.

We think, first and foremost, there needs to be a common definition of R&D that enables S&T and the other operational components to understand what is research and development and what is not.

Second, there needs to be at the Department level defined processes and roles to enhance coordination, building on some of the successes that S&T has been able to engender in its own efforts to coordinate. We think it should be moved up to a higher level, to the Department level.

Finally, there needs to be improved tracking of the individual R&D projects, in other words, improved information on who is doing what and at what cost. And again, there needs to be this strategic visibility.

Right now in DHS's Acquisition Directive, there is a placeholder for research and development and it literally says, "to be deter-

mined.” We think it is important for that “to be determined” to be translated into actual policies and procedures.

The good news on that front is when we issued our report last fall, the Department in its official comments agreed with our recommendations, agreed with our findings, and they have started to take action to address those. So that is encouraging, but it is still very much a work in progress and we are looking forward to having the Department complete its efforts, implement our recommendations, and, therefore, better position themselves to deliver even improved and more enhanced results on the R&D front. We think that is important, not just for the sake of DHS or the GAO, but it is important for the country to get better national security and homeland security outcomes from the R&D investments.

That concludes my remarks today. I look forward to your questions.

Chairman CARPER. Great. Thanks so much.

The person who actually suggested to me initially that we do these series of hearings on Department of Homeland Security oversight was Dr. Coburn, with the eye toward eventually moving toward reauthorization of the Department. We have never done that in its 10 years of existence, so this is, as I said earlier, a part of a series of hearings. I am going to yield to him for questions and then to Senator Pryor and then I will follow Senator Pryor.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Welcome. I would tell you, I have sat at hundreds of these hearings and that is the best performance analysis by the GAO of any Department I have ever heard. Most of the criticisms you just heard were not of S&T. They were overbranching Homeland Security and the R&D outside of S&T. That is what we really just heard. So I want to compliment Dr. O’Toole. I think she has done a great job so far.

I am concerned. One of the areas that, Dr. O’Toole, I want to ask you about, one of the things that you have been good at has been acquisition support, and I see in the President’s budget cutting that almost a quarter. I know that is a decision that may have been made above your level, but to me—and Mr. Maurer, if you would comment on that, as well—I see that putting some of the progress we have made at risk if, in fact, we allow that to go through. Would you care to comment on that?

Dr. O’TOOLE. Sure. We have two budget lines in S&T. One is our management budget line and the other is what is called the Research, Development, Acquisition, and Operations (RDA&O). This is part of GAO’s problem. So the acquisition support that you are talking about, where we take our systems engineers and our operational analysts and our scientists and we try and help the components structure requirements at the very beginning of an acquisition that are going to get us what we need, on time, under budget, and so making sure we understand the entire life cycle cost, is not getting cut. It is this RDA&O budget number that is misleading in what it talks about.

So, the kind of assistance that you are talking about and for which we set up a separate group is still intact and, in fact, growing. The demands exceed our grasp. We have 11 people in that sec-

tion and we have to pick and choose what we are going to work on. But——

Senator COBURN. But that component——

Dr. O'TOOLE [continuing]. That is ongoing.

Senator COBURN [continuing]. Is not being cut.

Dr. O'TOOLE. Correct.

Senator COBURN. OK. Thank you.

Let us talk about electromagnetic pulse, both natural and intended——

Dr. O'TOOLE. OK.

Senator COBURN [continuing]. And the new transformers that are available. Where is the work there and what are we seeing happening right now?

Dr. O'TOOLE. S&T is not doing any work on Electromagnetic Pulse (EMP). We are very aware of the threats to the grid from, as you say, all kinds of potential deliberate attacks, as well as natural events. The grid is the primary responsibility of the Department of Energy and they are doing work on this in collaboration, I believe, with DOD. But we do not have any R&D directed work on that.

We have a very strong collaboration with DOE on the project that I talked about and several others, so we are generally aware of their work, but we would dive in much more deeply if we were actually investing in that area.

Senator COBURN. And you do utilize the services of some of the labs——

Dr. O'TOOLE. Yes.

Senator COBURN [continuing]. In your research. You coordinate with that.

Dr. O'TOOLE. Yes.

Senator COBURN. Do you look at a review of everything they are looking at to see what they may be doing that might help you? In other words, rather than specifically, we need help here, do you ever do an inventory of what they are doing to see how that might prove as an augmentation to what you are doing?

Dr. O'TOOLE. So, we have talked about this a lot. It is very difficult to do inventories of DOD or DOE National Labs work because they are large inventories and constantly shifting. That is what happens.

Senator COBURN. Yes.

Dr. O'TOOLE. R&D is a constantly dynamic beast.

What we have done is asked the labs to give us their inventories of what they are investing in and for them to tell us who we should be working with on one project versus another. And we have made progress in that regard with the labs.

So, for example, Pacific Northwest Lab is very adept at process control systems in cybersecurity. Other labs are much more focused on big data issues. And we have learned through professional association who does what and how well. But the answer to your question is no.

Senator COBURN. OK.

Dr. O'TOOLE. We do it project by project.

Senator COBURN. So your Directorate basically manages a billion dollars a year in——

Dr. O'TOOLE. In a good year.

Senator COBURN. In a good year. Hopefully, we can have some more of those. But there is about a quarter of a billion in R&D, guesstimate, outside of S&T, is that your understanding?

Dr. O'TOOLE. That is certainly the GAO finding. First of all, half of our budget is R&D and the rest is the university programs, et cetera, et cetera. The dilemma in DHS is that because we are so operationally focused, there is, as David said, this large gray area which the components do not now regard as R&D. If you think about the spectrum of R&D, it starts with trying to understand fundamental phenomena and then you gradually apply it. You make a technology. You prototype it. Once you get it out into the field and it is working and you are using it, you are still tweaking it in virtually all cases. Think of any technology you own.

And what the components are doing is what they call tweaking—they do not call it tweaking. David calls it research. They call it operational performance improvements. So in these overlapping experiments or R&D efforts that he talked about between TSA and DHS, I mean, S&T, what we were trying to do was test brand new technologies, in this case, mass spectrometry, to see if it could actually detect these homemade explosives.

What TSA was trying to do, sort of to make a leap forward in the way we deal with Hazardous Materials Endorsements (HMEs), what TSA was trying to do is improve the efficiency in the way they operate the scanning machines and the trace explosive detection that is already deployed in the field. So they do not regard that as R&D. They think that is operational. And figuring out a definition that accommodates both parties, that truly captures R&D without inhibiting the agility of the components to make operational improvements, is the dilemma.

Senator COBURN. Dr. O'Toole, in your estimate, what percentage of this money that is operational improvement—is there other R&D going on in Homeland Security that is outside of your control?

Dr. O'TOOLE. Yes. I mean, the components are sending money to the DOE labs and the DOE labs definitely do R&D.

Senator COBURN. Right.

Dr. O'TOOLE. I cannot answer the percentage. I do not know. I do not have any analytical basis for saying. What we would like to do is form strong partnerships with all the components as we are doing. I think a Portfolio Review, for example, is a much more powerful mechanism for identifying research and development than are budget lines—

Senator COBURN. Right.

Dr. O'TOOLE [continuing]. That say, this is R&D. And we have persuaded the Coast Guard, for example, to use this Portfolio Review. They really liked it. Actually, they improved it. We are going to adopt their innovations. And the Immigration and Customs Enforcement (ICE) is now looking at it, as well. It takes a lot of work to do a Portfolio Review. It is a big investment. But that would be something that we are trying to encourage the components to adopt, and that will, I think, pick up and identify that work which we would all agree is R&D and should be captured.

Senator COBURN. Do you think the leadership at DHS buys into that, in other words, this Portfolio Review, so that we are actually

using some of the techniques that you have put in at S&T—where you have not had a partnership component unit working with you? In other words, do you see that transitioning to the point where we are going to have buy-in throughout all the components of DHS?

Dr. O'TOOLE. The Secretary is very much in favor of it and has said so. I think we will get there. Some components are much more willing than others. There is a spirit of, let us collaborate anywhere we can to save money and gain efficiencies abroad in the Department that I think is quite powerful.

Senator COBURN. All right. Thank you.

Chairman CARPER. Senator PRYOR.

Senator PRYOR. Thank you, Mr. Chairman. And you are correct. We were together over the weekend and someone was remarking that I am on six Committees, and I could see your jaw drop and you said, "Six Committees? No wonder you never come to Homeland Security." [Laughter.]

So, anyway, I am back. Thank you. It is great to be here, and I probably am on too much and doing too much, but thank you so much.

Let me say thank you both for your leadership on this issue. This is important. You are doing good work. It is nuts and bolts. It is probably not going to grab a whole lot of headlines, but it is important for the government to do this and important for us to have that oversight.

Secretary O'Toole, let me start with you. Last September, GAO recommended that DHS develop policies and guidance for defining, reporting, and coordinating R&D activities across the Department. I am curious just generally about the status of that. I know you talked some about that, but I would like just a brief status report on that and what you need to do to continue to implement those recommendations.

Dr. O'TOOLE. So, we have accepted all the recommendations. We have researched the different definitions of R&D around the government and have offered a suggestion of one that we think will work for DHS without impeding agile improvements by the components.

The Under Secretary of Management is preparing a second evolution of our fundamental Management Directive which would set up an integrated approach to how we do all work across DHS and would establish a lot more transparency and visibility into what everybody is doing in a manner that would be available to all of the components, including S&T. It would also give S&T a prominent role at the front end of any acquisition, which would be very important. Now, we come in just before we buy something and we do operational testing and evaluation (OT&E). We could save everyone a lot of grief and money if we had more expertise engaged at the front end.

Third, S&T has established a process whereby we are going to collect information on what the different components are working on with the DOE labs.

Senator PRYOR. So, in terms of the GAO recommendations, are you halfway through? Are you three-quarters of the way through? Have you implemented all of them? I mean, tell me where you are in trying to—

Dr. O'TOOLE. We are more than halfway. We are about done with the definition. The problem is that the definition will still come up against these different kinds of budget lines that will have to be worked through different Committees and may not be that illuminating in the end.

The Integrated Investment Life Cycle Model (IILCM) is hopefully going to be established in the next several months and we will have an annual S&T delineation of DOE work this year.

Senator PRYOR. And is that the kind of thing where you get the GAO report and then you just go to work implementing it, or is there contact with GAO about how they think you should do it and for them to sort of help you make good decisions there? Do you have any contact with GAO on this?

Dr. O'TOOLE. Well, we have certainly talked with Mr. Maurer and his team extensively about the report before and after they issued it. It is pretty straightforward. The dilemma is how you apply this definition across budget lines that we do not control.

Senator PRYOR. OK. Mr. Maurer, do you have a comment?

Mr. MAURER. Yes, absolutely. We typically, after we issue a report, we let the report and the recommendations stand on their own, but we often work with the departments and agencies we make recommendations to and basically assess their actions and we make an independent judgment of whether or not we think those actions are sufficient to close a recommendation.

I think, as of right now, we are encouraged by the progress that the DHS is making and we certainly leave it to them to work out all the details, because that is appropriate. But at the same time, we view those recommendations as open and not fully implemented at this point.

Senator PRYOR. But you feel like they are making progress?

Mr. MAURER. Absolutely.

Senator PRYOR. And do you feel like that you can measure that progress and, at some point in the future, say, hopefully this year, you will be able to say they have been able to do all this, or will there be ongoing problems?

Mr. MAURER. Well, I think that depends on what is actually implemented at the Department. Typically, what we want to see is not just a creation of a plan. We also want to see that plan implemented and put into practice. That has been one of the major challenges facing the Department, not just on the R&D front, but there have been a number of plans and directives to improve overall management of the Department, which, when you read the words on paper, are very encouraging and very positive, but you want to see those changes actually implemented and involve changes in the day-to-day operation of the Department and, hopefully, leading to cultural, organizational change within DHS.

Senator PRYOR. Secretary O'Toole, let me change gears, if I may, and ask you about the sequester and the management challenges that presents. So, I guess, just if you have some specific examples of ways that the sequester is making things difficult for you at DHS and maybe DHS Department-wide and how you would like to see all that resolved.

Dr. O'TOOLE. R&D is particularly disrupted by budgets that go up and down, because when you invest in an R&D project, it does

not bear fruit for several years. So not only does sequester threaten to cut funds for projects that are not yet completed, so you lose all your sunk costs, it makes it very difficult for us to decide what projects to begin. We have not begun any new projects for a while now because of budget uncertainties. What you really want is steady funding in R&D. Money that goes up and down is very difficult to deal with.

So, for example, in our Portfolio Review, one of the things that it produces is a picture of all the potential investments across all of these different areas and the scores associated with those investments. And you have to decide, what are you going to invest in, given your piggybank? With the sequester, we are holding off on some very good projects that we would like to begin, or having to choose between two projects and we can only do one.

Over time, this kind of uncertainty wears away at the morale and the quality of staff, frankly. If you ask any R&D director what their biggest problem is, it is recruiting and retaining talent. In R&D, when your budget goes down, you do not just pedal harder and work longer hours. Your project goes away. Your work goes away.

So if we have too long a period of this kind of uncertainty, I think it will impair our ability to recruit and retain staff. That is No. 1. Two, it makes it very difficult to make really wise investments in new projects. And, three, it ultimately leads us to end projects that might have borne fruit before they ripen.

Senator PRYOR. Thank you, Mr. Chairman.

Chairman CARPER. Boy, you ask really good questions. You have had a chance to practice and prepare, so it was good.

One of the things I loved to do when I was Governor—I still love to do it—is I love to do customer calls, and my guess is Dr. Coburn and Senator Pryor also do this back home, where we visit companies all over my State and we ask—our delegation does this, we do it with our Governor, Jack Markell—and we ask businesses, how are you doing? How are we doing and what can we do, we in government, our delegation, and when I was in Governor, in that role, what can we do to help you? We think that is part of creating a nurturing environment for job creation and job preservation, to ask our customers, in that case businesses large and small, how we can be helpful.

One of the things that I oftentimes ask—I usually ask it at the end of the hearing—what can we do to help you do your jobs better? I think you provided part of that answer already in what you just said. And one of the things Dr. Coburn and, frankly, Senator Pryor and I work on a lot is trying to develop bipartisan support for a comprehensive deficit reduction plan that includes entitlement reform, includes some revenues, and includes just a real focus on changing the culture of government, from spendthrifts and more to one of thrift where actually we look at everything we do and ask, how do we get a better result for less money?

But I am reminded—Tom and I were talking about this the other day in terms of weapons systems procurement—if the funding goes up and down, up and down, and we have a fixed contract, a fixed-price contract with, whether it is Lockheed or anybody else, it is pretty hard to—when they are talking about modernizing C-5 air-

craft or any other weapons system project—it is pretty hard to get what we need at a good price.

And the point that you make about the need for some certainty, some predictability with respect to funding is very well taken. I take that to heart.

Let me just ask you, in terms of asking our customer, doing customer calls, talk to us about who your customers are. Talk to us about how you communicate with your customers.

One of the trips I took earlier this year was up along the Canadian border. I was joined by Senator Levin of Michigan, to take a look at border security on the Northern border. And one of the memorable conversations I had up there, we spent some time in helicopters. We spent a lot of time on land with the Border Patrol folks, the Customs and Border Protection (CBP) people. But we also spent time with the maritime folks in small swift boats, fast boats, along the Great Lakes.

And we were talking to the fellow who was in charge of one of the units up there that included a bunch of the boats, maritime folks. He said he is very much interested in R&D. Interesting. He has had some jobs within the Department, pieces of the Department, that actually gave him the opportunity to be involved in R&D. But what I heard from him is he was not really convinced that the, say, the Directorate, the folks at the top of the Directorate, were as interested as they might be, ought to be, in terms of asking folks on the front line, what do you need?

In one of my old jobs, I was a Naval Flight Officer for many years in Navy P-3 aircraft and our job was to hunt for Red October, track Russian subs in all the oceans of the world—Soviet subs, actually—stuff like that. We would from time to time be asked by the Navy and also by Lockheed, who was the developer of our planes, builder of our planes, what do you need? What is working? What is not working?

I was on the Amtrak Board of Governors as Governor and we were always asking our customers, what do you need, because what we thought they were looking for and needing maybe was not what they did.

But who are your customers? How do you find out what they need?

Dr. O'TOOLE. So, our customers are the DHS components in all their variety and multitudes, hundreds of thousands of people, and the first responder community spread out over 73,000 jurisdictions and also a heterogeneous set of communities.

I have been up to the Northern border and the Great Lakes and talked to those people. We are working hard up there. It is hard to touch every person, but our outreach to the components is quite extensive. We have people deployed to Customs and Border Protection from S&T. We do not do a project without extensive engagement with the operators, whomever they may be, but the front line people.

In the particular situation that you are talking about, for example, they are using on the Great Lakes and across the Northern border a system of sensing integration that we developed in Los Angeles-Longbeach for the Coast Guard, and the CBP saw it, liked it, and moved it up to the Northern border.

At Ambassador Bridge in Detroit, where a lot of the Northern border truck and car traffic comes over, we just finished an Apex project that was trying out these smart locks which help to make CBP much more efficient, also help to make the vendors, particularly the car manufacturers, much more efficient, and improve their throughput and security.

So we are very opportunistic in the projects that we take on. We cannot do everything. So if somebody comes to us—if a component comes to us and says, we have a problem, we will respond to that. We will not now invest unless the head of that component or his or her No. 2 says, this is a big problem for us. We want S&T to invest here and we will agree in writing on the objective and the approach to that project. And we do this every year. We check to make sure that we are doing the right thing.

We have learned that the projects that succeed are those in which we have a partnering team that includes the operators, but also the people with the authority to commit money on the other side following that project throughout its gestation period. We do not say, OK, we are going to do this for you and walk away for 2 years and come back with a gizmo anymore. We will not do that.

And if, after 2 years of S&T investment, the component is not willing to invest their own money in furthering their project, or at least establishing an acquisition line so that they can pick it up in another year or two if it succeeds, we stop. So we stopped the Secure Transit Corridor that we were working at the Ambassador Bridge because CBP told us, we would rather you spend your resources on air entry and exit.

Chairman CARPER. That was a reassuring answer. I would like to say, as Dr. Coburn and our staff says I often say, everything I do, I know I can do better. And I would just urge the folks that work for you just to make sure that on a daily basis, on an ongoing basis, that they bring to work the spirit of asking, what do you need? How can we help? Just make sure that they are continuing to improve that communication and asking that question and responding to the answers.

I am going to slip out and take a quick phone call, and when we come back, I want to go from the Northern border to the Southern border. I spent a fair amount of time, as did Dr. Coburn, along our border with Mexico. As you know, we spent a lot of time in the Senate in the last month on legislation trying to figure out, among other things, how to make our borders more secure in a cost-effective way.

I want to come back and talk about force multipliers and the ports of entry. We have this huge throughput of traffic you have alluded to. Also, how do we use force multipliers to get better results for less money or the same amount of money with all these Border Patrol people we have, and there is a proposal to add a whole lot more to them. And we ought to figure out, what are we doing that makes a lot of sense, but what, in terms of what you are hearing from your customers down on the Southern border, that we can do, things like Enforcement Link to Mobile Operations (ELMO) that we hear about that you have probably been involved in, the handheld device for the CBP people. I just want to delve

into that and look forward to pursuing that and have some questions, too, for you, Mr. Maurer. Thanks very much. Dr. Coburn.

Senator COBURN. Well, thanks. As Senator Carper said——

Chairman CARPER. You can just hold off for now and we will come back. I was telegraphing my pitch.

Senator COBURN. No. Well, she had said something before that, but that is OK.

Chairman CARPER. All right. Thanks.

Senator COBURN.[Presiding.] Tell me the benefits in the way that you work with DARPA.

Dr. O'TOOLE. We have become very avid transition partners for DARPA. They work, as you know, on the leading edge of technology and we have on numerous occasions—I will give you some examples—worked with them to pick up their technology and apply it to DHS needs.

We just held a Joint Industry Day with DARPA and TSA that is oriented around these new approaches to aviation safety. We are using DARPA's \$25 million investment in compressive sensing, which is a way, mathematically, of getting more information out of a signal as part of this new checkpoint that I described.

We have used a big DARPA investment in a classified system for gathering and making sense of data that we are going to declassify and use to try and maintain a better situational awareness of the marine environment, which, as you know, is plagued by these submersible, semi-submersibles, and small boats that we have a hard time seeing and tracking.

We have benefited from DARPA's investment in a composite material-based box—they call them Hard Unit Load Device (HULDs), H-U-L-D—which is intended to house cargo being shipped in airplanes and to contain an explosion if some cargo in that box explodes. They developed a prototype. We have tested it, tweaked it a little bit. It is probably too heavy and expensive for what we need, but it has been a very good experience.

We have used DARPA's algorithms for identifying explosives in our applications, and I could go on and on. But we have formed very close liaisons with them almost across the board of disciplines.

Senator COBURN. And you feel comfortable you are not duplicating but you are, rather, extending their research——

Dr. O'TOOLE. Yes.

Senator COBURN [continuing]. In terms of——

Dr. O'TOOLE. Very comfortable.

Senator COBURN. All right.

Dr. O'TOOLE. We do not do what DARPA does.

Senator COBURN. Yes. You have these Centers of Excellence at the university level, which I assume you think you are getting good value from. Do you think you are always getting good value? Do you have good control over the expenditure of that money?

Dr. O'TOOLE. We are getting more and more value out of the Centers of Excellence. There are initial stand-up transactional costs. It takes about a year, from what we can tell thus far, for a new COE to really get rolling. And the more they engage with DHS, the more successful they are. So last year, for instance, the Centers for Excellence combined got more money from the DHS

components than they did from their S&T grants, which is a sign of confidence.

But, yes, I think they are a very good value, and as I said, as they mature, they become more so out of time.

We are also making a lot of efforts to get our own program managers from the Homeland Security Advanced Research Projects Agency (HSARPA) more familiar with and engaged in what the universities are doing so we can go out when we do technology foraging—that is actually the first thing that we do. Is there anything our COEs have that we could use?

Senator COBURN. OK. I will submit questions for the record, and I do not know whether this came from S&T funding or from the component funding, but there are a couple of studies that were released from the COEs that I cannot find a connection to Homeland Security from, and one is from the University of Hawaii and another from the University of Arizona, that I do not see how it has any application to what you are doing, but I will not go into that now.

Dr. O'TOOLE. OK.

Senator COBURN. But I will send you a letter on it and have you look at it.

Dr. O'TOOLE. OK.

Senator COBURN. One of my criticisms in grants is, too often, especially at Homeland Security, we do not have the followup.

Dr. O'TOOLE. Mm-hmm.

Senator COBURN. Here is what the grant was supposedly for.

Dr. O'TOOLE. Mm-hmm.

Senator COBURN. Did they actually spend the money on the grant?

Dr. O'TOOLE. Mm-hmm.

Senator COBURN. Did the grant give us something of value? Could we have done a better job in detailing down and honing down on what the grant was for? Do those people receiving grants know you are going to be checking on them—

Dr. O'TOOLE. Yes.

Senator COBURN [continuing]. For compliance? In other words, creating an expectation as, we are going to give you a grant. It has to be serious. It is not about fulfilling some professor's need for some extra money for his research. Rather, here is a need the government has and we are going to check on you. And, by the way, if you are not doing it, we are going to pull the money.

Because where we do that in the government, and it is not many places, we get much more value for what we send out because you change the culture. The culture becomes an expectation, if you get a Homeland Security S&T grant, you had better by dinghy be on the ball after it and you had better perform. Otherwise, you are not going to get the grant, and you might get that one pulled back.

Dr. O'TOOLE. I agree. We do not pull back money, but we give more money if you are performing. We review each COE twice a year with a Federal Steering Committee. And these are very desirable grants. If you have not performed, you are certainly not going to get the second round of grants. But there is definite incentive to performing well and that is measured by how you help DHS.

Senator COBURN. OK. Mr. Maurer, during your review, I presume you spoke with several of the components of DHS and their evaluation. What is their perception of S&T?

Mr. MAURER. That is right, Dr. Coburn. We spoke with a number of different operational components at DHS and our report, obviously, was issued back in September, so all of this audit work was done about a year and a half ago or so. At that time, we spoke with representatives from six different components.

We heard, frankly, a range of views. Some components were very complimentary of how closely they were working with S&T and they really applauded S&T's efforts to have a tighter link between operational needs and the R&D support and the other support that S&T can provide.

There were other components, or representatives from other components, that were, frankly, unclear of the linkages and they were not sure that what S&T was providing was in direct alignment with their overall operational needs and they felt that there was a need for enhanced coordination and collaboration.

Senator COBURN. Was that communication at the leadership level of those components or was it at sub-levels of that component?

Mr. MAURER. We were talking to people at the sub-levels, at the working level.

Senator COBURN. Yes, because I think the important point Dr. O'Toole made is we will work with you if you buy in. But if you are not going to buy in, we are not going to be there. And so I wonder, can you ferret out any of that for me in terms of the agencies where they were actually doing work and yet you still had a negative comment?

Mr. MAURER. Generally speaking, the components where there was a more positive feedback from S&T had the tighter links at that senior level and it had trickled down through the organization. Some of the areas where there were some concerns, it may have been a combination of sort of legacy and longer-term things, where the change had not percolated down into the trenches yet.

Senator COBURN. Yes.

Mr. MAURER. And I think that is actually not atypical within DHS, to be quite honest. I mean, there are good things happening within the Department, but you are really talking about changing the direction of an aircraft carrier. It takes a while for it to get all the way down.

Senator COBURN. All right. Thank you very much.

Mr. Chairman, let me have one other—

Chairman CARPER. [Presiding.] No, please, go ahead.

Senator COBURN. One other question, if I might.

Chairman CARPER. Sure.

Senator COBURN. The National Bio- and Agro-Defense Facility (NBAF) in Kansas, you got that under control?

Dr. O'TOOLE. Yes.

Senator COBURN. Going to come in on time, under budget?

Dr. O'TOOLE. Under budget—

Senator COBURN. On budget? How about on budget?

Dr. O'TOOLE. On budget, yes. I think we can do that. This has been a very extensively studied construction project. It is a unique facility, very highly engineered. But the country needs this labora-

tory to protect its agriculture industry, and I think we have great partners in Kansas. They really want to build this for their own reasons, which I think are sound. So everybody's interests are aligned.

Senator COBURN. OK. It is a big project, as you know.

Dr. O'TOOLE. Huge, yes.

Senator COBURN. It is bigger than your whole budget.

Dr. O'TOOLE. Yes.

Senator COBURN. So I would love updates on that as you get through. If you get in trouble, I would like to know earlier rather than later.

Dr. O'TOOLE. I agree. I will say, we did bring the National Bio-defense Analysis and Countermeasures Center (NBACC), which is the human BioSafety Level-IV (BSL-IV) lab, in on budget.

Senator COBURN. OK. Thank you.

Chairman CARPER. All right. Thanks, Dr. Coburn.

We have been joined by Senator McCaskill. There is nobody more vigilant than the two people sitting to my right in terms of trying to make sure there is a culture around here that focuses on better results for less money, and Senator McCaskill chairs a Subcommittee that focuses a lot on this and we are happy that she is here. It is all yours.

Senator MCCASKILL. Thank you, Senator Carper.

I believe that you have spent \$334 million to produce an antibiotic, Raxi, dosage in preparation for and anticipation of an antibiotic-resistant anthrax, is that correct?

Dr. O'TOOLE. No, Senator.

Senator MCCASKILL. OK. How much has been spent?

Dr. O'TOOLE. We have not spent any money on production of antibiotics. That would be the Health and Human Services (HHS) responsibility.

Senator MCCASKILL. OK. But the Federal Government has spent this money.

Dr. O'TOOLE. That is possible.

Senator MCCASKILL. You do not know?

Dr. O'TOOLE. No.

Senator MCCASKILL. You have no idea how much has been spent for vaccinations for an anthrax attack?

Dr. O'TOOLE. That is not my realm of responsibility, Senator.

Senator MCCASKILL. OK. So you do not know about Raxi?

Dr. O'TOOLE. I know of the drug—

Senator MCCASKILL. OK.

Dr. O'TOOLE [continuing]. But I do not have any direct oversight or engagement or responsibility with that issue.

Senator MCCASKILL. Well, is it not your job to determine overall homeland security as it relates to science and technology? Is that not your job?

Dr. O'TOOLE. My job is to manage the R&D investments on behalf of DHS. The realm of R&D that we do is set forth in the Statutory Act. We have very specific responsibilities in biodefense—

Senator MCCASKILL. So if you do not have testing capability in terms of health, then you would not be in charge of having, instead of GenWatch, instead of having BioWatch, having blood testing

done on individual responders to determine whether or not there has been some kind of terrorist bioattack?

Dr. O'TOOLE. No. We do not do that work. The bio——

Senator McCASKILL. That would be HHS responsibility?

Dr. O'TOOLE. Testing first responders——

Senator McCASKILL. Yes.

Dr. O'TOOLE [continuing]. For exposure? Yes. That would be the——developing those tests, developing a diagnostic test is something that we are very interested in, but we would not——

Senator McCASKILL. But have you not advocated for that?

Dr. O'TOOLE. I have advocated for a strategy that emphasizes the development of clinical diagnostics, because I think in a big bio-attack or a pandemic, particularly if resources such as treatments are scarce, it will be very important to be able to specifically define who is infected and who is not.

Senator McCASKILL. OK. I am a little confused, then. So you are involved in the strategy of clinical diagnostics when it comes to testing first responders in terms of blood tests that would give us some indication as to whether or not there had been an attack, but you have nothing to do with Raxi, any strategy or any opinion about whether Raxi has been a good investment for the Federal Government.

Dr. O'TOOLE. The medical countermeasure investments, which are defined as vaccines and antivirals and antibiotics, are under the purview of HHS and DOD for its own troops. DHS does not engage in research and development related to medical countermeasures. We have had a historical mission involved in trying to detect bioattacks and attain situational awareness over an attack once it occurs, which is the realm in which I think diagnostics would be important.

Senator McCASKILL. Well, let me just ask for your opinion then, even though it is not your——maybe you are going to say you do not have an opinion, which I would find shocking. Do you think it is a good idea that we have spent \$5,100 per dose and spent over \$334 million for an antidote when there has never even been a test that has proven that antidote will work, and that all of these doses will expire and be worthless to us in 2015, and the person who had been recommending this everywhere he went in a professional capacity was on the board of directors of the only company that developed the drug and made more than a million dollars from that company during the period of time he was recommending this strategy, not only to HHS, but also to your predecessors and I believe you have had meetings with Mr. Danzig.

Dr. O'TOOLE. I have known Mr. Danzig for over 20 years. I think he is a dedicated public servant. He works as a member of a panel for a contractor of ours on what is called the BioNet Assessment, which is an Homeland Security Presidential Directive (HSPD)–10 mandated panel that is supposed to look at our progress in bio-defense periodically and report back. I have never heard him in any meeting on biodefense—and I have been in a lot, particularly prior to my job here, which has kind of moved me out of that realm, frankly—I have never heard him advocate that drug.

But let me answer your first question.

Senator McCASKILL. Well, Secretary O'Toole, it is in writing. I would recommend you Google him. There is article after article about the importance of doing this. You are not going to sit there and tell me that Mr. Danzig has not advocated buying this vaccination, this treatment.

Dr. O'TOOLE. What I said was I have never heard him advocate it.

Senator McCASKILL. OK.

Dr. O'TOOLE. In terms of—

Senator McCASKILL. But you know he has been advocating it—

Dr. O'TOOLE. I believe you—

Senator McCASKILL [continuing]. Far and wide for years.

Dr. O'TOOLE. I believe you.

Senator McCASKILL. OK.

Dr. O'TOOLE. OK. In terms of—

Senator McCASKILL. But you do not need to believe me. You know it, do you not?

Dr. O'TOOLE. Pardon me?

Senator McCASKILL. You know this, do you not?

Dr. O'TOOLE. No, not from personal experience or information, I do not.

Senator McCASKILL. So you have not read about this?

Dr. O'TOOLE. No, I have not.

Senator McCASKILL. You are telling me that in your capacity of responsibility and leadership at the Department of Homeland Security, you have no idea that there has been a serious allegation of conflict of interest—

Dr. O'TOOLE. Oh, no. I am well aware of the serious allegation of conflict of interest, but I do not believe everything I read, and I do know Richard and I had personal experiences with him.

Let me go back to your first question, though, which is a very serious strategic point about what are we doing to protect the country against biodefense, OK. This is a very complicated area technically, OK, and in my view, which you have asked for so I will offer it—I am a little out of my area of responsibility here—it has not gotten sufficient congressional attention and oversight. It is very difficult to figure out, particularly in medical realms, when you are talking about drugs and vaccines, where there is a very long, complicated runway between the idea and the success, it is very difficult to figure out what to invest in.

The added complication for biological weapons-related diseases is that we cannot ethically test a lot of this stuff in humans, which is the dilemma that you raise, Senator, regarding this pharmaceutical. So we need to have a very careful strategy of investment.

This is big money that we are talking about, as you point out. That is not a lot of money per dose for your average biological, but it is a lot of money, particularly since we have to deal with many different potential agents and we are trying to protect the country, not just one, two, or a thousand patients. So there are very difficult decisions to be made, almost Hobbesian choices in some cases, about which medical countermeasure to invest in and what are the principles upon which we will be investing.

And in my opinion, I think that deserves more attention from Congress than it has gotten. I think we are investing a lot of

money. I think we are under-investing and I would like to see us take a more strategic approach. We have to buy down this cost with new technologies. It is a very difficult set of markets to move, very complicated. But I do think it would be a good thing to spend more of the Congress's attention on biodefense.

Senator MCCASKILL. I am reading your responsibilities and it says, finally, some of the Under Secretary's responsibilities and authorities are primarily coordinative. These include collaborating with the Secretary of Agriculture, the Attorney General, and the Secretary of Health and Human Services in designating and regulating biological select agents.

Dr. O'TOOLE. Mm-hmm.

Senator MCCASKILL. And that is why I am a little surprised at your initial reaction that this is not anything that you have anything to do with and your assertions that you are not really aware of any of the—

Dr. O'TOOLE. Well—

Senator MCCASKILL [continuing]. Highly, frankly, questionable expenses that we have embraced without—

Dr. O'TOOLE. Well, you are hitting on an important seam. Bio-defense is one of these issues which is very important to national security but is not a top priority of any one agency. It is an inherently interagency set of responsibilities that is distributed over many different agencies.

It primarily resides in HHS. What S&T does in DHS is we examine potential threat agents and we do analyses of these threats and then we determine if they really look like they could be made into a biological weapon. At that point, we hand off that information, which is called a Material Threat Determination, to HHS. They do their own analysis as to whether or not it is a highly consequential public health problem, and on the basis of those data, they decide whether and in what way to invest in medical countermeasures.

Senator MCCASKILL. I have a number of more questions about BioWatch, but I know my time is up and you all may want to go, because we have billions in BioWatch and it is almost as bad as Raxi.

Chairman CARPER. Well, you are going to get another chance.

Senator MCCASKILL. Thank you.

Chairman CARPER. So do not go away. Thanks for those questions. Thanks for the answers. That was a good tutorial for me.

I telegraphed my pitch earlier, I think just about the time Senator McCaskill was getting here, and I want to go to the Southern border. Talk to us a little bit about force multipliers. One of the things that some of us have been concerned about the—I supported the immigration reform bill. I did so. I was not convinced that we really need to add 20,000 Border Patrol officers down on the border given how many we have there. We spend more money for border security right now than we spend in all other Federal law enforcement activities combined, so that is a lot of money.

I am convinced that we need more people in what we call the ports of entry, those lands ports. We have huge amounts of vehicular traffic, truck traffic, a lot of trade going back and forth. I saw some really interesting and impressive technology, a handheld de-

vice called the ELMO used at the ports of entry by our Customs and Border Protection officers.

And one of the things that I want you to talk a little bit about is what are some fruits of our R&D activities that have been deployed along our Southern border with Mexico that we can point to and say, this is working and this is where we got the idea. Where did the idea come from? Maybe it came from your customers down on the border, the people who work there for us.

Dr. O'TOOLE. Mm-hmm.

Chairman CARPER. And maybe give us some insight into some of the activities that you are working on that we hope will help make the men and women we have on the border, 20,000 Border Patrol, 21,000 Border Patrol and thousands of others at the land ports. Talk to us about that—

Dr. O'TOOLE. Mm-hmm.

Chairman CARPER [continuing]. What we have that is deployed, how you all worked in it, and some projects that you are working on that will enable us to be even more effective.

I guess the implicit question is, what do we need to be doing here to support those activities so that those thousands, tens of thousands of people we deployed on the border can be more effective.

Dr. O'TOOLE. We are doing a lot of work on the border. The Southern border is not a consistent entity. The kinds of technologies that will work in Arizona are different from what we need in Texas, for example, where there is a lot more vegetation and a river to cross and a very fast vanishing point once you get across. You can get in a car, be on a highway, and be gone very quickly.

We have done, as I said, a recent operational analysis that shows that we can change procedures at no cost in a way that would reduce the time CBP agents spend processing aliens whom they pick up and get them back out to the border. We have made suggestions of other process changes that would cost some money, because they involve changes to computer systems, that would push those efficiencies further.

We think of the border in terms of air surveillance, ground surveillance. On the Southern border, underground surveillance is very important because we are seeing more and more tunnel activity. One of the projects that we have underway in collaboration with DOD and some of the intelligence agencies is to figure out how we can guide Border Patrol agents in using the proper technology to find tunnels. It turns out that different technologies work differently depending upon the soil conditions. So we are creating a compendium of what works where and how to maximize your likelihood of finding tunnels.

We have also instrumented some of the public infrastructure tunnels, the sewer drains and so forth, that people use as conduits so that we have more awareness of people coming through there and can more efficiently deploy Border agents when there actually is activity and not having them stand at the entry of the tunnel day and night.

We have deployed ground-based radars and something called a trip wire on the Southern border. The trip wire is buried and it follows the contours of the land. One of the problems with the cameras and radars is it cannot see into the gullies. The trip wire costs

about a tenth as much as the fence to deploy, has a very low false positive rate, allows you to determine whether it is an animal or a person or a vehicle that has tripped the wire, and has been very effective so far. It is in operational field testing now on the Southern border.

We have also done a lot of work in marine surveillance and have a major program underway with Air and Marine Operations Center (AMOC) to——

Chairman CARPER. I am sorry, with whom?

Dr. O'TOOLE. AMOC, the Air and Marine——

Chairman CARPER. OK, thanks.

Dr. O'TOOLE [continuing]. And the CBP which uses DOD technology to gather more data from different sensors. We are taking existing sensors and repurposing them. So, for example, we are taking a National Oceanic and Atmospheric Administration (NOAA) weather buoy, changing the radar signal a little bit to give us notice of small dark boats in the area.

So we are taking more data. We are putting it into this open mongoose system that fuses the data, aggregates it and analyzes it and then spreads it out to the people who need to use it in the Port Authorities and so forth. That program is now deployed in pilot at AMOC and will become progressively more functional over the next 6 months or so.

We have also taken the mobile surveillance systems, which are the cameras and radar on trucks that CBP relies upon, particularly in Arizona, and we have upgraded them so that you have a wider field of view, a better resolution. We have improved the software so that they are still operable in bad weather, in windy weather, and we have made them easier to use and lowered the maintenance and operational cost. They, too, are now under operational testing at CBP.

Chairman CARPER. Senator McCaskill, we could almost have a hearing—this is fascinating stuff for me. I spent a fair amount of time down on the border with Senator John McCain and Secretary Napolitano, Congressman McCaul who heads up the Homeland Security Committee over in the House. This is really actually very helpful information in terms of us passing a comprehensive immigration reform bill that actually tries to strengthen further our border security.

Dr. O'TOOLE. We——

Chairman CARPER. Let me just mention——

Dr. O'TOOLE. Of course.

Chairman CARPER. I want to yield to Senator McCaskill, but we will come back and maybe have another round.

I feel bad for Mr. Maurer just sitting here. He is just sitting here listening to your testimony, rolling his eyes—no, he is not rolling his eyes. [Laughter.]

Mr. MAURER. No. I have my game face on. I am staying focused. [Laughter.]

Chairman CARPER. Do you want to jump in here?

Mr. MAURER. Yes, sure.

Chairman CARPER. Before you do, and then I need to yield to Senator McCaskill, this guy named Tony Wayne—Senator McCaskill probably knows him—he was the No. 2 person, Deputy

Chief of Mission (DCM), over in Kabul in Afghanistan when Karl Eikenberry was our Ambassador there. He is now our U.S. Ambassador to Mexico. And I talked with him on the phone last month just to get some input on border security, what we ought to do more of or less of.

And one of the things we talked about were tethered dirigibles, lighter than air assets, and we talked about what we have deployed in Kabul in lighter than air surveillance and we have down in Kandahar and other places and he says it has been very effective in that part of the world. And we talked a little bit about using tethered dirigibles.

If the wind is over 15 knots, you cannot fly a drone. We only have four drones in Arizona. We only fly two of them at any point in time. They fly 5 days a week, 16 hours a day. The rest of the time, they are not around. They are around, but they are not being used. The C-206 aircraft that we basically send—we have 18 of them. We send people out with binoculars to look at the border, not very smart, but there is a lot of technology. But when we come back, I want to ask you about tethered lighter than air.

Mr. Maurer, just jump in here and then I am going to yield to Senator McCaskill.

Mr. MAURER. Just really quickly, two points on the Southern border. One is we currently have ongoing work for the House Science Committee looking at R&D efforts on the border maritime realm at DHS. That report will be forthcoming in September, so be looking for that. I think that could help in deliberations.

The second point I would like to make is as the Congress considers what to do on comprehensive immigration reform it underscores, really, the importance of having a strong management foundation at the Department, because if we are really going to be hiring 20,000 more additional Border Patrol agents, that is a tremendous human capital challenge. You are also going to have to put information technology (IT) in the hands of these people. They are also going to have to have financial management systems to track the costs. And you are going to require new technologies and put them in their hands so they can do an effective job. So, really, it is the management foundation that enables that mission, and that is why we placed a lot of emphasis in terms of our oversight and our work on the management front and I think that is one thing to always keep a good focus on.

Chairman CARPER. That is a great point. Let me just ask our staffs, both the Democrat and Republican staff here, just to make sure we come back to Mr. Maurer on that. If we are fortunate enough to get into conference on immigration reform, it is a huge amount of money we are going to spend in the Senate-passed version. I am not convinced all of it is wisely. Let us just make sure that we are coming back to the points that he made, OK. Thanks very much. Senator McCaskill.

Senator McCASKILL. Thank you.

You have clarified what I think you see a role in terms of stockpiling vaccination or treatment for bioagents that could be used as a weapon against Americans. Are you going to recommend or have any opinion as to whether or not we should buy additional doses of Raxi, since it is all going to be worthless in 24 months?

Dr. O'TOOLE. So, S&T participates—in some cases, I am the participant—in what is called the Executive Steering Committee at HHS that reviews these decisions periodically. I raised——

Senator MCCASKILL. So, were you part of that when they made the decision to purchase it, but you had no idea how much it was?

Dr. O'TOOLE. I do not think I was part of the decision, but I raised concerns on the point of the strategic intent of what we were doing.

Senator MCCASKILL. Mm-hmm.

Dr. O'TOOLE. Anthrax is of great concern as an agent because we have seen it used. The U.S. built anthrax weapons. We know the Russians did, as well, in their time, as did the British. And there are few technical barriers to doing so. So, it is the kind of weapon that you could imagine terrorists getting their hands on.

The other problem with bio——

Senator MCCASKILL. Although there are technical barriers to making lethal—according to the documentation I have read from scientists, there are barriers to making lethal doses of antibiotic-resistant anthrax.

Dr. O'TOOLE. Yes. That is true. But——

Senator MCCASKILL. But that is what we are buying the antidotes for at \$5,100 a dose.

Dr. O'TOOLE. There are technical barriers to making multi-drug-resistant anthrax. There are no technical barriers to making an anthrax that is resistant to the primary drugs in our stockpile. Some of this is getting into classified information, so I apologize. But multi-drug-resistant anthrax, I think, is not likely to be a terrorist weapon.

And I was part of a discussion in DHS in which we did not think it was wise to proceed with an R&D project to develop an antidote, if you will, a drug product against or a vaccine against multi-drug-resistant anthrax.

Senator MCCASKILL. I guess I am back to my question. Will you be recommending that we buy more doses of Raxi that we have spent \$334 million on that will be worthless in 24 months? Yes or no?

Dr. O'TOOLE. No.

Senator MCCASKILL. OK. BioWatch—how much have we spent on BioWatch?

Dr. O'TOOLE. How much has S&T spent on BioWatch?

Senator MCCASKILL. How much has DHS spent on BioWatch?

Dr. O'TOOLE. Billions of dollars. I do not know the exact——

Senator MCCASKILL. And how much of that was spent before you took your position?

Dr. O'TOOLE. S&T has spent no money on BioWatch since I took my position.

Senator MCCASKILL. How much had DHS spent before you took your position?

Dr. O'TOOLE. I do not know that figure. I can get it for you.

Senator MCCASKILL. I want to clarify for the record, it has been your stated position that you do not support or do not believe we should go to the next generation of BioWatch?

Dr. O'TOOLE. My stated position before I became Under Secretary was that investing in Gen-3 BioWatch while not also invest-

ing in more traditional approaches to public health surveillance was a mistake.

Since I have become Under Secretary, I have advised the Department that the performance of the Gen-3 candidates that the Office of Health Affairs (OHA) has tested thus far is not such that under DHS's own acquisition procedures would warrant further investment until performance can be improved. And those recommendations, which were mirrored by the Homeland Security Studies and Analysis Institute (HSSAIs) evaluation, which the Secretary requested, were a large part—not the only, but a large part of the basis for the Acquisition Review Board's (ARB) decision to put a hold on further acquisition of Gen-3, on proceeding with the Gen-3 acquisition.

Senator MCCASKILL. And is there any effort at this point to proceed with acquisition of assays or anything in order for us to do blood testing on first responders or testing of blood donors or anything of that nature?

Dr. O'TOOLE. As part of BioWatch, you mean?

Senator MCCASKILL. In lieu of BioWatch. What has been advocated, and once again by Mr. Danzig, is that we develop what would be a very expensive, obviously, very expensive process of doing blood testing of, I guess, first responders that would volunteer to have their blood tested on a regular basis and/or others have suggested blood donors. It has been written up in some of the medical journals that they do not think that would be effective.

Is there any discussion in the groups that you sit on, in the places you collaborate, or in the executive committees you stand on, to substitute for Third Generation BioWatch a blood testing protocol that would somehow, in lieu of BioWatch, give us notice that there is some kind of bioweapon being unleashed somewhere in America?

Dr. O'TOOLE. Not for substitution for environmental sensors. We are going to need environmental sensors and we need to improve what we have. Whether that is Gen-3 BioWatch is one set of questions. I do not think it is, but that is a technical question that we have to determine empirically.

The overall problem is that what we want is very early notice of a bioattack, if possible, before people become sick with symptoms, because by then, it is, as far as we know, very difficult to rescue them. That is certainly the case with anthrax, for example.

Ten years ago—even the Defense Science Board suggested that we should be investing in rapid, cheap diagnostic tests that would be part of a panel of blood tests that people coming in for clinical care would get. So, for example, if you have an upper respiratory infection, it would be good for your doctor to know if that is viral or bacterial in origin because the latter requires antibiotics, the former does not. It would have all kinds of good consequences beyond that individual patient's well-being.

If we had a cheap enough diagnostic that when you ran that test you also, by the way, checked for anthrax, tularemia, or the other bioweapons agents that we thought might be used, at almost no extra cost, it would give us a way, if we deployed that, for example, in a sample of hospitals around the country, to achieve very specific and actionable early warning.

We have reached a point technologically where these kinds of very fast and simple tests are almost within reach. There are very few market forces pressing diagnostics forward, and one of the problems is how do we actually have the Food and Drug Administration (FDA) approve these multianalyte tests that look for more than one bug at a time.

But we do need a way to get beyond the current process of diagnosis, which is to take blood from a sick person, someone who is already sick, culture that blood, which itself takes 24 to 48 hours, and then go looking for the bug, which you often cannot find even if it is there. So you are now 2, 3 days into the bioattack and you do no good for that individual patient, who is probably dying by now, and it does not give you the kind of early warning we are looking for to protect the population with vaccination or whatever.

Senator MCCASKILL. Dr. O'Toole, I am trying to make the point here that we spent billions on a tool to tell us if we were having a bioattack and now there seems to be consensus that we have wasted it, because we are not going to use it anymore. We are not going to build upon it. Because if we do not do Third Generation, obviously, we are saying that it is not going to be effective for what we are trying to do.

Dr. O'TOOLE. I do not think that the money spent on BioWatch as deployed has been wasted, OK.

Senator MCCASKILL. OK.

Dr. O'TOOLE. I think it is possible to improve BioWatch as deployed in ways other than investing in Gen-3.

Senator MCCASKILL. Let me move on to a couple of other things. What is the ratio of contractors to employees at S&T?

Dr. O'TOOLE. It is about one-to-one.

Senator MCCASKILL. So you only have one contractor—so the vast majority of your budget, half of it is spent on employees and half of it is spent on contractors? Are you not passing through most of the money to people—

Dr. O'TOOLE. No.

Senator MCCASKILL [continuing]. Who have contracts with you to do research?

Dr. O'TOOLE. Yes.

Senator MCCASKILL. OK. So—

Dr. O'TOOLE. Our Mergers and Acquisitions (M&A) budget is spent on Federal employees. Our contractors are different from a lot of Systems Engineering and Technical Assistance (SETA) contractors. We contract, for example, with scientists to help us on projects—

Senator MCCASKILL. I am very aware of who you contract with, and I am on the Armed Services Committee and have spent years on contracting and R&D. So I understand that the vast majority of the money that we appropriate to you is not spent on your employees, correct?

Dr. O'TOOLE. Correct.

Senator MCCASKILL. What percentage of the money we appropriate to your Department is spent on employees as opposed to other contractors? They may be scientists, but they have a contract with us. They have an R&D contract with us. They have a develop-

ment contract with us. They have all kinds of contracts that are being managed, ostensibly, by your division.

Dr. O'TOOLE. Sure.

Senator MCCASKILL. OK.

Dr. O'TOOLE. Well, I can get that for you. The problem is that I have my M&A budget, which tells me what we are spending on Federal employees, and then what you are calling contractor costs are embedded in our project costs, so I do not have an overall sum of that number.

Senator MCCASKILL. What percentage of your employees are actually doing research as opposed to overseeing research done by others?

Dr. O'TOOLE. The only employees in S&T who are actually doing research are those who work in our five laboratories.

Senator MCCASKILL. OK. So I know I am over, and I can finish on the next round—

Chairman CARPER. Yes, you are.

Senator MCCASKILL [continuing]. Because this will involve Mr. Maurer, because I want him to talk about some of the documentation for acquisition and how lacking it is, especially when you realize this is primarily a pass-through organization.

Chairman CARPER. Mr. Maurer—do you want him to respond at this point in time or do you want to just—we will have one more round.

Senator MCCASKILL. Well, this is me studying your reports, so maybe you can speak to it. We obviously have acquisition documentation that has not even been completed and you are in the sustainment phase. It does not do you much good to figure out that the acquisition is not needed if you are already supporting it in a sustainment phase, and I studied your report and would like you to speak to the fact that since, primarily, this is a pass-through organization, a core competency is going to be the documentation at the onset of these projects, before we ever begin paying for these projects. Could you speak to that, Mr. Maurer?

Chairman CARPER. I would like for you to go ahead and respond to that question. I would ask you to do it fairly briefly, if you could. If you need more time, we will just come back for one final round.

Mr. MAURER. I will keep it short and sweet. You hit on a key point and a key challenge of acquisition at DHS, not just on BioWatch, but many others. DHS historically, since they developed acquisition guides, have had a good policy. They have not always followed that policy. They have gotten the cart before the horse in many acquisition projects, and not just BioWatch, and it is exactly the point you pointed out, which is that they have not clearly defined the requirements up front and/or they have not clearly demonstrated that the project or the program is going to work as advertised in real world conditions before spending a lot of money trying to deploy it, and that has been a problem that has plagued the Department for years.

They are starting to take action to address that. They are trying to revamp their approach to acquisition, and I think that is encouraging, but they still have a long way to go.

Senator MCCASKILL. Thank you, Mr. Chairman.

Chairman CARPER. That was short and sweet. Thank you.

Mr. MAURER. Thank you.

Chairman CARPER. I am going to go back, if I can, to—I just wish Senator McCaskill were more passionate about this stuff. [Laughter.]

Senator MCCASKILL. Sorry. I know I am obnoxious. I apologize, Dr. O'Toole.

Chairman CARPER. Actually, she is on her good behavior today.

Senator MCCASKILL. But it came out of your mouth. There has not been enough oversight here, and I do not want you to be scared because I do have someplace I have to be in a few minutes, but I could go on a long time on this Department.

Chairman CARPER. OK. That is great, because I have someplace I need to be in a few minutes, too. [Laughter.]

Let us go back a little bit to tethered dirigibles, the kind of technology that Tony Wayne, our Ambassador to Mexico, was talking with us about when he saw it firsthand over in Afghanistan. This may be outside your lane or outside your wheelhouse, but in terms of the kind of technology we could put on tethered dirigibles to do surveillance work along the borders on days that the drones are not flying, that they cannot get into the controlled airspace of the Department of Defense, any idea? We have all these assets over in Afghanistan. The question is, do we want to leave them there or can we bring them back here? Could we redeploy them along the border? Any thoughts along those lines?

Dr. O'TOOLE. Yes. S&T has actually—

Chairman CARPER. And, Mr. Maurer, if you have any thoughts along those lines, we would welcome those, too.

Go ahead, please.

Dr. O'TOOLE. S&T has actually tested the DOD Aerostats on behalf of CBP to see how they perform. They are great. There is a lot that you can do with them. They do not perform well in weather which is fairly frequent on the border.

The trouble with the Aerostats is they are very expensive. They are very expensive to operate and maintain. So we are going to have to make decisions—

Chairman CARPER. That is interesting. You would think with an Aerostat, you put in your tether, you put it up in the air, and it stays up for days as opposed to having to have an aircraft, either manned or unmanned. Even the drones are unmanned, but you have huge costs to support them. That is interesting that they would be that expensive.

Dr. O'TOOLE. Yes. I mean, look, we are going to need a suite of technologies on the border and S&T is very eager to participate in these decisions. Going back to your how can we help you question, we would like to be engaged. We think there should be some kind of steering committee that ponders these difficult decisions and ways investments in one technology or another and—

Chairman CARPER. Well, we are going to be needing to use some steering here, so try to figure out how—

Dr. O'TOOLE. Well, and there are going to be very difficult decisions to make, as Senator McCaskill is pointing out. These are complex technologies, complex situations, and a lot of judgment will have to be brought to bear.

But the Aerostats are great. They are not the answer. There is a lot of very cool technology out there, and putting together a package that is efficacious and cost effective and can actually be maintained over time is going to be the challenge.

Chairman CARPER. All right. Thanks.

I want to turn, if I could, to—Mr. Maurer, anything you wanted to add to that now?

Mr. MAURER. Just really briefly.

Chairman CARPER. Please.

Mr. MAURER. We issued a report in the last year or two specifically on Aerostats and I will get that directed to your staff.

Chairman CARPER. Give us just a little tease on it, a little—

Mr. MAURER. Well, I did not actually do it myself, but we looked across the different Aerostat technology. I think a lot of it was focused on DOD, but it may be useful for your purposes and oversight on this Committee, as well.

Chairman CARPER. I would just ask our staff, let us just make sure we followup on that offer. Thank you.

If I could, one question and then I am probably going to go back to yield the floor to Senator McCaskill.

Senator MCCASKILL. I just have one more.

Chairman CARPER. OK. But let us talk a little bit about cybersecurity R&D duplication. I think the distinction you made between overlap and duplication was a good one and very instructive for us. But for Dr. O'Toole, let me just ask, one very important issue to this Committee and I think certainly to the Senate and to the Congress and to the President and our country is that of cybersecurity. And in such a fast-paced and evolving environment like ours, cybersecurity research and development is really important, as you know, as we try to stay out ahead of the bad guys.

At the same time, a whole lot of agencies have a mission that touches on cybersecurity, a big one, but one of several. How does S&T coordinate with some of these other Federal agencies, and maybe even non-Federal agencies, but especially the Federal agencies and with the private sector to avoid duplication of cyber research and development efforts?

Dr. O'TOOLE. Cybersecurity is coordinated by law by the High-Performance Computing Act of 1991 out of the Office of Science and Technology at the White House. It is under the aegis of what is called Networking and Information Technology Research and Development (NITRD), the National Coordinating Office for Networking and IT R&D. So this NITRD is broader than just cybersecurity, but it has a senior steering group devoted to cybersecurity R&D coordination and also several interagency working groups devoted to cybersecurity.

Our Director of our Division of Cybersecurity in S&T co-chairs the Non-Classified Cybersecurity Working Group. We do not do classified cybersecurity work. And they meet very regularly. There are many working groups on big data. There are various aspects of cybersecurity. We are also participants in the Classified Steering Committee on Cybersecurity.

And the collaboration and cooperation is quite intense. This is an area of R&D that is very coordinated in the U.S. Government. We have a very good handle on who is doing what, and people are

eager to stay in their lane, to collaborate with others in order to get the most out of resources. We are collaborating, as I said, with DOE, for example, on electric grid cybersecurity. And they meet monthly to talk about particular topics and everybody presents what they are doing. So who is doing what is made quite transparent.

To your question about how do we cooperate with the private sector, the U.S. Government's investment in cybersecurity is coordinated through the Industrial Coordinating Councils, also managed out of the White House. So we are very involved in S&T in the Financial Sector Coordinating Council, in the Electric Grid Council, and also, we have a consortium of the big five oil and gas companies with whom we are working on a variety of cyber projects that they choose. They decide what the biggest vulnerabilities are and then we help them with fixes and we help them to disseminate those fixes.

Chairman CARPER. Take just 1 minute, and then I am going to yield to Senator McCaskill and run out and take a quick phone call, but how do you track the performance of your cyber R&D programs? And maybe just give one or two quick examples, but just be very brief, please.

Dr. O'TOOLE. Cyber moves very fast. You can get a fix out there and it will be overtaken by the adversary months later. So this is very complicated.

We basically measure progress by whether our solution has been picked up. We have had McAfee and Microsoft, for example, buy and incorporate cybersecurity solutions that we developed by supporting small companies. We also track how widely it is being used. In that one case, a \$5 million investment in collaboration with DARPA, actually, resulted in half-a-billion computers being equipped with this particular malware protection.

And we also get feedback from the venture capital community, which is extremely active in this area now, on the quality of our fixes. They are very interested in what we invest in because we, have a reputation of doing good work. But it is hard to judge efficacy in this field and we do it by, does it get commercialized? Does it get picked up? And how widely dispersed is the fix?

Chairman CARPER. OK, thanks.

I am going to yield to Senator McCaskill and I will be right back, so—

Senator MCCASKILL. I have a—and I will not be long, so should I dismiss the witnesses when I am finished? No. Ask them to stay? OK. I did not get what he said. [Laughter.]

You are on your own. I am going to just ask you a couple of questions and you are on your own.

I do understand that this is difficult, what you are tasked with doing, because you are being tasked to do cutting-edge research and technology to protect America. And I am not convinced that we are doing cutting edge. I think that there are component parts in DHS that are doing—and the GAO report, in fact, cited that, that we have research going on in component parts.

I also am aware, Dr. O'Toole, that, for some reason, fair or unfair, your agency ranks at the very bottom in terms of best places to work. It is very bad, your rankings, from the people who work

there. And I do not want you to—if you want to, you can respond today, but I would, as part of my questions for the record, there will be a number of specific questions about various projects, about when is the next risk assessment, how quickly are we pulling the plug.

I do not want to be critical that you are pulling the plug on Gen-3 for BioWatch because I think part of the problem is plugs have not been pulled and we have wasted an awful lot of money. And, believe me, you have a way to go before you get to your big brother, the Pentagon, in terms of money that has been wasted, and the entire government in terms of IT.

But I would like you to maybe in answers to these questions try to give a thoughtful response as to why the people who work in your Department rank your Department so low in terms of a place to work and to address the risk assessment and the fact that it is not occurring every 2 years and that means that we are getting down the line on things that are being done without really evaluating on an ongoing basis whether or not we are throwing good money after bad.

I think your agency because of the responsibilities you have, has a much higher risk than many others in terms of good money being thrown after bad. And I am worried, because of a lack of documentation on projects, the fact that some of your recommendations that you are giving to some of your components, you did all that work on transit workers and then TSA just ignored you. Basically, we spent a lot of money developing technology for TSA and they said, never mind, we do not want it, and did not pay any attention to you.

So there is something not right here, and I want to try to spend some time and energy—and be fair to you—to respond, because I do not think we have done enough oversight in this area. But I have kind of gotten into it now and I find it fascinating and interesting and that is really bad news for you because it means I am not going to go away until we get some more specific answers to these.

So if you would like to respond about your——

Dr. O'TOOLE. I would.

Senator MCCASKILL [continuing]. Issues here, but it will also be part of the questions I will give you for the record.

Dr. O'TOOLE. Good. I would appreciate that, Senator.

First of all, I would like to offer to come and talk to you at length about these issues and particularly how S&T is trying to—and I think we have succeeded to a great extent—evolve a very efficient approach to R&D and how we are trying to partner with the components who do the acquisitions, and as you say, tighten up the front end of acquisitions when we devise the requirements that are going to guide what it is that we invest in. We do not want to find out at the tail end, as we are about to procure something, that we made a mistake and we are not getting what we need. But I would welcome the opportunity to talk about this or anything else you would like in person and at length.

In terms of morale, this has been a source of enormous distress to me and to the Secretary, and actually to the entire DHS leadership, and we have discussed it for hours on end. I am happy to give

you my view of what I think is going on, which I am sure is imperfect. We in S&T did followup surveys after the first abysmal congressional survey to try and get to the bottom of what is wrong and there are many facets to this.

First of all, it would be useful if Congress made the survey every 2 years rather than every year, because what happens is just as we start to put in place the fixes, the results of the previous survey, the next one comes out. So it feels like there is never any progress.

DHS employees are there for the mission. They say this again and again and they say it in the survey. I think it is very disheartening to have your agency constantly, almost without exception, bashed in the media and criticized. And God knows, as you say, we have this huge mission that is very difficult——

Senator MCCASKILL. Welcome to our world. Amen. Touche. [Laughter.]

Dr. O'TOOLE. That is one thing, because these people are public servants. They are not in it for the money.

Second, one of the things that they told us in our survey was that they felt they did not have enough recognition for what they did do, so we put in place a whole series of, not rewards, but recognition ceremonies for progress that we had made and extra efforts that people had did, all of which has gone away in sequestration. We cannot have reward ceremonies. We cannot give bonuses. The 3-year freeze in salaries is beginning to really hurt. I mean, people are hesitating to buy houses and have second children because of this. So, over time, even though these people are not in their jobs to make money, that long-term pay freeze is very important.

For us, one of the big impediments to doing our work, to getting out and meeting our customers and collaborating with others, is this rather draconian freeze on travel and conferences. Particularly for R&D, conferences are how we do work. And when you have to hire contractors in order to manage the paperwork involved in requesting permission to travel, something is wrong.

So in the interest of more efficiency, in the interest——

Senator MCCASKILL. Wait a minute. You have 439 people that work for you and you have to hire a contractor to do travel documents?

Dr. O'TOOLE. Yes, to do it more efficiently, because I do not want to use Ph.D.s to fill out travel documents. We put together a very efficient process——

Senator MCCASKILL. So all the people that are overseeing contracts and paperwork are Ph.D.s that work for you? What percentage of the people who work for you are Ph.D.s?

Dr. O'TOOLE. No, the people who are overseeing contracts do not work for me. They work for the Office of Management.

Senator MCCASKILL. OK.

Dr. O'TOOLE. We can talk about this at length——

Senator MCCASKILL. Yes, we need to, because——

Dr. O'TOOLE. I should not have gotten you started.

Senator MCCASKILL. You should not have told me you were hiring contractors to handle travel documents. That was not something——

Dr. O'TOOLE. Well, no, it is——

Senator MCCASKILL. Now I have another set of questions I need to ask.

Dr. O'TOOLE. But I am saving money and I can prove it.

Senator MCCASKILL. I would like to see that.

Dr. O'TOOLE. OK. I can prove it. I am saving money doing it that way.

Anyway, what has happened is people, as I am sure you do, feel very beleaguered. One big problem is the Civil Service Reward and Advancement Program. People say it is not fair. It is not. It is not. It is very broken. I mean, I am trying to run this organization and I have very little capacity to hire or fire. Imagine running an organization of this size and not being able to hire the skill set you need or fire people who are not performing. But that is the case across the Federal Government and people feel that very much is unfair.

Senator MCCASKILL. Well, I appreciate your answer. I think what I would like you to give some thought to is this is a comparative survey and a lot of the problems that you indicated just now are across the Federal Government. So that would not be the answer as to why you are 292 out of 292, because 250 have those problems and 10 have those problems. So that is what I would like you to reflect on, and we can visit——

Dr. O'TOOLE. I will——

Senator MCCASKILL. And I really appreciate you being here, and I hope you understand that all of this oversight is because it is needed and it is part of our job, and I hope that I was not too rough on you, but I was taken aback when you first kind of did not want to talk about Raxi and what it was and I think, clearly, in your job, I expected you to want to talk about it.

So we will visit in person and continue and I will get questions to you.

Thank you both very much. Thank you, Mr. Chairman.

Chairman CARPER. Thanks very much, Senator McCaskill. Thank you for your passion that you bring to this work.

Sometimes I offer our witnesses an opportunity to give a short closing statement. Since we are running overtime right now, I am going to ask you to do that. You have just, sort of, given one, Dr. O'Toole, and I am just going to ask Mr. Maurer if you would like to make just a short concluding statement, just if you want to reiterate some things, emphasize some things, underline some things, feel free. If something new has come to mind you think you ought to leave it before us, this is a good time to do that.

Mr. MAURER. Sure. Absolutely. I think the key takeaway from our discussion earlier from the GAO perspective is that it is important for DHS to define R&D. It is important for DHS to be able to know who is doing R&D within the Department, to have effective coordination mechanisms in place, to be able to make the necessary strategic tradeoffs, to make the wise decisions and make the most effective use of taxpayer dollars.

Chairman CARPER. All right. Thanks.

Dr. O'Toole, just one last quick comment from you, if you want.

Dr. O'TOOLE. Just I appreciate the opportunity to be here and I hope the Committee will be an advocate for using science and technology to make DHS more effective, efficient, and safer.

Chairman CARPER. I think it is safe to say that we will be. I hope you will not leave here discouraged. I hope you will leave here encouraged, both of you.

I said to our staffs on both sides here, I said, I came into this hearing sort of uncertain as to how productive it was going to be, how constructive it was going to be. I think it has been, for me, very helpful and really encouraging. I am encouraged by your leadership, Dr. O'Toole, very encouraged.

Dr. O'TOOLE. Thank you.

Chairman CARPER. And we have a lot of witnesses who come before us—I would say this to Mr. Maurer—we have a lot of witnesses from GAO. You are just two very excellent witnesses. For those who you work with and whom you lead, I want you to take back my appreciation for the work that is being done.

Our staffs have heard me tell, probably more than they want to remember, the story of my driving to the train station. I go back and forth on the train most nights to Delaware. I drive into the train station early in the morning, listen to National Public Radio (NPR), and before I got to the train station to catch my train to come down here, and hearing about a year ago an international study done to ask the following question. What is it that gives people joy or satisfaction in their work? What makes people really satisfied in their work? What is it?

And some people said they—from all over the world, thousands—they like getting paid. [Laughter.]

Some people said they liked having fringe benefits, sick leave, vacation, pension, whatever. Some people said they like the folks they work with. Some people said they like the environment, the space in which they work.

But do you know what most people said? Most people, the thing that gave them real satisfaction about their work is that they found that the work they were doing was important. They felt it was important. And the second half of that is they felt like they were making progress. Put those two together. That is what most people said.

And I think the same is true here. We had a near meltdown in the Senate, as you may know. The old nuclear option fortunately defused and I think we have just a renewed spirit of cooperation and collegiality. I hope it extends beyond this week, and I am encouraged that it will.

But just to take back to the folks you work with and lead that the work you are doing is important and I believe we are making progress, and God knows we need to.

I have a beautiful closing statement that was prepared for me. I just have one quote here I am going to just throw out before I close, and it is Carl Sagan who once said, "science is a way of thinking much more than it is a body of knowledge." That is pretty good.

Part of our challenge is to figure out how to use science, good science, to help protect our country and the people here, and I am

encouraged we are doing a lot of smart stuff, and clearly, we can do more of that.

I have a couple questions I am going to submit for the record, and I know Senator McCaskill and, I presume, Dr. Coburn and other colleagues will, too. The hearing record is going to remain open for about 15 days—I think that is until August 1—at 5 p.m. for the submission of statements and questions for the record.

I want to thank our staffs, both our Minority and Majority staffs, for their work in preparing for this hearing. They do not just happen by themselves, but they have done good work. You all have done very good work here today.

And with that, this hearing is adjourned. Thank you.

Dr. O'TOOLE. Thank you, Mr. Chairman.

[Whereupon, at 12:17 p.m., the Committee was adjourned.]

A P P E N D I X

Opening Statement of Chairman Thomas R. Carper

“The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency” July 17, 2013

As prepared for delivery:

Earlier this year, the Department of Homeland Security turned ten years old. To mark that anniversary, Dr. Coburn and I announced that this committee would hold a series of hearings examining whether the Department is effectively and efficiently accomplishing its core missions. Today's hearing – the second in our series – will focus on the role of the Science and Technology Directorate.

Threats to our national security evolve constantly. So too, then, must the strategies and technologies we use to combat them. That's where the Science and Technology Directorate comes in. The work performed by the men and women at the Directorate cuts across all of the various components and missions of the Department. That work involves the harnessing of cutting-edge technology and research and development projects from the private sector, universities and the National Labs to deploy force multipliers that can make us more effective in the effort we embarked on after 9/11 to prevent and respond to terrorist attacks and natural disasters. In essence, the Science and Technology Directorate functions as a problem solver.

For example, the Science and Technology Directorate worked closely with the Transportation Security Administration (TSA) and the Defense Advanced Research Projects Agency (DARPA) to develop a better x-ray system for checked baggage. As a result of that work, a 10 percent reduction in false alarms rates is expected. This is projected to save millions of dollars in efficiencies through the reallocation of staffing costs.

As another example, the Directorate examined agent operations at two stations along the southwestern border in Texas that process apprehended illegal immigrants. It recommended improvements to their operations that enabled the two border stations to significantly reduce their processing time, saving up to two hours per illegal immigrant processed. This enabled an additional officer to remain in the field rather than be stuck in the office processing paperwork.

In its early days, the Directorate was the subject of criticism as it carved out its role in the Department. It focused then on basic research which, in some instances, could not be quickly put to use. Today, I believe that the Directorate has proven itself to be more effective. More often than it has in the past, it has a laser focus on development of critically needed products that can be used immediately.

As we all know, the fiscal environment in the federal government has been very challenging over the past several years. This underscores the urgent need for agencies across government to spend taxpayer dollars more wisely. The Science and Technology Directorate can – and has been – a key part of the Department of Homeland Security's efforts in that regard. It is critical, then, that it continue to work aggressively and effectively with Department components and first

responders to find solutions that allow DHS and its partners to operate more efficiently and effectively.

I thank the witnesses for coming today and look forward to their testimony – especially about how we can continue to use the Science and Technology Directorate to get better results for less money – something I’m determined to use my Chairmanship of this Committee to push throughout our federal government.

###

**Testimony of the Honorable Tara O'Toole, M.D., MPH
Under Secretary for Science and Technology
U.S. Department of Homeland Security**

**U.S. Senate
Homeland Security and Governmental Affairs Committee**

July 17, 2013

Introduction

Good morning Chairman Carper, Ranking Member Coburn, and distinguished members of the Committee. Thank you for the opportunity to testify before you today in recognition of the ten-year anniversary of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T). During my tenure, the Directorate has built on congressional direction; the leadership of the two Under Secretaries who preceded me, Dr. Charles McQueary and Rear Admiral Jay Cohen; and on the talent and dedication of S&T staff to create a research and development (R&D) organization suited to meeting current and future demands of homeland security missions.

My testimony will describe why the development and adoption of new technologies are critical to meeting current and future demands of homeland security missions; how S&T knowledge products, technical analysis, laboratories, and university-based Centers of Excellence contribute to the effectiveness and efficiency of DHS operations; and how S&T is improving the capabilities and safety of first responders.

I will also describe how S&T has restructured its R&D processes to focus on high-impact projects that are rapidly transitioned to use in the field and that deliver a high return on investment for the American taxpayer.

Our progress toward these ends has benefited greatly from building strong partnerships with DHS Components and first responder communities and by leveraging R&D investments made by other federal agencies, universities, the private sector, and international partners. S&T has also expanded the application of our engineers' and scientists' technical expertise beyond technology development to include the analysis of operational problems, the instillation of systems-based solutions, and assistance with DHS acquisition processes.

Science and technology are essential to achieving DHS missions and to gaining operational efficiencies

DHS confronts a global landscape in which technology is both a key driver of evolving threats and an essential source of solutions to these threats. The tide of history has brought us, in the 21st century, to a hyper-connected world where science and technology are pursued and produced on a global scale with ever more powerful tools becoming accessible to nations, groups, and individuals. The United States faces determined and adaptive adversaries who will take full advantage of all the tools available to achieve their ends.

For example, cell phones are both an essential tool for economic development as well as an invaluable aid to recruitment, financing, and planning of terrorist operations. A cell phone costing approximately \$400 today matches the computing power of the fastest \$5 million supercomputer in 1975.¹ The Internet, which an additional two billion people will access by 2025,² is a driver of the modern economy, the medium of choice for distributing recipes for making improvised explosive devices (IEDs), and the source of cybersecurity attacks that the Defense Science Board has called an “existential” threat to national security.³ Revolutionary advances in the biosciences, many of which are not yet translated into products, are expected to have social and economic consequences that dwarf the impacts of information technology. Thankfully, malevolent uses of biology have been limited, but more than a decade has passed since the Defense Science Board noted that “there are no technical barriers to groups or individuals creating a powerful bioweapon.”⁴

Over the past three years alone, we have witnessed several highly complex and consequential disasters ranging from the Deepwater Horizon explosion and subsequent oil spill, to the Fukushima Daiichi nuclear disaster and Super Storm Sandy. Predictions point to the increasing likelihood of these types of events.⁵ Our nation must improve its capacity to predict, prevent, and rapidly respond to and recover from such catastrophes – and science and technology will be essential to addressing these needs. The S&T Directorate is well positioned to be a source for solutions to these challenges.

Technology and analytical capability are the tools which will make it possible to meet growing demands most cost effectively. They are the key to doing more with less. Lastly, the Department faces increasing mission demands that will quickly outpace available resources. Air travel to the U.S. increased 12% from 2009 to 2012 and is projected to grow at 5% each year over the next five years.⁶ Currently, 11.6 million containers come into our ports and are screened each year; DHS estimates that this volume will grow up to 3% per year over the next 5 years.

Mission of the DHS S&T Directorate is broad, varied, and serves many partners

The mission of DHS S&T is to *strengthen America’s security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise*. Congress created the S&T Directorate under the Homeland Security Act of 2002, to among other things “[conduct] basic and applied research, development, demonstration, testing and evaluation activities relevant to any or all elements of the Department.”⁷ S&T also has a statutory

¹ James Manyika et al., *Disruptive Technologies: Advances that will transform life, business, and the global economy* (McKinsey Global Institute, May 2013).

² Ibid.

³ Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (June 2001).

⁴ Defense Science Board, *Biological Defense* (June 2001).

⁵ Adam B. Smith and Richard W. Katz, “U.S. Billion-dollar Weather and Climate Disasters: Data Sources, Trends, Accuracy, and Biases,” *Natural Hazards* 67, no. 2 (June 2013).

⁶ Department of Commerce, “U.S. Commerce Department Forecasts Growth in International Travel to the United States Through 2016,” <http://www.commerce.gov/news/press-releases/2012/04/23/us-commerce-department-forecasts-growth-international-travel-united-s> (April 29, 2012).

⁷ Sec. 302(4) of Public Law 107-296 (codified at 6 U.S.C. § 182(4)).

responsibility for establishing a system for transferring homeland security developments or technologies to Federal, State, local governments, and private sector entities.

In the past decade, S&T has undergone many changes and continues to evolve. The extraordinary breadth and diversity of DHS's missions requires S&T to address a wide range of programs including DHS Components' near-term needs for new operational capabilities and improved operational effectiveness, efficiency, and safety. S&T also has responsibilities related to understanding and creating solutions to biological and chemical threats, and to conducting the R&D required to meet homeland cybersecurity needs. While DHS S&T's work is often identified with technology development, equally important are the Directorate's contributions to homeland security in the form of analyses or "knowledge products." These include analyses of alternative technology options; assessments of complex issues such as the relative risk of different chemical, biological, radiological and nuclear threats; operational testing and evaluation of technologies proposed for acquisition; detailed technical characterization of potential biological threat organisms to support both human and agricultural biodefense; and the creation of consensus standards that enable cost-effective progress across many fields. S&T also manages five national laboratories that provide unique homeland and national security capabilities and has direct access to the Department of Energy's extensive national laboratory system. In addition, the Directorate's capacity to engage R&D activities worldwide is greatly augmented by S&T's nine university-based Centers of Excellence (COEs) and 13 bilateral international agreements.

In order to meet the broad scope of our mission, S&T has built a highly trained and technically-proficient staff that is DHS's core source of science, engineering, and analytical expertise. To utilize our staff and budget for maximum impact, we have focused our energies on efforts that have a direct and demonstrable link to improving the efficiency, effectiveness, and safety of DHS's operational missions and enhancing the safety, interoperability, and communications capabilities of the first responder community. S&T's contributions to the Department and the Homeland Security Enterprise (HSE) fall into four general categories:

- *New capabilities and knowledge products* – S&T creates new technological capabilities that address DHS operational needs or are necessary to address evolving homeland security threats.
- *Process enhancements and efficiencies* – S&T conducts systems-based analysis to provide streamlined, resource-saving process improvements to existing operations.
- *Acquisition support* – The Department achieves more effective and efficient operations and avoids costly acquisition failures and delays by leveraging S&T's technical expertise to improve project management, operational analysis, and acquisition management.
- *Understanding of homeland security risks and opportunities* – S&T's relationships across DHS and the HSE contribute to strategic understanding of existing and emerging threats as well as opportunities for collaboration across departmental, interagency, and state/local boundaries.

S&T's R&D strategy emphasizes high impact deliverables, rapid transition of products to use in the field, and a high return on investment

Since 2010, S&T has pursued an R&D strategy designed to meet the urgent operational needs of DHS Components and first responders as well as Congress' expressed interest that S&T deliver meaningful products more rapidly than the typical decades-long R&D cycle. In addition, S&T's R&D strategy must take account of the wide spectrum of DHS missions and make the best use of S&T's limited resources. To satisfy these requirements, we have re-shaped our R&D efforts in three ways.

First, to ensure that our R&D projects reflect priority HSE needs and accommodate operational realities, S&T has forged strong partnerships with DHS components and first responder communities. Second, DHS's urgent operational needs require rapid technology development time frames. Our goal is to have programs deliver meaningful, useful new technologies to end users and operators within two to five years. To achieve this, S&T focuses on the late stages of R&D. We actively seek out technologies in which others have already invested, and we work to adapt, evolve, and apply these technologies to DHS needs. Third, we seek to maximize our return on investment in R&D by aggressively pursuing collaborations with other R&D organizations – federal agencies, universities, the private sector, and with foreign government partners.

Strong partnerships with DHS Components and first responders deliver results

Innovation and successful technology development requires a deep understanding of the problem to be solved; partnerships with users and operators are essential. In the past, many successful R&D prototypes developed by S&T did not transition because of failure of the project to reflect leaders' priorities, lack of plans for operational pilots, or failure to devise an appropriate and timely commercialization strategy or acquisition process for the technology. Today, all Homeland Security Advanced Research Projects Agency (HSARPA) R&D projects are grounded in "R&D strategies" that are developed in partnership with the users and which explicitly assess the increased capabilities, efficiencies, or safety to be gained should the project succeed. The R&D strategies are used by the Components to inform their acquisition planning timelines so that R&D programs can successfully transition into operational environments. We have learned from some of our most successful efforts, like the Apex projects,⁸ that the better S&T understands the priorities, operational context, and constraints of the end users/operators, the greater the impact of our solutions.

Additionally, S&T's HSE and First Responders Group (FRG) have developed a sophisticated and layered approach for prioritizing the needs of first responders in the 73,000 state and local jurisdictions across the country. FRG works directly with first responder organizations to identify priority gaps in capabilities, establish operational requirements and standards, and ensure interoperability. Projects in FRG's three strategic thrust areas – increasing responder

⁸ Apex projects are cross-cutting, multi-disciplinary efforts requested by DHS components that are high priority, high-value, and short turn-around in nature. They are intended to solve problems of strategic operational importance identified by a component leader. Each Apex project is codified with a signed charter agreement; the resulting S&T team is mirrored by an equally able, multidisciplinary team from the partner Component.

safety and effectiveness, enabling communications, and providing a common operating picture – result directly from close collaboration with the end users. Reflecting our focus on transition, we have worked to ensure that technologies developed in coordination with S&T are available to first responder communities nationwide; S&T’s technologies are included in the Federal Emergency Management Agency’s (FEMA’s) Authorized Equipment List from which public safety agencies are authorized to purchase with their federal grant dollars. We have also collaborated with private sector companies to commercialize S&T products including multi-band radios, the Controlled Impact Rescue Tool, and the disposable Backboard Cover.

Robust partnerships with R&D collaborators contribute to high return on investment and rapid transition

The S&T strategy to maximize our return on investment and ensure a fast transition to use requires that we capitalize on any existing technology that could be adopted by or adapted to DHS purposes and that we leverage ongoing R&D efforts undertaken by other federal agencies, industry, universities, and by our international partners. This is a challenging task because of the vast and continuously shifting body of R&D unfolding in public and private sectors around the world. We term this initial environmental scan “technology foraging,” and it has already had a large impact on S&T’s ability to deliver a high return on investment.

One example of S&T adapting existing technology to DHS purposes addressed the U.S. Coast Guard’s (USCG) need to track small vessels approaching a seaport. While most large vessels have communication, tracking devices, and identification tagging systems, many small vessels, including those that may be used for illicit activities do not. S&T, in partnership with the National Oceanic and Atmospheric Administration (NOAA) and DHS maritime components, developed software that uses currently deployed coastal NOAA weather radar systems to process the radar signal differently, enabling CBP and USCG to better identify and track small vessels.

Another example pertains to the Transportation Security Administration’s (TSA) screening operations. In this case, S&T combined, adapted, and applied tens of millions of dollars’ worth of basic science from the Defense Advanced Research Projects Agency (DARPA) and universities to the problem of detecting homemade explosives in the aviation environment. These investments in advanced data collection, compressive sensing (a mathematical means of extracting more information from signals such as X-ray diffraction), and in meta-materials for satellite communications were not originally funded by DHS or intended to impact DHS missions. However, S&T has applied these investments in basic research in ways which will result in more effective and less costly walkthrough checkpoint screening technology that dramatically enhances passenger experience as well as the effectiveness and efficiency (via lower false alarm rates, higher throughput, and lower costs of operations) of how TSA screens people, cargo, and luggage.

S&T actively forges partnerships with the private sector through a variety of mechanisms including Broad Agency Announcements, industry days, webinars, and our Small Business Innovation Research Program (SBIR). Since 2004, SBIR awards have produced 31 patents and 42 products on the market. We also have created unique public-private partnerships to share risk and accelerate technology development. For example, S&T initiated the Linking Oil and Gas

Industry to Improve Cybersecurity (LOGIIC) program, a unique public-private partnership that convenes five major oil and gas competitors to work with government on development and distribution of cybersecurity solutions that protect the industry's critical infrastructure. LOGIIC has been highly successful because industry participants partner in project concept development, share project costs, and then adopt solutions while making them available to the entire oil and gas industry. Completed projects to date address security issues in process control systems and application of white-listing technologies (the use of designated safe-to-run software). S&T often collaborates and shares costs with commercial entities on projects including first responder technologies, electric grid resilience, biodefense, and explosives detection among many areas.

S&T has also had a successful working relationship with In-Q-Tel (IQT)⁹ to identify small, innovative start-up companies and invest in them to adapt their emerging commercial technologies. Every S&T dollar invested in IQT projects has leveraged almost \$3 of additional U.S. Government agency funds and more than \$10 of private capital. Thirteen S&T projects in diverse fields are underway with one investment already delivering portable, secure, wireless camera kits to the U.S. Secret Service. Another, which uses DNA markers to rapidly validate familial relationships and confirm identities, is expected to begin field trials with U.S. Citizenship and Immigration Services (USCIS) in FY 2014.

S&T has established robust international collaborations, administered through 13 bilateral agreements, which enable DHS to leverage funds, human capital, and R&D facilities in support of our mission. Our collaboration with international partners also substantively advances S&T's ability to address critical DHS missions. For example, S&T's international work includes collaborations with six international partners on cybersecurity efforts ranging from identity management to network resilience. We have also conducted joint homemade explosives testing with Israel, and we work with the United Kingdom on the detection of liquid explosives in aviation screening and on the development of rapid diagnostics for biodefense. The newest bilateral agreement, with the Netherlands, is already yielding valuable cooperation in areas of mutual benefit such as financial and fraudulent document forensics and cybersecurity.

Partnerships – with both S&T's end users/operators and with other R&D collaborators – are a cornerstone of how S&T does its work and have become the key to maximizing the S&T return on investment. Such collaborations allow S&T to identify high-priority problems and exercise a global reach across the dynamic spectrum of R&D efforts.

Ongoing review of the R&D portfolio ensures alignment with S&T strategy

S&T utilizes an annual portfolio review process to ensure that its projects reflect our emphasis on a high return on investment, high impact, and accelerated transition to use. The portfolio review process, originally developed by Fortune 500 companies and now widely deployed in the private sector and some Department of Defense (DoD) laboratories, uses a panel of experts to evaluate individual projects against specific scoring criteria selected by S&T that reflect our strategic goals and priorities. Evaluators include S&T leadership, outside experts, and

⁹ IQT is the independent strategic investment firm that serves as a bridge between the U.S. Intelligence Community and start-up firms on the leading edge of technological innovation. S&T joined IQT in 2010.

“customers” – senior officials from DHS Components and representatives from the first responder community.

Each project is treated as a discrete investment, and its risks and potential impacts are evaluated against the common scoring criteria. Because all projects are evaluated in a consistent manner, the results can be rolled together to develop an integrated view of the entire portfolio of investments. Essentially, the process provides a method for examining research investments across diverse fields and disciplines using a common language, which helps the organization develop a coherent view of both individual projects and the positioning and likely impact of the overall portfolio. The process is disciplined, repeatable, transparent, strategic, and focused on continuous improvement.

Over the course of three years, we have driven our R&D portfolio towards S&T’s top priority of transitioning useful new technologies to use as rapidly and efficiently as possible. Accomplishing this has meant the culmination of our new philosophy for R&D: reduction of the technical risk by exploiting already or partially developed technologies; getting much closer to customers and involving them directly in project planning, execution, and resourcing; and building a stronger network of R&D collaborators. We have seen tangible results. Since 2010, S&T has raised the percent of projects benefiting from non-S&T funding from 12% to 55%. The percentage of projects deemed likely to transition in the near term has risen from 25% to 49%, and the percentage of investment targeting high-impact, high-feasibility outcomes has increased from 38% to 54%. Some might question why these proportions are not even higher. But research, even late-stage R&D, is always risky. The results of three years of portfolio review have repositioned S&T’s R&D portfolio from “sub-optimal” to “benchmark.”

Beyond R&D: Supporting DHS missions through operational analysis, acquisition support, and other non-traditional contributions

S&T’s value to the Department and the HSE extends beyond technology development. Component support also includes acquisition support, requirements generation, test and evaluation, operational analysis, standards development, and other non-traditional efforts. Collectively, these additional avenues for the thoughtful application of analytical and scientific expertise expand the ways S&T delivers efficiencies and cost savings to the HSE.

Acquisition support: Helping the Department make prudent investments in effective technologies

S&T plays a critical role in overseeing the quality and suitability of DHS acquisitions through the Directorate’s operational test and evaluation (OT&E) activities. By statute and DHS policy, S&T is responsible for establishing T&E policy and procedures for DHS Major Acquisitions¹⁰ and providing independent OT&E oversight and assessment. The Director for Operational Test and Evaluation (DOT&E), serving as the principal T&E advisor to the Secretary and Component heads, ensures that programs that come before the Acquisition Review Board (ARB) have been thoroughly and appropriately vetted via the evaluation of a system’s technical performance, operational effectiveness, and suitability. This is the final step before the Department makes significant investment into production and fielding of acquired systems.

¹⁰ Major Acquisition programs are those with total lifecycle cost estimates exceeding \$1 billion.

To date, S&T has participated in more than 135 ARBs. Careful operational testing can prevent the Department from investing in ineffective technologies. For example, in an ongoing OT&E assessment of the USCG's new Fast Response Cutter, preliminary assessment identified critical reliability deficiencies in the main diesel engine; the manufacturer has since conducted a root cause analysis and completed an engine redesign to meet USCG mission requirements. Early detection of these types of issues can prevent significant and costly repairs and/or delays later in acquisition.

In the initial stages of acquisition, S&T has also helped components translate mission needs into testable requirements that ensure DHS procurements work as expected, deliver on time, and develop within budget. S&T continues to work with the Under Secretary of Management to bolster the "front end" of the Department's acquisition processes and procedures to avoid underperformance and misallocation of resources.

Operational analysis: A method for deploying resources more effectively

Another potentially powerful source of DHS cost savings and added capability comes from operational analytics – assessments of how work is done today and how operations might be adjusted to improve effectiveness, efficiency, and safety. These analyses form the basis for new technology development but can also be used to reconfigure a task. S&T works to make systems-based, operational analysis a key part of every project that we do and to help the DHS components adopt and routinely apply such tools to their work.

Standards development: A high impact method for promulgating technical rigor and consistency

Standards development is a difficult, seldom-noticed process that is critical to establishing technical rigor and consistent, cost-effective performance in technology development. Over the past decade, S&T has worked with the National Institute of Standards and Technology to fund the development of more than 130 technical standards, including 40 standards related to radiation detection recently adopted by DoD. Since 2001, responders have been called to address more than 30,000 suspicious packages involving powders. These incidents are often costly and disruptive; furthermore, the previous lack of uniform collection, processing, and analysis limited the admissibility of the substances as evidence to use against perpetrators. The S&T-led interagency effort to standardize sampling of suspected biothreat powders has bolstered the ability of investigators to locate and prosecute perpetrators of powder attacks and has increased the safety of responders during these incidents.

*Supporting Anti-terrorism by Fostering Effective Technologies (SAFETY) Act program:
Incentivizing industry to adopt anti-terrorism technologies and practices*

At Congress' direction, S&T established and manages the SAFETY Act program. This unique program incentivizes the private sector's development and adoption of anti-terrorism preparedness/resiliency technologies and practices by offering liability protections and litigation management. Since the first application in 2003, the SAFETY Act program has approved more

than 600 applications from a wide range of companies, and in recent years, more than 50% of program applicants are from small businesses.

Over the past decade, the breadth of applications covered by the SAFETY Act has evolved to include sophisticated and layered security systems and practices for major facilities such as sporting venues and airports. S&T has taken special care to implement the program in a balanced, merit-based fashion—and the private sector recognizes its value. Recent feedback from a senior executive of an applicant highlights this notion, “[You] have a top notch program, one that has the necessary rigor to be viewed as truly credible, not just from a government perspective, but from industry as well.” The SAFETY Act lowers risks for the private sector and encourages the adoption of critical technologies and practices that ensure a more resilient and better protected nation.

University-based Centers of Excellence leverage the ingenuity of academia

S&T’s nine university-based Centers of Excellence (COEs) represent consortia of more than 275 colleges and universities in 47 states; each COE assembles leading faculty and graduate students to dedicate their intellect towards significant and diverse homeland security challenges such as border security, explosive threats, and resilience to natural hazards. Partnering with S&T and the components, the COEs pursue a mix of basic and applied research to deliver practical tools and analytic products which increase the effectiveness of components and save money. For instance, a storm surge and flood model developed by the Coastal Hazards Center (CHC) at the University of North Carolina-Chapel Hill now informs USCG and FEMA operational decisions. During Hurricane Irene, CHC’s analysis led the USCG to relocate a Command Center just before its primary location was damaged by the hurricane. During Hurricanes Isaac and Sandy, FEMA, the National Hurricane Center, and state emergency management agencies used the tool to precisely stage resources and accurately anticipate stress on flood control structures.

Another example is an analytical tool developed by the University of Southern California-based National Center for Risk and Economic Analysis of Terrorism Events (CREATE) to help law enforcement deploy assets such as patrols with maximum effectiveness. USCG has adopted this tool for its ports, waterways, and coastal security mission and has deployed the tool in Boston Harbor, Port of New York/New Jersey, and the Ports of Los Angeles and Long Beach. Based on the initial positive results of patrolling higher-priority targets both more frequently and less predictably without additional capital or operating costs, USCG plans to deploy the tool in ports nationwide over the next several years, as well as expand it to other types of port operations. The Federal Air Marshal Service and Los Angeles International Airport (LAX) have also used the tool and experienced similar success, with LAX saving \$500,000 per month in overtime costs after implementing the technology. The COEs have become part of the fabric of DHS; they provide a unique value and are emblematic of how S&T delivers value to the Department in ways that go beyond technology development.

S&T manages laboratories to conduct critical national security work

S&T has five laboratories centered on critical homeland security missions. Each a national asset, the labs fill a unique niche by providing testing, analysis, and novel research that is not found elsewhere in the national laboratory system.

- *National Biodefense Analysis and Countermeasures Center (NBACC)* provides the Nation a 24x7 operational biodefense capability with fully accredited, state-of-the-art laboratories. It conducts experiments, with the capacity to conduct classified experiments, that address fundamental knowledge gaps in biodefense in addition to serving the Federal Bureau of Investigation with testing and analysis on suspected biothreat samples, including analyses of the recent ricin envelopes mailed to public officials. NBACC has contributed to more than 100 federal law enforcement cases.
- *Plum Island Animal Disease Center (PIADC)* has served as the frontline for research on foreign animal diseases that could devastate markets for livestock, meat, milk, and other animal products. Operated in partnership between the Department of Homeland Security and the U.S. Department of Agriculture, it is also the only laboratory in the country that can conduct initial diagnostic testing for foot-and-mouth disease (FMD). PIADC scientists were recently co-inventors with a private company for a patent on the first ever FMD vaccine that can be manufactured in the United States. Unlike other FMD vaccines, this vaccine is the first vaccine that can be safely manufactured on the U.S. homeland. The National Bio- and Agro-Defense Facility (NBAF) – a high containment research laboratory dedicated to protecting the Nation’s one-trillion dollar agricultural sector from emerging zoonoses and agro-terrorism – is slated to replace the aging PIADC and will be an essential facility for national security.
- *Transportation Security Laboratory (TSL)* has provided certification testing of more than 100 explosive detection systems platforms on behalf of TSA and industry utilizing its unique dual ISO 9001 and ISO 17025 accredited operational capabilities.
- *National Urban Security Transportation Laboratory (NUSTL)* directly supports first responders by conducting tests, evaluations, and assessments of technologies and systems—both in the lab and in operational settings. Leveraging its New York City location, NUSTL developed and deployed a radiation sensor network that will provide real-time data to incident managers to guide response decisions following a radiological or nuclear event.
- *Chemical Security Analysis Center (CSAC)* is best known for the development of the Chemical Terrorism Risk Assessment (CTRA), which is a comprehensive evaluation of the risks associated with domestic toxic chemical releases. The CTRA is extensively used by DHS components and many interagency partners as a customizable tool to analyze and prioritize chemical release risks and generate tailored assessments.

Selected Achievements of the S&T Directorate

Attached as an appendix is a brief description of some of S&T’s work for DHS and the HSE. Collectively, these highlight S&T’s contributions through delivery of new capabilities, increases to efficiency and effectiveness, and support to first responders. Additional information on these and other projects can be provided upon request.

Conclusion

Scientific research and technology development are a fundamental means of enabling DHS to “do more with less.” S&T’s work has clearly demonstrated that new technologies, knowledge products, and systems-based operational analysis produced by the Directorate can significantly improve HSE mission effectiveness, operational efficiency, and safety. It is possible to conduct R&D in a manner that drives investments towards clear priorities, aids transparency and accountability, eliminates unwanted project redundancies and fragmentation, and effectively leverages other organizations’ R&D investments.

There are, however, limitations to S&T’s current strategies. Because it is not possible to address all of the highest priority R&D needs across DHS components and first responder communities, the Directorate is, to some degree, opportunistic in its choice of projects. Also, S&T has responsibilities in some areas – notably biosecurity and civilian cybersecurity – which, to meet critical overarching national needs, extend beyond certain requirements of its DHS component customers or the first responder community. S&T has also found it difficult to “transition” successful R&D projects to use by private sector entities, such as those responsible for the bulk of the nation’s critical infrastructure sectors. In the current economic environment, the private sector’s embrace of added security or resiliency is dependent upon approval by corporate boards focused on thin profit margins.

Homeland security missions encompass some challenges that will require long-term R&D investments that are less likely to be made by the private sector. Certain problems in biosecurity, cybersecurity, protection of critical infrastructure, and catastrophic disaster response and recovery will require sustained, strategic, government investments that are beyond the responsibilities of S&T. The Directorate’s current collaboration with the UK Home Office, a mutual effort to develop rapid diagnostic tests that might make a strategic difference in the event of bioattacks, is one example of collaboration among governments and might offer useful insight into how such big problems could be tackled.

Over the past ten years, S&T has been fortunate in its people, whose talent and dedication to the homeland security missions are the essential resource from which all else springs. To be successful, S&T must be a workplace that continues to attract such people. This will require reasonably predictable funding levels, the ability to recruit and retain specialized expertise as needed, and congressional and Departmental support of the S&T mission. It also requires affording the opportunity for S&T professionals to remain engaged with their professional communities and keep abreast of developments in their fields.

Solutions to most of the major challenges in homeland security will require the innovative application of science, technology, and analytics. During the past decade, the Directorate has created an organization with significant and growing ability to help DHS and the HSE achieve their missions more effectively, efficiently, and safely. This progress is due to the hard work of S&T’s people, to our deepening understanding of the complex problems confronting our operational partners and first responders, and to the Directorate’s increasing capacity to identify and make use of innovation from all corners of the globe and all sectors of society. I am honored to lead the DHS S&T Directorate and look forward to your questions.

**APPENDIX A:
Selected Achievements of the S&T Directorate**

New capabilities

Below are brief descriptions of some of the new capabilities that S&T has transitioned or is developing for its DHS and HSE partners. These descriptions are intended for illustrative purposes; additional information on these and other projects can be provided.

Domain Name System Security Extensions (DNSSEC) protocol

- *Problem:* Because of the open architecture of the Internet, it is possible for hackers to redirect users from websites they intend to visit onto a hacker's website where sensitive data such as bank information can be stolen.
- *Solution:* To help counteract malicious hijacking, S&T worked with international partners through the Internet Engineering Task Force (IETF) to develop the DNSSEC protocol, which safeguards the architecture that delivers Internet users to their intended websites.
- *Impact:* More than 30% of the top-level domains (including, .com, .org, .us, and .uk) utilize the protocol, and the Internet Corporation for Assigned Names and Numbers has mandated DNSSEC implementation for all new domain names, which continues to spur adoption of the protocol. S&T continues to advocate wider implementation to safeguard more users of the Internet.

Buried Tripwire

- *Problem:* Certain terrain and foliage-rich environments along the southern border are difficult to monitor with traditional line-of-sight radars and cameras. Above-ground sensors are also vulnerable to attack.
- *Solution:* The Buried Tripwire technology can follow land contours (no blind spots), accurately pinpoint the intrusion right at the entry point, and distinguish between vehicles, humans and wildlife.
- *Impact:* The tripwire data is integrated into the Southern Border CBP Command Center for operational use. It increases monitoring capability, significantly lowers false alarm rates, and costs 1/10 of the current fence design to implement.

Foot-and-Mouth Disease (FMD) vaccine

- *Problem:* A 2001 FMD outbreak in the United Kingdom caused \$8 billion in losses and resulted in the culling of more than 10 million sheep and cattle. Since use of previous vaccines during an outbreak would make vaccinated and infected cattle indistinguishable under current diagnostic tests and result in greater delays to re-opening U.S. export markets, no previous FMD vaccines were usable in the United States, which has a \$1 trillion agriculture industry.
- *Solution:* S&T worked with the Department of Agriculture (USDA) and industry to develop and patent the first successful FMD vaccine in more than 50 years and also the first FMD vaccine licensed for use in the United States.
- *Impact:* The vaccine is now being transitioned to manufacturing with an industry partner. During an FMD outbreak, the vaccine allows vaccinated animals to be distinguished from infected ones and to be placed back into production rather than culled, potentially reducing

the cost of an outbreak by billions of dollars due to millions of vaccinated animals being allowed to live.

TSA security checkpoint of the future

- *Problem:* Due to increasing air travel and evolving threats, there is a need to improve security, throughput, passenger experience, and operational efficiency at airport checkpoints.
- *Solution:* S&T is guiding development of walkthrough detection machines with integrated shoe screeners that will produce better images, process passengers more quickly, and cost a fifth the amount to produce and a quarter the amount to maintain compared to existing screening systems. Screening machines will be responsive to dynamic threat environments, allowing TSA to increase the sensitivity of its machines in real time in response to threats faced. These technologies are being developed by a consortium of industry, university, and government partners, with S&T leveraging \$25M in DARPA-funded basic research on compressive sensing for this project.
- *Impact:* When next-generation machines are delivered and deployed, passenger experience will increase substantially. Passengers will pass through checkpoints more quickly and efficiently and will no longer have to remove their shoes. Detection sensitivity will be increased and false alarms will decrease.

Border Enforcement Analytics Program (BEAP)

- *Problem:* ICE investigators currently use multiple, disparate data sets to generate investigative leads related to export enforcement and counter-proliferation. The size and nature of these data require time- and cost-intensive human processing that would be more effectively handled by computers.
- *Solution:* S&T combines academic and operational knowledge to produce new “big data” solutions, under appropriate privacy and civil liberties controls, that make sense of a large amount of data and significantly augment investigative capability.
- *Impact:* In addition to new capabilities that will open the door to new sources for prosecution, early test results show that ICE will significantly improve the efficiency of investigations. For example, in a preliminary experimental environment, the BEAP system processed 166 million export records and identified 277 potential violations in 16 seconds. BEAP is also paving the way for “big data” solutions that will help other increase capability and save resources with other DHS Components and elsewhere in the HSE.

Resilient Electric Grid (REG)

- *Problem:* Because of limitations inherent to current technology in the electric grid, utilities must separate the grid into isolated subsections. This prevents rolling power failure but, especially in dense urban areas, also prevents power sharing during emergencies, prolongs power outages, and leads to slow restoration efforts with substantial costs.
- *Solution:* S&T partnered with industry to develop superconducting power cable that overcomes previous limitations and allows interconnection of power stations, meaning faster and more efficient restoration of power in emergencies.
- *Impact:* REG is currently in operational demonstration in Yonkers, NY, in collaboration with the Department of Energy and Consolidated Edison. S&T is also exploring a scaled up implementation with NSTAR in Boston, MA, to lower the cable’s production costs and move towards wider implementation.

Increasing efficiency and effectiveness

Below are brief descriptions of some of the ways that S&T is saving money and otherwise increasing the efficiency and effectiveness of its DHS and HSE partners. These descriptions are intended for illustrative purposes; additional information on these and other projects can be provided.

Science and Technology Operational Research and Enhancement (Apex STORE)

- **Problem:** The Secret Service requested support delivering technology to bolster the efficiency and effectiveness of its remote Protective Mission, which includes responsibility for the safety of the President and Vice President, their families, visiting heads of foreign states, and other distinguished foreign visitors.
- **Solution:** In a comprehensive two-year project, S&T delivered ten technologies to the Secret Service. S&T also worked with the U.S. Secret Service to develop a rigorous analysis and acquisition process that can be utilized to help facilitate future procurement and deployment of new technology that can enhance Secret Service capabilities.
- **Impact:** S&T fundamentally shifted how it invests in the Secret Service and supports the deployment of needed capabilities. Secret Service has implemented several of the technologies and is scheduled to take delivery of more in the near future. One example is the Looxcie camera system, which is a lightweight, hand carried, self-contained surveillance system that enables agents to monitor secured spaces more efficiently than through the use of additional manpower alone. Looxcie also costs one third of the existing legacy surveillance system while providing more capability. Another example of the technology procured is the ARMOR system, a lightweight, portable ballistic shielding system. The ARMOR system is lighter and more modular than the legacy system, leading to decreased transportation costs and more rapid deployment in the field.

Standard Unified Modeling, Mapping Integration Toolkit (SUMMIT)

- **Problem:** Conducting disaster response exercises requires large support teams as well as costly and time-consuming production of realistic scenarios, guidebooks, manuals, and decision charts.
- **Solution:** SUMMIT is a software tool that eliminates large support teams and long waits for results through rapid, cost-effective verification and validation of response tactics, plans, and procedures that enables analysts, emergency planners, responders, and decision makers to seamlessly access integrated suites of modeling tools and data sources for planning, exercises, or operational response.
- **Impact:** FEMA adopted this tool and saves \$2 million per National Level Exercise. SUMMIT is available to other federal, state, and local agencies and has been used to support exercises in the Naval Postgraduate School, Los Angeles County Emergency Medical Services, and Utah Department of Public Safety.

Mobile Surveillance System (MSS) upgrade

- **Problem:** CBP uses MSS units to help monitor the borders for illegal entry between Ports of Entry, but existing units have less than optimal sensor performance and agent tools.

- *Solution:* S&T and CBP jointly developed an upgraded unit with better sensor capabilities and updated agent tools and maps. The radar is less expensive but more capable, has a greatly reduced false alarm rate, can operate effectively in inclement weather, and has lower operation costs.
- *Impact:* The upgraded unit has been in operational use on the southwest border since August. Capable of searching a much wider area, it has enabled many apprehensions and outperformed legacy MSS units in diverse environments, including conditions where legacy units would have been inoperable.

Forward Operating Base (FOB) Power Efficiency

- *Problem:* CBP wishes to reduce fuel and fuel trucking costs for its 14 FOBs and reduce the risk of fuel spills on environmentally sensitive roads.
- *Solution:* S&T is working with CBP to field fuel efficient generators and modular solar panel systems which reduce the operating costs for the FOBs.
- *Impact:* A new fuel efficient generator system will be installed at a remote Arizona FOB in FY13 that will save an estimated \$112K annually in diesel fuel and trucking costs. The fuel efficient generator will pay for itself in the first year it is deployed.

Checked Baggage

- *Problem:* False alarms in TSA checked baggage screening require baggage to be fully searched by TSA staff. Each percentage point reduction of false alarm rates improves TSA operational efficiency as well as passenger experience by requiring fewer secondary inspections and moving passengers through faster.
- *Solution:* In collaboration with DARPA and TSA, S&T is developing next generation x-ray systems that incorporate advanced measurement methods from DARPA's Knowledge Enhanced Compressive Measurement program. These systems have the potential to significantly lower the false alarm rate.
- *Impact:* These next generation x-ray systems are anticipated reduce TSA false alarm rates by at least 10% for checked baggage screening operations, which allows DHS to be more efficient and effective by reallocating staffing costs associated with clearing false alarms to other high priority missions.

Vehicle and Cargo Inspection System (VACIS) upgrade

- *Problem:* CBP scans for threat items such as drugs, currency, weapons, etc, at land ports of entry, Border Patrol checkpoints, airports, and other locations. The non-intrusive inspection equipment used for this mission is operating beyond its ten-year lifecycle, and its performance is degrading. CBP lacks funding for new X-ray systems.
- *Solution:* S&T developed an upgrade to existing VACIS equipment that significantly improves image quality without replacing the entire system. This upgrade will cost under \$500K per system, substantially less than a new \$3.5M system and resulting in nearly \$300K savings per year in operation and maintenance.
- *Impact:* In addition to lower operation and maintenance costs, increased non-intrusive inspection capabilities will result in approximately 20% fewer manual inspections of cargo containers each year, an approximately \$30M savings per year for CBP.

Value to first responders

Below are brief descriptions of some of the ways that S&T is fulfilling its statutory responsibility to increase the effectiveness, efficiency, and safety of the more than 60,000 local, state, tribal, and federal first responder agencies. These descriptions are intended for illustrative purposes; additional information on these and other projects can be provided.

Multi-Band Radio (MBR)

- *Problem:* Today's hand-held emergency response radios typically operate on a single band and cannot directly access other frequency bands. This means that most agencies cannot communicate with those outside of their jurisdiction—or even within their own jurisdictions, sometimes—if they operate on different radio bands.
- *Solution:* MBR provides emergency response agencies with the unprecedented capability to communicate on all public safety radio bands.
- *Impact:* S&T's efforts and work directly with industry spurred development of a robust commercial MBR market with competition from multiple vendors leading to more mature MBR products at lower cost to first responders. MBR is now equal in cost, size, and weight to existing high-end portable radios and is commercially available through three manufacturers. To date, MBR have been purchased by state and local responders in Dallas, TX, Phoenix, AZ, and Missouri as well as the U.S. Marine Corps, Department of Interior, and U.S. Capitol Police.

Controlled Impact Rescue Tool (CIRT)

- *Problem:* In some disaster areas, victims may be trapped in collapsed concrete buildings, but existing tools to reach and rescue these victims are time consuming and endanger the lives of trapped persons and operators during the rescue effort.
- *Solution:* S&T partnered with industry to develop a new breaching tool that is less destructive, faster, and more controlled and thus safer to trapped victims.
- *Impact:* CIRT is now commercially available to first responders through Raytheon. The tool breaches reinforced concrete walls 85% faster than alternative technology and at the same time gives first responders greater control and overall safety.

Virtual USA® (vUSA)

- *Problem:* In an emergency, responders must quickly and easily access relevant, reliable, and up-to-date information from multiple partners on power outages, road closures, traffic incidents, hospital and shelter statuses, weather, etc. The proliferation of proprietary emergency response technologies has decreased interoperability among information sharing systems.
- *Solution:* S&T worked with state and local emergency management agencies and other DHS Components to develop vUSA, which improves information sharing and collaboration at all levels of government, allows agencies to build on existing investments and maintain data ownership, and enhances resiliency and disaster response by strengthening partnerships.
- *Impact:* vUSA is part of the White House Open Government Initiative and was used to assist in regional response to the 2010 Deep Water Horizon oil spill, 2011 regional response to Midwest floods, 2012 California wildfires, and the 2013 Presidential Inauguration.

Finding Individuals for Disaster and Emergency Response (FINDER)

- **Problem:** First responders need the ability to rapidly assess whether there are living victims buried in rubble and other debris in the aftermath of a disaster.
- **Solution:** FINDER uses low-power radar to detect breathing and heartbeats of buried victims, even under several feet of rubble and building debris.
- **Impact:** FINDER will increase the efficiency and effectiveness of search and rescue teams by more quickly directing rescuers to where the victims are and greatly increasing victims' chance of survival.

Wildland Firefighter Advanced Personal Protection System

- **Problem:** Wildland firefighters carry significant amounts of equipment and often hike miles in hot, humid conditions to reach fire lines. Traditional gear is heavy and uncomfortable, and wildland firefighters suffer more heat stress injuries than burn injuries.
- **Solution:** S&T leveraged extensive research by the DoD on undergarments for in-theater personnel to develop new firefighting gear (including jacket, shirt, pants, underwear, and socks) that is lighter, more flexible, more breathable, and more effective against radiant heat.
- **Impact:** S&T is working closely with the California Department of Forestry and Fire Protection, California county and local fire agencies, and the U.S. Forest Service and delivered more than 1,000 prototype ensembles currently in pilot tests by Californian wildland firefighters.

Ambulance Patient Compartment Design Standards

- **Problem:** Research has shown that emergency medical services (EMS) personnel experience a fatality rate of 12.7 per 100,000 workers each year—three times the average national occupational rate.
- **Solution:** S&T partnered with the National Institute for Occupational Safety and Health (NIOSH), the National Institute for Standards and Technology (NIST), and representatives from the EMS and manufacturing communities to develop ambulance patient compartment design and safety standards that will safeguard both EMS personnel and ambulance patients.
- **Impact:** Joint S&T, NIOSH, and NIST Ambulance Safety and Design Guide will provide ambulance design manufacturing criteria as part of ambulance purchasing requirements.



United States Government Accountability Office

Testimony
Before the Committee on Homeland
Security and Governmental Affairs,
U.S. Senate

For Release on Delivery
Expected at 9:00 a.m. EDT
Wednesday, July 17, 2013

DEPARTMENT OF HOMELAND SECURITY

Oversight and Coordination of Research and Development Efforts Could Be Strengthened

Statement of Dave C. Maurer, Director
Homeland Security and Justice

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

I am pleased to be here today to discuss our prior work examining the Department of Homeland Security's (DHS) research and development (R&D) efforts. Conducting R&D on technologies for detecting, preventing, and mitigating terrorist threats is vital to enhancing the security of the nation. DHS, through its Science and Technology Directorate (S&T), conducts research, development, testing, and evaluation of new technologies that are intended to strengthen the United States' ability to prevent and respond to nuclear, biological, explosive, and other types of attacks within the United States. S&T also has responsibility for coordinating and integrating all such activities of the department, as provided by the Homeland Security Act of 2002.¹ Although S&T conducts R&D and has responsibility for coordinating R&D, other DHS components, including the Domestic Nuclear Detection Office (DNDO) and the U. S. Coast Guard, conduct R&D in support of their respective missions.

Since it began operations in 2003, DHS, through both S&T and other components, has spent billions of dollars researching and developing technologies used to support a wide range of missions, including securing the border, detecting nuclear devices, and screening airline passengers and baggage for explosives, among others. In June 2009, the National Academy of Public Administration (NAPA) reported on S&T's structure, processes, and the execution of its cross-government leadership role.² NAPA reported that although S&T was charged by statute to provide a leading role in guiding homeland-security related research, S&T has no authority over other federal agencies that conduct homeland-security related research, and that the weaknesses in S&T's strategic planning increased the risk for duplication of efforts. NAPA recommended, among other things, that S&T follow the Office of Management and Budget (OMB) and GAO guidance in formulating a strategic plan to guide its work. In July 2012, S&T provided a draft strategy that identifies the roles

¹Pub. L. No. 107-296, § 302, 116 Stat. 2135, 2163-64 (codified as amended at 6 U.S.C. § 182).

²National Academy of Public Administration, *Department of Homeland Security Science and Technology Directorate: Developing Technology to Protect America* (Washington D.C.: June 2009).

and responsibilities for coordinating homeland security science and technology related functions across the U.S. government to the White House's Office of Science & Technology Policy for review. As of July 2013, the White House had not yet approved that draft.

DHS uses several mechanisms to report R&D spending, including budget authority (the legal authorization to obligate funds), obligations (binding agreements to make a payment for services), and outlays (payments to liquidate obligations representing amount expended). Further, OMB requires agencies to submit data on R&D programs as part of their annual budget submissions on investments for basic research, applied research, development, R&D facilities construction, and major equipment for R&D using OMB's definition of R&D. According to OMB, R&D activities comprise creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture, and society, and the use of this stock of knowledge to devise new applications.³ R&D is further broken down into the categories of basic research, applied research, and development.⁴ DHS is one of nine federal agencies that reported a total of \$5 billion in budget authority in fiscal year 2011 for homeland security R&D.⁵ Moreover, GAO is statutorily required to identify and report annually to Congress on federal programs, agencies, offices, and initiatives that have duplicative goals and

³ OMB Circular No. A-11 Section 84.4. This definition includes administrative expenses for R&D, but excludes physical assets for R&D (such as R&D equipment and facilities), routine testing, quality control mapping, collection of general-purpose statistics, experimental production, routine monitoring and evaluation of an operational program and the training of scientific and technical personnel.

⁴ According to OMB, basic research is a systematic study directed toward a fuller knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind. Applied research is a systematic study to gain knowledge or understanding to determine the means by which a recognized and specific need may be met. Development is a systematic application of knowledge or understanding, directed toward the production of useful materials, devices, and systems or methods, including design, development, and improvement of prototypes and new processes to meet specific requirements. OMB Circular No. A-11 Section 84.

⁵ The other agencies conducting homeland security R&D included the Departments of Agriculture, Commerce, Defense, Energy, and Health and Human Services; the National Aeronautics and Space Administration; the Environmental Protection Agency; and the National Science Foundation.

activities.⁶ The annual reports describe areas in which we found evidence of fragmentation, overlap, or duplication among federal programs.⁷

My statement today is based on our September 2012 report, including selected updates conducted in June 2013 and July 2013 related to DHS's R&D efforts and its oversight of R&D efforts across the department.⁸ Like the report, this statement addresses (1) how much DHS invests in R&D and the extent to which it has policies and guidance for defining R&D and overseeing R&D resources and efforts across the department, and (2) the extent to which R&D is coordinated within DHS to prevent overlap, fragmentation, and unnecessary duplication across the department. For our September 2012 report, among other things, we analyzed data related to DHS's R&D budget authority for fiscal years 2010 through 2013 and R&D contracts issued by components to private industry and universities for fiscal years 2007 through 2011. Further, we analyzed data from the Department of Energy's (DOE) national laboratories from fiscal years 2010 through 2012 to identify how much DHS components obligated for R&D-related work at the national laboratories. For the selected updates, we interviewed agency officials on DHS's progress in implementing our recommendations. More detailed information on the scope and methodology appears in our September 2012 report. We

⁶ Pub. L. No. 111-139, § 21, 124 Stat. 29 (2010), 31 U.S.C. § 712 Note.

⁷ Fragmentation occurs when more than one federal agency (or more than one organization within an agency) is involved in the same broad area of national interest. Overlap occurs when multiple programs have similar goals, engage in similar activities or strategies to achieve those goals, or target similar beneficiaries. Overlap may result from statutory or other limitations beyond the agency's control. Duplication occurs when two or more agencies or programs are engaging in the same activities or providing the same services to the same beneficiaries. GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*, GAO-11-318SP (Washington, D.C.: March 1, 2011). GAO, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue*, GAO-12-342SP (Washington, D.C.: Feb. 28, 2012). GAO, *2013 Annual Report: Actions Needed to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO-13-279SP (Washington, D.C.: April 9, 2013).

⁸ GAO, *Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened*, GAO-12-837 (Washington, D.C.: Sept. 12, 2012). GAO-13-279SP. GAO, *Department of Homeland Security: Opportunities Exist to Strengthen Efficiency and Effectiveness, Achieve Cost Savings, and Improve Management Functions*, GAO-13-547T (Washington, D.C.: April 26, 2013). GAO, *Government Efficiency and Effectiveness: Opportunities to Reduce Fragmentation, Overlap, and Duplication through Enhanced Performance Management and Oversight*, GAO-13-590T (Washington, D.C.: May 22, 2013).

conducted this work 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS Does Not Know Its Total Investment in R&D, and Policies and Guidance Could Help Strengthen Oversight of R&D Efforts

In September 2012, we reported that DHS does not know how much its components invest in R&D, making it difficult to oversee R&D efforts across the department. According to DHS budget officials, S&T, DNDO, and the U.S. Coast Guard are the only components that conduct R&D and we found that they are the only components that report budget authority, obligations, or outlays for R&D activities to OMB as part of the budget process. However, we reported that the data DHS submitted to OMB underreported DHS's R&D obligations because DHS components obligated money for R&D contracts that were not reported to OMB as R&D. Specifically, for fiscal year 2011, we identified an additional \$255 million in R&D obligations by other DHS components. These obligations included DHS components providing S&T with funding to conduct R&D on their behalf and components obligating funds through contracts directly to industry, universities, or with DOE's national laboratories for R&D.

Further, we reported that the data for fiscal years 2010 through 2013 DHS submitted to OMB also underreported DHS's R&D budget authority and outlays because DNDO did not properly report at least \$293 million in R&D budget authority and at least \$282 million in R&D outlays.⁹ We reported that DHS budget officials agreed that DHS underreported its R&D spending and when asked, could not provide a reason why the omission was not flagged by DHS review.

In addition, we reported that DHS's R&D budget accounts include a mix of R&D and non-R&D spending. For fiscal year 2011, we estimated that 78 percent of S&T's Research, Development, Acquisition, & Operations account, 51 percent of DNDO's Research, Development, & Operations account, and 43 percent of the Coast Guard's R&D budget account fund R&D activities. As a result, this further complicates DHS's ability to identify its total investment in R&D.

⁹ At the time of our report, budget figures for fiscal year 2013 were agency estimates.

We also reported in September 2012 that DHS does not have a departmentwide policy defining R&D or guidance directing components how to report R&D activities. As a result, it is difficult to identify the department's total investment in R&D, which limits DHS's ability to oversee components' R&D efforts and align them with agencywide R&D goals and priorities, in accordance with Standards for Internal Control in the Federal Government.¹⁰ DHS officials told us that DHS uses OMB's definition of R&D, but the definition is broad and its application may not be uniform across components, and thus, R&D investments may not always be identified as R&D. We found that the variation in R&D definitions may contribute to the unreliability of the reporting mechanisms for R&D investments in budget development and execution, as discussed above.

Officials at DHS's Program Accountability and Risk Management office, responsible for DHS's overall acquisition governance process, agreed the department had not developed policies or guidance on how components should define and oversee R&D investments and efforts. At the time of our report, they stated that they were in the process of updating Acquisition Management Directive 102-01 to include additional sections pertaining to nonacquisition investments and that such R&D policy and guidance could be incorporated into such updates in the future.¹¹ We recommended that DHS develop and implement policies and guidance for defining and overseeing R&D at the department that includes a well-understood definition of R&D that provides reasonable assurance that reliable accounting and reporting of R&D resources and activities for internal and external use are achieved. DHS agreed with our recommendation stating that it planned to evaluate the most effective path forward to guide uniform treatment of R&D across the department in compliance with OMB rules and was considering a management directive, multi-component steering committee, or new policy guidance to help better oversee and coordinate R&D. DHS planned to complete these

¹⁰ *Standards for Internal Control in the Federal Government* state that policies and mechanisms are needed to enforce management's directives, such as the process of adhering to requirements for budget development and execution and to ensure the reliability of those and other reports for internal and external use. GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

¹¹ Acquisition Management Directive 102-01 defines policy and provides guidance for managing and tracking DHS's acquisition programs,

efforts by May 1, 2013, but as of June 2013, the department had not yet determined which approach it would implement to address our findings and recommendations. We will continue to monitor DHS's efforts to develop its approach for defining and overseeing R&D at the department.

**S&T Coordinates
Some R&D at DHS,
but DHS R&D Is
Fragmented and
Overlapping,
Increasing the Risk of
Unnecessary
Duplication**

**S&T Has Taken Some
Actions to Coordinate
R&D across DHS**

We reported in September 2012 that S&T has developed coordination practices that fall into four general categories: (1) S&T component liaisons, (2) R&D agreements between component heads and S&T, (3) joint R&D strategies between S&T and components, and (4) various R&D coordination teams made up of S&T and component project managers, as discussed below.

S&T component liaisons. In September 2012, we reported that S&T officials stated that one of the primary ways that S&T mitigates the risk of overlap and duplication is through component liaisons staffed at S&T and S&T officials staffed at component agencies. According to S&T officials, these component liaisons have been integral to S&T's coordination efforts. We reported that S&T had eight liaisons from the Transportation Security Administration (TSA), Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), National Protection and Programs Directorate (NPPD), the Secret Service, and the U.S. Coast Guard. In addition, S&T had seven employees detailed to other components, including CBP, the Secret Service, DHS's Office of Policy, DHS's Tactical Communications Program Office, DNDO, and TSA, as well as two liaisons at Federal Emergency Management Agency (FEMA) and DHS's Office of the Chief Financial Officer.

R&D agreements between component heads and S&T. We reported that S&T signed high-level agreements with CBP and the Secret Service to help coordinate activities and address components' strategic operational

problems within 2 years of initiation. S&T also had three memorandums of agreement and 42 technology transition agreements with DHS components as a means to coordinate R&D efforts.

Joint R&D strategies between S&T and components. We reported that S&T and TSA issued a joint R&D strategy for aviation security that identified TSA's R&D priorities based on gaps in TSA's current capabilities. We reported that S&T intended to work with the Secret Service, CBP, ICE, and FEMA to build component-specific R&D strategies linked to component acquisition programs, but we did not receive information on when S&T planned to complete those strategies at the time of our report.

R&D coordination teams. In September 2012, we reported that S&T's previous Under Secretary instituted the Capstone Integrated Product Teams (IPT) process as the primary mechanism for coordinating R&D efforts between S&T and components. Additionally, the IPT process included teams to coordinate R&D at the project level by soliciting input from components to identify and address technology gaps and needs, among other things. We reported that the IPT process was no longer in place to coordinate R&D activities at the component level, but IPTs were being used by the division directors to coordinate R&D activities at the project level. Additionally, we reported that, in the fall of 2011, S&T began implementing two new coordination teams—a cross-functional team composed of S&T personnel focusing on strategic priorities and an integral partner team—led by S&T's newly created Acquisition Support and Operations Analysis division, to focus on components' operational needs. According to S&T division directors, these new teams were not fully implemented at the time of our September 2012 report, and they used established relationships with components through the IPT process to identify components needs and coordinate R&D. In July 2013, we requested information from DHS on when these coordination teams would be fully implemented but did not receive that information.

R&D Activities are Fragmented and Overlapping

Despite S&T's efforts to coordinate R&D activities, in September 2012, we reported that R&D at DHS is inherently fragmented because several components within DHS—S&T, the Coast Guard, and DNDO—were each given R&D responsibilities in law, and other DHS components may pursue and conduct their own R&D efforts as long as those activities are coordinated through S&T. Fragmentation among R&D efforts at DHS may be advantageous if the department determines that it could gain better or faster results by having multiple components engage in R&D activities

toward a similar goal; however, it can be disadvantageous if those activities are uncoordinated or unintentionally overlapping or duplicative. Specifically, we found at least six department components involved in R&D activities in our review of data on about 15,000 federal procurement contract actions coded as R&D taken by DHS components from fiscal years 2007 through 2012. We examined 47 R&D contracts awarded by these components and found 35 instances among 29 contracts in which the contracts overlapped with activities conducted elsewhere in the department. Taken together, these 29 contracts were worth about \$66 million. In one example of the overlap, we found that two DHS components awarded five separate contracts that each addressed detection of the same chemical.

While we did not identify instances of unnecessary duplication among these contracts, DHS has not developed a policy defining who is responsible for coordinating R&D activities at DHS that could help prevent overlap, fragmentation, or unnecessary duplication. We reported in September 2012 that DHS did not have tracking mechanisms or policies to help ensure that overlap is avoided and efforts are better coordinated consistent with Standards for Internal Control in the Federal Government.¹² According to S&T officials, a process does not exist at DHS or within S&T to prevent overlap or unnecessary duplication but that relationships with components mitigate that risk. They also stated that S&T has improved interactions with components over time. We reported that the existence of overlapping R&D activities coupled with the lack of policies and guidance defining R&D and coordination processes is an indication that not all R&D activities at DHS are coordinated to ensure that R&D is not unnecessarily duplicative. Furthermore, we reported in September 2012 that neither DHS nor S&T tracked all ongoing R&D projects across the department, including R&D activities contracted through the national laboratories. As part of our review, we identified 11 components that reimbursed the national laboratories for R&D from fiscal years 2010 through 2012, but S&T's Office of National Laboratories could

¹² GAO's *Standards for Internal Control in the Federal Government* state that policies and procedures ensure that the necessary activities occur at all levels and functions of the organization—not just from top-level leadership. This ensures that all levels of the organization are coordinating effectively and as part of a larger strategy. Additionally, internal control standards provide that agencies should communicate necessary information effectively by ensuring that they are communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals.

not provide us with any information on those activities and told us it did not track them. According to S&T, the Office of National Laboratories' ability to provide information on activities across the department is limited by components inconsistently operating within the defined process for working with the national laboratories.¹³ As a result, we recommended that DHS develop and implement policies and guidance for overseeing R&D that includes a description of the department's process and roles and responsibilities for overseeing and coordinating R&D investments and efforts, and a mechanism to track existing R&D projects and their associated costs across the department. DHS agreed with our recommendation stating that S&T is implementing a collaborative, end-user focused strategy to coordinate and interact with components to better ensure S&T's efforts align with components' needs and that it is considering developing new policy guidance for R&D activities across the department. As of June 2013, DHS has not developed new policy guidance but is conducting portfolio reviews across the department, as directed in committee reports accompanying the fiscal year 2013 DHS appropriation act, aimed at coordinating R&D activities.¹⁴ A policy that defines roles and responsibilities for coordinating R&D and coordination processes, as well as a mechanism that tracks all DHS R&D projects, could better position DHS to mitigate the risk of overlapping and unnecessarily duplicative R&D projects. We will continue to monitor DHS's efforts to develop a policy to better coordinate and track R&D activities at the department.

Chairman Carper, Ranking Member Coburn, and Members of the Committee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

¹³ The Homeland Security Act of 2002 gave DHS the authority to use DOE laboratories to conduct R&D and established S&T's Office of National Laboratories to be responsible for coordinating and using the national laboratories. Pub. L. No. 107-296, § 309, 116 Stat. 2135, 2172 (2002) (codified at 6 U.S.C. § 189). Additionally, DHS Directive 143 further directs ONL to serve as the primary point of contact to recommend contracting activity approval for work by the national laboratories, and review all statements of work issued from DHS and directed to the national laboratories.

¹⁴ See S. Rep. No. 112-169, at 15-16 (2012).

GAO Highlights

Highlights of GAO-13-766T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate.

Why GAO Did This Study

Conducting R&D on technologies for detecting, preventing, and mitigating terrorist threats is vital to enhancing the security of the nation. Since its creation, DHS has spent billions of dollars researching and developing technologies used to support its missions including securing the border, detecting nuclear devices, and screening airline passengers and baggage for explosives, among others. Within DHS, S&T conducts and is responsible for coordinating R&D across the department, but other components, such as the Coast Guard and DNDO, also conduct R&D to support their respective missions.

This statement discusses (1) how much DHS invests in R&D and the extent to which DHS has policies and guidance for defining R&D and overseeing R&D resources and efforts across the department, and (2) the extent to which R&D is coordinated within DHS to prevent overlap, fragmentation, or unnecessary duplication. This statement is based on GAO's September 2012 report on DHS R&D efforts, along with selected updates conducted in June 2013 and July 2013. To conduct the selected updates, GAO interviewed agency officials on the status of implementing GAO's recommendations.

What GAO Recommends

In its September 2012 report, GAO recommended that DHS develop policies and guidance for defining, reporting and coordinating R&D activities across the department; and that DHS establish a mechanism to track R&D projects. DHS concurred with GAO's recommendations and has actions underway to address them.

View GAO-13-766T. For more information, contact Dave Maurer at (202) 512-9627 or maured@ga.gov.

July 17, 2013

DEPARTMENT OF HOMELAND SECURITY

Oversight and Coordination of Research and Development Efforts Could Be Strengthened

What GAO Found

In September 2012, GAO reported that the Department of Homeland Security (DHS) does not know the total amount its components invest in research and development (R&D) and does not have policies and guidance for defining R&D and overseeing R&D resources across the department. According to DHS, its Science & Technology Directorate (S&T), Domestic Nuclear Detection Office (DNDO), and U. S. Coast Guard (Coast Guard) are the only components that conduct R&D, and GAO found that these are the only components that report budget authority, obligations, or outlays for R&D activities to the Office of Management and Budget (OMB) as part of the budget process. However, GAO identified an additional \$255 million in R&D obligations made by other DHS components. According to DHS, it is difficult to identify all R&D investments across the department because DHS does not have a department wide policy defining R&D or guidance directing components how to report all R&D spending and activities. As a result, it is difficult for DHS to oversee components' R&D efforts and align them with agency wide R&D goals and priorities. GAO recommended that DHS develop specific policies and guidance to assist DHS components in better understanding how to report R&D activities, and better position DHS to determine how much the agency invests in R&D to effectively oversee these investments. DHS concurred with the recommendation and reported that it planned to evaluate the most effective path to guide R&D across the department. GAO will continue to monitor DHS's efforts to develop its approach for defining and overseeing R&D at the department.

In September 2012, GAO also reported that S&T has taken some steps to coordinate R&D efforts across DHS, but the department's R&D efforts are fragmented and overlapping, which increases the risk of unnecessary duplication. R&D at DHS is inherently fragmented because S&T, the Coast Guard, and DNDO were each given R&D responsibilities in law, and other DHS components may pursue and conduct their own R&D efforts as long as those activities are coordinated through S&T. S&T uses various mechanisms to coordinate its R&D efforts including component liaisons, component R&D agreements, joint R&D strategies, and integrated R&D product teams composed of S&T and component officials. However, GAO identified 35 instances of overlap among contracts that DHS components awarded for R&D projects. While GAO did not identify instances of unnecessary duplication among these contracts, DHS has not developed a policy defining who is responsible for coordinating R&D and what processes should be used to coordinate it, and does not have mechanisms to track all R&D activities at DHS that could help prevent overlap, fragmentation, or unnecessary duplication. GAO recommended that DHS develop a policy defining the roles and responsibilities for coordinating R&D, and establish a mechanism to track all R&D projects to help DHS mitigate existing fragmentation and overlap, and reduce the risk of unnecessary duplication. DHS concurred with the recommendation and reported that S&T is conducting portfolio reviews across the agency, as required by a fiscal year 2013 appropriation requirement, aimed at coordinating R&D activities. We will continue to monitor DHS's efforts to develop a policy to better coordinate and track R&D activities at the department.

**Post-Hearing Questions for the Record
Submitted to the Honorable Tara J. O'Toole
From Senator Tom Coburn**

**“The Department of Homeland Security at 10 Years: Harnessing Science and
Technology to Protect National Security and Enhance Government Efficiency”
July 17, 2013**

Question#:	1
Topic:	R&D Projects 1
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: What was the total funding obligated by the Department of Homeland Security (DHS) on research and development (R&D) projects coordinated through or funded at least in part by the Science and Technology (S&T) Directorate in FY 2011 and FY 2012 respectively, including funding and in-kind support by DHS components other than the S&T Directorate?

Response: Total R&D project funding coordinated through S&T:

	(\$ in Millions)		
	<u>S&T Funding</u>	<u>Funding from other Components</u>	<u>Non DHS</u>
FY 2011	\$494.3 million	\$46.7 million	\$32.8 million
FY 2012	\$310.3 million	\$29.8 million	\$29.5 million

In addition, S&T receives nonmonetary support from components and partners.
Examples of this support include:

- Lab space for testing and storage
- Physical infrastructure like bridges for onsite vulnerability testing
- Labor resources like FTE officer/screener time to participate in studies/experiments
- Free and unlimited use of special equipment (spectrometers, x-rays, biometric devices, aircraft, routers, servers, vehicles, electron microscopes, threat materials, biological materials)
- Free hosting space for operational testing/piloting (subway stations and tunnels, airports, test beds, ranges)

Question#:	2
Topic:	R&D Projects 2
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide a list of each R&D project in which the S&T Directorate was involved from January 1, 2011, to July 17, 2013, and on which S&T has completed or otherwise discontinued work. For each project, indicate: (a) the approximate dates on which the S&T Directorate's work started and ended on the project; (b) the total cost of the project, broken down by support from S&T Directorate's budget and support (reimbursable, in-kind, or direct) from other components, partners, and customers; (c) why the project was discontinued (for example, transitioned to a component); and (d) the name of each component, customer, or partner to which the S&T Directorate transitioned the project, if any.

Response: Please see the attached spreadsheet on the main workflow.

5/20/11 5:01 PM

5/20/11/3/01

Page 2 of 4

[illegible]

10/31/2015

10/31/2015

Question#:	3
Topic:	R&D Projects 3
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: To better direct funding, the S&T Directorate has implemented an annual portfolio review of the Directorate's funding of on-going R&D projects based on operational focus, innovation, partnerships, and project quality, including likelihood of transition. Has the Directorate implemented a similar process for reviewing projects after transition to the field to evaluate whether the project effectively met a component or first responder need and whether the portfolio review accurately assessed those four attributes? If so, what is that process?

Response: The S&T Portfolio review focuses on the current R&D portfolio and includes metrics related to transition and performance. While there is no current formal review process that takes place after a technology transition, S&T works with the component partners through the entire R&D process. S&T program managers spend time in the field with their partners to better understand the requirement and to ensure that the products that S&T provides fit the operational need of the partner agency to increase the capability to perform the organizational mission. When the product has reached maturity, extensive field testing and piloting are implemented and executed. Once field testing is completed and the project moves through the various stages of the technology development life cycle, such as rapid prototyping, S&T remains a constant partner.

In addition, S&T focuses its efforts to build, update, and improve upon past technology advances. This cyclical development requires constant consultation with components and provides continuous updates on how technology is progressing, how it can be improved, and ultimately defines the next generation of technologies to keep up with current activities. The S&T R&D strategies also provide a mapping tool to link current programs to priority areas. This mapping allows S&T to determine current gaps in components' mission space, and provides direction for future development. The strategies are updated on a yearly cycle to keep up with changing needs and threats.

Question#:	4
Topic:	EMP
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In response to my question about the potential impact of electromagnetic pulse (EMP) events on critical infrastructure (CI), like the electric grid, you told me that “S&T is not doing any work on EMP.” Yet, in September, 2012, Brandon Wales, the Director of the Infrastructure Analysis and Strategy Division of DHS’s National Protection and Programs Directorate, said that “S&T has led much of the Department’s research in the EMP area and is conducting important work through the Recovery Transformer (RecX) Project to increase the resiliency of the EHV transmission power grid, through the use of more mobile and modular transformers.” Moreover, according to documents provided by your office to my staff, the President’s FY 2014 budget proposes \$1 million for a “Solar Storm Mitigation Project,” to enable CI owners to “prepare for geo-magnetically induced currents ... events by developing a forecasting system and mitigations options.” Please explain the inconsistency between your testimony and that of Mr. Wells and the cited documents. What are the statuses of the Solar Storm Mitigation and RecX Projects, their deliverables/transitions, and their respective timetables?

Response: While S&T does not have any active projects that are focused specifically on EMP events, S&T has funded the Recovery Transformer (RecX) Project to increase the resiliency of the extra high voltage (EHV) transmission grid against all possible events, including physical and cyber attacks as well as EMP and solar storms. The RecX is designed to be a more mobile and modular transformer that can be quickly deployed to replace damaged or destroyed transformers, regardless of the cause of the outage. EMP and solar events on the electric grid largely impact the EHV transformers specifically; thus the RecX has applicability as a possible solution deployed by utility companies in such scenarios. The April 16, 2013, rifle attack on PG&E’s Metcalf substation in San Jose, CA, resulted in five damaged EHV transformers and 10,000 gallons of leaked cooling oil. While no power was lost due to this attack, it is a reminder of the additional vulnerabilities that the grid faces.

In March 2012, the RecX was successfully deployed in less than one week in a pilot demonstration that included transporting, installing, and energizing the units in CenterPoint Energy’s grid. The RecX has been in operation in CenterPoint’s grid since the demonstration and has now completed its one-year operational period, successfully marking the completion of the demo. S&T is now working with all stakeholders to determine the best path for transitioning the RecX capabilities to the transmission grid owners and operators.

The Solar Storm Mitigation Project is a “New Start” effort planned for FY 2014 pending FY 2014 appropriation. If funded and initiated, the primary focus of the project would be

Question#:	4
Topic:	EMP
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

on improving the forecasting capabilities of solar storms and their projected impacts on the electric grid. Improved forecasting would allow owners and operators to be able to take proactive operational measures to protect the grid from incoming solar storms with greater confidence and decreased chances of “false alarms.” In the last few years, significant work has been done by industry, spearheaded by the North American Electric Reliability Cooperation (NERC), in understanding the impacts of solar storm events on the grid, and their impacts. Should this project be executed, it will be closely coordinated with the Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), NERC, and other stakeholders.

Question#:	5
Topic:	BioWatch
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In response to a question from Senator McCaskill at the July 17, 2013, hearing, you stated that “S&T has spent no money on BioWatch since [you] took [your] position.” Yet according to a project overview (“quad sheet”) the S&T Directorate provided to my staff, one of the Directorate’s current R&D projects is called “Next Generation Biological Detection,” the first customer for which is listed as “OHA BioWatch.” The quad sheet also indicates that transition products include “autonomous agent detection and rapid characterization methods.” How is this project distinguished from BioWatch Gen-3, or BioWatch generally?

Response: S&T has not funded any costs associated with the operation of BioWatch since it was transitioned to OHA in 2007, and S&T has not funded any of the development or testing costs for Gen-3 since completing its investment in a Gen-3 candidate in 2008. As S&T’s portfolio includes the development of civilian biodefense technologies, the Directorate has continued to fund research and development of more advanced environmental monitoring and biosurveillance technologies. Some of the programs S&T funds could be used to augment or modify BioWatch, but also could be deployed in broader operational settings such as large building or mass transit hubs, outside of the BioWatch program.

As a component of the overall thrust to improve environmental monitoring, the “Next Generation Biological Detection” project within S&T is funding research and technology improvements to support early detection of a biological attack. The efforts within this project include:

1. Sequencing of biological background samples to understand the composition and diversity of the samples to improve capabilities to selectively detect and characterize biological threat agents.
2. Improved sample processing techniques and testing of commercially available laboratory multiplex platforms (capable of analyzing a sample for multiple agents at once) to deliver cost savings and efficiencies within current laboratory processes with greater automation and more reliable results.
3. Analysis of novel detection architectures and data integration across additional environmental monitoring data sources (not just Gen-2 or Gen-3) that can be leveraged for early warning, and provide higher confidence indications that an attack has occurred for faster response actions.

Question#:	5
Topic:	BioWatch
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

This project is working closely with many interagency and state and local partners, including OHA, CDC, and DoD, to develop the requirements for these efforts and transitioning the final knowledge and technology products to the field.

Question#:	6
Topic:	University-based COEs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide a list of all past and current end-to-end (E2E) projects and their respective COEs.

What criteria does the Directorate or Department consider in re-competing COEs or deciding not to continue a COE?

Response: End-to-End (E2E) projects are larger research efforts with particular emphasis on end-user engagement from inception to product use. The goal is to encourage the more rapid transition of academic research from Centers of Excellence (COEs) into practice in DHS components or with first responders. E2Es involve ongoing partnerships between the COEs and DHS components or city, state, or national associations.

E2E is a Science and Technology/Office of University Programs initiative to encourage more focused transition of academic research from COEs to DHS components, other federal agencies, or first responder organizations. An E2E project incorporates a team of people representing all phases of the technology creation-transition-adoption continuum, from early stages of research to use in practice. E2E projects address a homeland security challenge or need; proposed research goals; data collection; analytical approaches; performance metrics; outcomes and outputs; market assessments; potential transition paths; a test and evaluation plans; intellectual property issues; and legal and privacy issues and practical barriers to technology adoption. An E2E project captures the life-cycle of a research effort starting with an idea and ending with a product in the hands of a user.

E2E projects could extend from three to five years and involve developing partnerships between COEs and DHS components; other federal agencies, state, local, tribal and territorial jurisdictions; national associations of first responder organizations; and private companies. An E2E project requires dedication by all parties throughout the project's lifetime, early development of a transition strategy, and commitment by end users to use results and facilitate partnership activities, such as hosting faculty and students. An E2E project involves much more hands-on management, planning, and engagement with outside parties by a COE Director or management team than is common in most academic research.

Question#:	6
Topic:	University-based COEs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

All past and current end-to-end (E2E) projects and their respective COEs:

COE	E2E Project Title & Description	Status
National Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California	ARMOR Technologies The Assistant for Randomized Monitoring Over Routes (ARMOR) technologies (ARMOR, PROTECT, IRIS, GUARDS) are intelligent patrol randomization, resource management, and risk management software.	Transitioned to USCG and FAMS and commercialized; no future OUP funding. Selection of a new CREATE E2E project is not yet finalized.
National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland	“Supporting Countering Violent Extremism (CVE) Efforts through Resources and Training” This E2E is a broad-based effort to put START research to immediate use by maximizing the education impact of existing initiatives, and tailoring START educational programs to meet the needs of the practitioner community.	An extensive market analysis was conducted to determine demand for START’s Graduate Certificate in Terrorism Analysis and/or a self-paced online Continuing Education Unit (CEU). The Global Terrorism Database (GTD) is an example. GTD is a foundational component of START’s education and training mission. GTD training modules have been developed to help practitioners learn how to do basic statistical analysis with GTD data and the tools available in MS Excel. An example of an impact measure is the number of users downloading raw data from the GTD. START keeps statistics on the organizations downloading the data.
National Center for Food Protection and Defense (NCFPD), University of Minnesota	Criticality Spatial Analysis (CRISTAL) CRISTAL is a platform for data collection, documentation, and analysis of food system components, facilities and connections in order to increase the ability of food companies and government to assess risks and respond to threats.	The CRISTAL prototype is in development to collect and document data on food system components and facilities, quantify risks to the food system, and identify links in disparately owned food facilities and systems with the goal to compartmentalize and incorporate multiple users by

Question#:	6
Topic:	University-based COEs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

		improving input interfaces, risk assessment algorithms, and data analysis.
National Center for Zoonotic and Animal Disease Defense (ZADD), Texas A&M University – FAZD	AgCONNECT Business Continuity Tool (BCT) The BCT is part of the <u>AgCONNECT</u> data sharing platform. BCT compartmentalizes proprietary or business-sensitive data from animal agriculture producers, but enables sharing the data in a useful form in an emergency so that decision makers can make more informed, faster decisions regarding quarantine zones and product movement.	In process of developing complex intellectual property agreements, licenses and distribution mechanisms. Note: this project is successful only because a trusted third party – TAMU’s subsidiary TCAT – has access to the data, but will not access or share it except in an emergency. The producers have agreements with the TAMU researchers and technology developers to protect their confidential data. The potential benefit of this system could run into the tens of millions of dollars.
National Center for Border Security and Immigration (NCBSI), University of Arizona – BORDERS	Automated Virtual Agent for Truth Assessments in Real-Time (AVATAR) The AVATAR kiosk is designed to interview low-risk border crossers, e.g., “Trusted Travelers” to reduce labor hours and improving processing time. It is designed to measure any departure from physiological baselines (e.g., eye movement, vocalics, etc.) and enable selection of people subject to secondary screening.	The technologies have gone through development and preliminary validation studies with volunteers. The next steps are a rigorous scientific review of the current state of the technologies and then field tests in operational environments.
Center for Maritime, Island, and Remote and Extreme Environment Security (MIREES) Stevens Institute – Center for Secure	Integrated Maritime Detection Systems CSR is developing and transitioning emerging technologies to support the use of an integrated, layered approach to Maritime Domain Awareness (MDA). The layers	CSR is working towards implementing its layered technology in two sites (NY/NJ harbor and the Caribbean) and demonstrating the portability of its approach by participating in relevant exercises. CSR has

Question#:	6
Topic:	University-based COEs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

and Resilient Maritime Commerce (CSR)	include satellite-based wide area surveillance; High-Frequency (HF) Radar systems providing over-the-horizon surveillance of the approaches; and near-shore and harbor surveillance systems centered on underwater acoustic technologies. Integration of these systems is aimed at achieving surface and underwater vessel detection, classification, and tracking.	licensed part of this system (passive acoustic technology) to a UK firm.
Center for Maritime, Island, and Remote and Extreme Environment Security (MIREES), University of Hawaii – Center for Island, Maritime and Extreme Environment Security (CIMES) and– Arctic Maritime Domain Awareness (MDA) CIMES)	Arctic Maritime Domain Awareness (MDA) Arctic MDA is a suite of tools to improve the ability of first responders (e.g., the U.S. Coast Guard) to (a) navigate ice-rich waters of the Arctic, and (b) provide persistent surveillance and monitoring of the craft transiting the region.	Researchers are attempting to integrate all sensor systems and platforms to create a common operating picture for understanding sea-ice, water, shoreline systems and to promote persistent surveillance for detection of vessel traffic in near-real time.
Center of Excellence for Coastal Hazards (CHC), University of North Carolina	“Identifying and Analyzing the Driving Forces of Hurricane Recovery for Disaster Stricken Areas to Improve Long-term Planning” This project, begun in May 2013, is conducting research to develop a method of measuring coastal recovery trends and processes for use within the National Disaster Recovery Framework (NDRF).	Initiated in May 2013. Still in development.
Center of Excellence for Coastal Hazards (CHC), Jackson	Disaster Response Intelligent System (DRIS) The COE has developed a desktop	Developing transition and commercialization pathways with the aid of the National Institute of

Question#:	6
Topic:	University-based COEs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

State University	decision-support tool that integrates multiple data sources (e.g., live weather and traffic feeds, local infrastructure maps) and analysis tools (e.g., hurricane models, plume models) to help emergency managers' planning, response, and recovery efforts.	Hometown Security in Kentucky. Three pathways are being developed: (1) Low cost tools for local emergency managers, (2) more elaborate tools for private sector users, and (3) research and education tools for universities.
Center for Visualization and Data Analytics (CVADA) Rutgers University and Purdue University	Coastal Operations Analysis Suite of Tools (COAST) COAST is a suite of data analytics, operations analysis, and visualization tools to increase the efficiency of all USCG missions.	In development with USCG participation. Some elements of the COAST suite of tools, including the Coast Guard Search and Rescue Visual Analytics (cgSARVA), have already been validated by the USCG R&D Center.
Center for Awareness and Location of Explosives-Related Threats (ALERT), Northeastern University	Video Anomaly Sensing and Tracking Toolbox (VAST) VAST leverages research at ALERT COE partners who have developed a number of video-based anomaly detection, and tagging and tracking technologies. VAST will enable current TSA video monitoring camera systems to function in a real time vs. current forensic mode.	Phase 1 VAST operational test at Cleveland Airport complete. 100% detection of (airport staff) intruders through exit lanes. Phase 2 is extending technology to track movement of lane violators from camera to camera. A commercial partner is engaged in the VAST project, along with airport, TSA staff, faculty and students.

Criteria for re-competing COEs or deciding not to continue a COE:

As a regular practice for the past several years, DHS S&T's criteria for competing or re-competing a COE in a topical area are:

1. Have DHS components or first responders identified this area as a priority long-term challenge (that university research can help address)? Note: the COEs only conduct research in response to problems or questions developed by DHS or its partners.
2. Is there a genuine research or knowledge gap?
3. Is funding available to support a COE?

Question#:	6
Topic:	University-based COEs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

4. Is research in this area essential to DHS's mission, i.e., is it noted in legislation or otherwise integral to DHS operational agencies or first responders?
5. Is the research area a priority in the Quadrennial Homeland Security Review?
6. Are other Federal agencies supporting research in this topical area? Conversely, if DHS does not pursue this research, will no research be conducted?

Question: What was the basis for the decisions in FY 2012 relating to continuing the START COE as START II and discontinuing the NTSCOE and PACER COEs?

Response: Due to budget constraints, we made the decision to reduce the number of COEs to enable the remaining nine COEs to maintain their research, education, and administrative functions. DHS determined to end the National Transportation Security COE (NTSCOE) and Center for the Study of Preparedness and Catastrophic Event Response (PACER) because the period of performance for each was ending, and there were no contractual commitments past FY 2011.

DHS had not made a commitment to either NTSCOE or PACER that COEs would be re-competed in their topic areas. DHS met its commitment to Congress by funding the NTSCOE for four years (FY 2008 through FY 2011). PACER's area of research was effectively assigned to the Centers for Disease Control at DHHS by the Pandemic and All-Hazards Preparedness Act of 2006 (PAHPA), which created the Preparedness and Emergency Response Research Centers (PERRCs). Funding PACER would have been redundant to the PERRCs.

When the FY 2012 OUP budget was determined, DHS was in the process of a re-competition for a COE for the Study of Terrorism and Behavior (CSTAB). The CSTAB COE funding opportunity announcement closed in December 2010. We competed a COE in this topical area based on first, significant demand for this type of research and analysis from DHS components (11 DHS components and offices participated in writing research questions or topics for the funding announcement), and second, prior commitments from S&T to continue funding in this area. The topics of terrorism and behavior research met all the conditions listed above for establishing a COE.

Question#:	7
Topic:	Acquisitions Support
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In response to my question about the proposed cut to Acquisitions Support in the President's proposed budget for FY 2014, you testified that the "RDA&O[] budget number is misleading," and that "acquisition support ... is not getting cut." Yet, the President's budget for FY 2014 proposes to appropriate \$41.703 million for the Acquisition and Operations Support (AOS) Program Project Activity (PPA) for FY 2014, a 13% reduction from Congress's FY 2013 appropriation of \$47.984 million. Please explain this apparent contradiction.

Response: The proposed reduction to the Science and Technology Directorate's (S&T) Acquisition and Operations Support (AOS) budget does not affect the total funding for programs that support acquisition. The AOS budget includes such items as SAFETY ACT, Homeland Security Studies and Analysis Institute (HSSAI), Standard, Test and Evaluation, International and Interagency and Acquisition and Operations Support. The two budget lines that support acquisition are Test and Evaluation and Acquisition and Operations Support. In FY 2013 these totaled \$9.4M and in FY 2014 the request is for \$11.2M. The reduction affected core funding for HSSAI, SAFETY ACT, International and Interagency and other small programs.

Question: During the hearing, you testified that "the demands [for acquisitions support] exceed [y]our grasp," and you "have to pick and choose what [you] are going to work on." What criteria does the S&T Directorate consider in determining which acquisitions projects it will support? What is the process for that determination and who makes that decision?

Response: S&T, through the Acquisition Support and Operations Analysis Group (ASOA), provides engineering and analytical support to manage the impact of technology on risks and threats; identify technology-based opportunities; support the assessment of programmatic requirements and alternatives; and support the Department's acquisition process, particularly with regard to technology readiness, requirements, capabilities, and operational test and evaluation.

ASOA's analytic workforce to support acquisitions is nominal – 10 subject matter experts – when compared against the needs of the Department. Current DHS demand exceeds ASOA resources; therefore S&T is highly selective in choosing which projects to execute. However ASOA does provide subject matter expertise in an advisory capacity when applicable.

The criteria S&T considers includes:

Question#:	7
Topic:	Acquisitions Support
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

- i. What is the issue? Is it an emerging threat or operationally urgent?
- ii. What is the scope and duration of the project?
- iii. Will the partner be able to provide resources against the project?
- iv. Is this something that must be done in-house, or can S&T help the partner scope the issue and direct it to a Federally Funded Research & Development Center (FFRDC)?

Ultimately, projects are selected after discussion with the Component partner and codified in a memorandum of agreement or charter, signed at the Under Secretary, Deputy Under Secretary or equivalent level.

S&T also plays a critical role in overseeing the quality and suitability of DHS acquisitions through the Director, Operational Test and Evaluation (DOT&E). By Secretary Delegation and DHS policy, S&T DOT&E is a member of the Acquisition Review Board (ARB) and is responsible for establishing T&E policy and procedures for DHS Major Acquisitions and providing independent OT&E oversight and assessment. DHS policies guiding acquisition (i.e., MD-26-06, MD-102) and the DHS Major Acquisition Oversight List (MAOL) dictate which programs are required to adhere to OT&E oversight. Additionally, the DOT&E, serving as the principal T&E advisor to the Secretary and Component heads, ensures that programs that come before the Acquisition Review Board have been thoroughly and appropriately vetted via the evaluation of a system's technical performance, operational effectiveness, and suitability. The FY 2013 Senate report 112-169 that accompanied the Appropriations Bill stated, "The Science and Technology Directorate has established an effective test and evaluation process for DHS major acquisitions."

Question#:	8
Topic:	NBAF
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide a detailed budget and expenditure plan for the proposed NBAF that identifies the individual costs which, in sum, equal the \$1.229 billion planned for obligation in FY 2014.

Response:

	Prior	FY 2012	FY 2013	FY 2014-2020	Total
Fund Source					
Requested Appropriation	153,600	50,000	*	714,000	917,600
Kansas In-Kind Contribution	40,700		40,000	231,300	312,000
Obligations (Planned)					
S&T – Obligation	110,700	13,000	49,900	744,000	917,600
Kansas In-Kind – Obligation	40,700		40,000	231,300	312,000
Expenditures (Planned)					
S&T – Expenditure	81,350	44,300	15,630	776,320	917,600
Kansas In-Kind – Expenditure	32,900	7,800	7,860	263,440	312,000
Total	114,250	52,100	23,490	1,039,760	1,229,600
NBAF Project Expenditures					
Management and Procurement Support	13,200	200	3,000	21,800	38,200
Planning and Studies (including site selection, EIS, risk assessments, Mission Need Assessment)	11,200	3,700			14,900
Technical Services (including pre-design and pre-construction services, cost estimating, title services, site security)	13,650	5,000	2,300	14,300	49,550
Facility Detailed Design	43,300	35,400			78,700

Question#:	8
Topic:	NBAF
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Existing Infrastructure and Utility Improvements	22,400			5200	27,600
Site Preparation	9,200	7,600			16,800
Construction Support Services (including construction administration and materials testing)	1,300	200	1,300	54,630	112,060
Physical Construction-CUP (Construction) – Gift Funds			16,890	63,270	80,160
Physical Construction-Lab Facility (Construction)				871,390	871,390
Commissioning (for both CUP and Lab Facility)				9,170	9,170
Total NBAF Project Expenditures	114,250	52,100	23,490	1,039,760	1,229,600

***S&T did not request funding in FY2013, but received \$30.7M (after sequestration). This amount was not included in this chart. Future years will reflect the increase in appropriations.**

DHS S&T is awarding construction of the NBAF in three separate fixed-price modifications to the construction management services contract. In September 2009, McCarthy Mortenson Joint Venture was awarded a base contract through a competitive process based on its expertise in constructing biocontainment labs. The contract provides options to award future construction tasks for the duration of the NBAF development process as the construction manager.

The first modification, completed in August 2012, was for site preparation activities, such as utility distribution and site grading, to support the initiation of construction activities. This modification was awarded using Kansas gift funds.

The second modification is for the construction of the CUP, which was authorized by Congress in 2011. This modification was awarded in February 2013 using FY 2011 appropriations and matching Kansas gift funds.

The third modification is for construction of the main laboratory facility. Pending FY2014 appropriations, award of this modification is scheduled for May 2014 following the process of negotiating the fixed price with the construction manager as outlined in the contract. This contract modification will be awarded using FY 2014 appropriated funds and Kansas gift funds.

**Post-Hearing Questions for the Record
Submitted to the Honorable Tara J. O'Toole
By Senator Claire McCaskill**

**“The Department of Homeland Security at 10 Years: Harnessing Science and
Technology to Protect National Security and Enhance Government Efficiency”
July 17, 2013**

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Since 2004, the Science and Technology Directorate (S&T) of the Department of Homeland Security (DHS) has received more than \$9.4 billion to gather relevant research and invest in technology requirements for DHS components. In your testimony you stated, “We will now not invest unless the head of that component requests that S&T invest in a particular area.”

Please provide a list of the projects currently funded by DHS S&T, the level of funding, the requesting component, and the written request from the relevant component head.

Response:

The Science and Technology Directorate's Research and Development Work for DHS Components and Others. The projects listed in the table below include projects that support more than one component. Totaling the subtotals for each component will produce a total larger than the S&T's Research and Development (R&D) budget. This illustrates the value of investing in S&T. One project can benefit several components and other Homeland Security Enterprise (HSE) partners.

Customs and Border Protection				Additional in-kind or outside funding
Description	FY 2013	FY 2014	Other DHS Components/ Partners	
<u><i>Agricultural Screening Tools Project</i></u> – This project improves the ability of Federal agencies such as the U.S. Department of Agriculture (USDA) and the Food and Drug Administration (FDA) to screen for and detect high-priority	3,325,000	2,525,000	USDA, FDA	Multiple FTEs (technical and administration) from USDA, estimate of \$1.5M per year. (FY12) “The primary customer

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

foreign animal diseases that threaten the U.S. agricultural critical infrastructure by developing and standardizing protocols and tools.				for these tools is USDA's National Animal Health Laboratory Network (NAHLN). USDA invests per annum over \$1.5 million in the NAHLN and over \$1 million in salaries and program management. While not all of this funding is specifically directed towards the transition of Agricultural Screening Tools, it supports the infrastructure that is used to validate and implement these tools into the animal health network architecture.
<i>Air-Based Technologies Project</i> - This project improves the use of airborne sensors from Unmanned Aircraft Systems (UAS), aerostats, fixed and rotary wing manned aircraft by both CBP and the first responder community for improved detection, identification, and classification of illicit activity and improved situational awareness during emergency events (e.g. floods, forest fires). It also supports the U.S. Coast Guard (USCG).	5,000,000	5,979,890	USCG	"Direct Cert" funding provided to run and oversee a University competition to design and build a quiet UAS.(IARPA, FY12)
<i>Border Spotter Project</i> - This project will provide an ability to detect, locate and disrupt spotters employed by traffickers along the Southwest (SW) Border.		500,000		
<i>The National Center for Border Security and Immigration (NCBSI)</i> - This Center improves the capabilities of CBP, ICE, U.S. Citizenship and Immigration Services (CIS), USCG, and State and local agencies to detect people and goods moving across U.S. borders (legally or illegally), using a fully integrated, system-of-systems approach.	3,429,230	3,075,115	USCIS, ICE	

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

<i><u>Cooperative Biometrics Project</u></i> - This project improves DHS Components' screening and throughput by collecting two or more biometrics in less than 10 seconds at a 95 percent acquisition rate. It is working with Federal partners and the biometrics industry to develop more robust iris recognition and improved fingerprint and facial image acquisition and matching technologies for integration with DHS biometric screening processes.	4,503,000	5,000,000	ICE, NPPD-FPS	
<i><u>Biometric Database Interoperability Project</u></i> - This project enables the cost-efficient and operationally effective matching, analysis, and exchange of biometric and actionable identity-based information between DHS and its mission partners, including DOD, FBI, and other Federal agencies.	1,467,125	1,200,000	ICE, NPPD-OBIM, DOD, FBI	
<i><u>Currency Detection Project</u></i> - This project enables CBP, ICE, and the Transportation Security Administration (TSA) to stem the flow of bulk cash being illegally smuggled out of the U.S. (estimated at over \$6.5 billion/year, largely the proceeds of illegal narcotics activity). The project will develop technology to detect bulk currency at pedestrian border crossings, air passenger facilities, and other places where smuggling of bulk currency occurs. Prototype units will be developed for demonstration and experimentation, then evaluated for potential use by CBP, ICE, and TSA officers.	2,000,000		ICE, TSA	
<i><u>Ground-Based Technologies Project</u></i> - This project will improve CBP's ability to detect illegal incursions along U.S. terrestrial borders by developing advanced sensors and surveillance systems.	4,000,000	4,000,000		* Buried Cable Structured Testing: 1 Dispatcher to evaluate GUI, 2 horses and agent riders, 1 ATV and agent rider, 1 helo and agent pilot; 1 Cessna 182 aircraft and 2 pilots * MSS Engineering Field Test: 1 Eng (OTIA SWFO); 2 agents *Provided engineering

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

				support for the design of the tripwire system connection to the CBP network, consumption of tripwire data into national sensor data base, and distribution of data to SBInet and command center operators. Also provided Field Support and Deployment personnel supporting system connection to CBP network by providing access to necessary facilities and network switching equipment, and by providing interface into CBP network change request administrative processes ** ASU Tower (Deringer)-Water Test : test target assets (24ft SafeBoat; 2 jet skis; 3 agents) Provided engineering support for the design of the testbed sensor and processing equipment connection to the CBP network. Also provided Field Support and Deployment personnel supporting system connection to CBP network by providing access to necessary facilities and network switching equipment, and by providing interface into CBP network change request administrative processes. Provided server room space and environmental

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

				control to host testbed processing equipment. (BP, CBP/OIT, FY12)
<u><i>Maritime Cargo Security Pilot Project</i></u> - This project demonstrates to CBP and partner nations enhanced methods to provide security for maritime cargo in the global supply chain.	1,311,883	1,500,000		
<u><i>Maritime Secure Hybrid Composite Container Build/Pilot Project</i></u> - This project will demonstrate to CBP the capability to secure maritime cargo throughout the global supply chain by using the S&T-developed Secure Hybrid Composite Container with embedded security grid, providing 6-sided tampering monitoring, lighter weight, and longer life (as compared to current steel containers).		1,000,000		Singapore Ministry of Home Affairs is co-funding (\$1.5M) toward development of the Secure Hybrid Composite Container which can detect intrusion to all of its 6 sides. The maritime prototype container is undergoing final testing. Prototype container to be delivered to Singapore in Dec 2013. (FY12)
<u><i>Mobile Biometrics System Project</i></u> - The project improves U.S. border security efficiency and officer safety by providing mobile solutions to Federal, State, and local partners. The objective of this project is to give agents and first responders the ability to identify foreign and domestic threats in the field at the time of interdiction using fingerprints, face, iris, and latent prints at crime scenes.		2,061,000		*USCG Equipment Purchases for DHS S&T Mobile Biometrics Program pilot - USCG In-Kind Acquisition (FY12) *\$1M from USCG and \$225K from FEMA, FY12
<u><i>Multi-Application Multiplex Technology Platform Project</i></u> - This project will provide a robust, specific, and sensitive suite of detection assays that can be used by Federal Laboratories and the private sector by developing a rapidly deployable, easy-to-use, highly multiplexed nucleic acid detection system.	10,030,371	4,000,000		
<u><i>Noncooperative Biometrics Project</i></u> - This project improves DHS Components' ability to identify and prevent potential threats from entering the U.S. and facilitates the movement of legitimate travelers in near real time. This project will test and evaluate state-of-the-art facial recognition systems using video in crowds for various air, rail, and sea port	1,350,000	3,500,000	ICE	

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

scenarios.				
<i>Passive Methods for Precision Behavioral Screening Project</i> - This project improves DHS Components' primary screening and throughput, reduces economic screening impacts, and improves classification accuracy and referral to secondary screening by transforming the screening process from active to more dynamic and passive detection.	375,000	2,200,000	TSA/U.S. Secret Service (USSS)	~\$100k, CIA, FY12
<i>Polymerase Chain Reaction Collection Efficiency Project</i> - This project provides CBP the capability to detect illegal activity through the use of forensic analysis on genetic material collected from suspicious cargo/packages.		1,800,000		
<i>Rapid Response Prototyping Team Project</i> - This project provides rapid evaluation and integration of commercial-off-the-shelf (COTS) and near-COTS technology where there is an identified border security need.	1,000,000	1,000,000		CBP/OTIA provided matching funds (per MOA) to execute project. ~\$1M, FY12
<i>Risk Prediction Project</i> - This project improves CBP's and TSA's capability to identify suspicious behaviors associated with illegally transporting persons and materials prior to their entering the U.S. by deriving, developing, and testing high-speed anomaly-based threat models specific to DHS's air, land, and sea cargo targeting environments.	2,500,000	3,430,000	TSA	
<i>Small Dark Aircraft Project</i> - This project significantly improves CBP's capability to detect, track, and interdict low flying, low observable aircraft (helicopters, ultra-lights, fixed wing) carrying illicit cargo/contraband across the U.S. border.	2,500,000	1,900,000		~\$4.7M To develop and transition technologies to detect and track low-flying aircraft crossing the northern U.S. border. (CBP, FY11) Provided support for short duration testing including 6 agents (total of 2 man months), 3 ground vehicles, helicopter and Cessna aircraft for targetting and

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

				logistics support (CBP/OBP, FY12)
<i>Small Dark Vessels Project</i> - This project improves the ability of DHS components to detect, track, identify, and interdict self-propelled semisubmersible (SPSS) and fully submersible vessels (FSV) transporting illicit cargo into the U.S.	3,000,000	2,000,000	USCG/ ICE/ Navy	In kind support - Dash 8 aircraft, (1) Go Fast boat + (1) CBP agent, (1) diesel vessel, (1) research vessel + (1) DEA special agent (DEA/CBP/ DHS, FY12)
<i>Tunnel Activity Monitoring Project</i> - This project provides CBP the capability to detect and track human activity in public infrastructure storm drains and sewers which are being used increasingly as conduits for smuggling and illegal entry.	1,260,000	1,000,000	ICE	
<i>Tunnel Age Project</i> - This project will develop an accurate and consistent methodology to determine tunnel age for use by CBP and ICE field agents.		1,000,000	ICE	
<i>Tunnel Detection Project</i> - This project will develop technology to enable CBP and ICE to reliably detect tunnels to prevent contraband and illegal immigrant smuggling using clandestine tunnels by using modeling and simulation techniques to predict the effectiveness of the most promising tunnel detection technologies.	1,750,000	2,900,000	ICE	~\$4.8M - CPB/OTIA provided S&T/BMD funds to execute the project already underway. S&T using the funds to extend SME support services via contract and IAA mods. S&T personnel will manage the work (FY12)
<i>Rapid DNA Project</i> - This project enhances the security and integrity of the USCIS immigration system and the CBP Office of Border Patrol by providing a new rapid and low-cost capability to verify family relationships.	2,090,000	2,300,000	CIS	~\$848k from CIA/DIA, FY11
<i>Vehicle and Cargo Inspection System (VACIS) Upgrade Project</i> - This project increases the performance of existing CBP nonintrusive container inspection systems to extend their useful life and increase throughput. These improvements will increase operational efficiency but will not alter current standard operating procedures. This effort will provide a proof-of-concept system and produce	900,000			

Question#:	9
Topic:	S&T
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

prototypes for testing and field evaluation.				
Total CBP	51,791,609	53,871,005		

Question#:	10
Topic:	MTAs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: As we discussed at the hearing, S&T has a statutory obligation to coordinate with other agencies, including the Departments of Defense (DOD) and Health and Human Services (HHS) to assess risks posed by chemical, biological, radiological, and nuclear (CBRN) agents. Specifically, S&T is responsible for development of the Material Threat Assessments (MTAs) and the Terrorism Risk Assessments (TRAs). It is our understanding that MTAs are supposed to be performed for each CBRN or class of agent or every two years.

Can you confirm that MTAs are supposed to be conducted for every two years for each CBRN?

Response: The Terrorism Risk Assessments—Bioterrorism Risk Assessment (BTRA), Chemical Terrorism Risk Assessment (CTRA), and Integrated CBRN Terrorism Risk Assessment (ITRA)—are required under HSPD 10, 22, and 18, respectively, to be conducted and updated every 2 years, which can lead to a Material Threat Assessment (MTA). MTAs are conducted when an agent is deemed to be high risk in one of the Terrorism Risk Assessments. The goal and intent of the MTA is to perform a detailed analysis of an agent's potential for production, storage stability, dissemination potential and efficacy, source strength, viability after dissemination. The MTA also assesses the number of potentially exposed individuals from a plausible, high consequence scenario and the agent's ability to cause infection and impact National Security. These findings are used to support decisions as to whether a Material Threat Determination (MTD) is warranted in support of Project BioShield. If the MTA determines that an agent possess the potential to impact National Security, a recommendation will be made to the Secretary of DHS to issue an MTD in consultation with the Secretary of HHS. This informs the medical countermeasure (MCM) requirements process and is necessary for HHS to use the Project BioShield Special Reserve Fund to procure MCMs.

Question: What is the frequency with which MTAs are currently being conducted for each CBRN?

Response: Following the development of the biennial Terrorism Risk Assessments, the results are examined to determine which agents pose the greatest risk to the Homeland. An MTA takes place for any new agents identified as posing a significant risk or if an agent previously examined in the MTA process has undergone a significant change in

Question#:	10
Topic:	MTAs
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

risk profile, warranting a re-examination of the MTA. MTAs are conducted when new, high risk threats are identified.

Question: What are the dates on which the last two a MTAs were finalized for each CBRN?

Response: The last 2 MTAs were for Volatile Nerve Agents and Cyanide completed in 2007 and Smallpox MTA completed in 2012. Since that time, no new or modified MTAs have been developed. Existing MTAs will continue to be evaluated and new MTAs generated, if appropriate, following the completion of the next iteration of the TRAs to align with HHS's updated MCM requirements process.

Question: For each CBRN, what is the minimum likelihood of an attack above which DHS will recommend that HHS procure countermeasures?

Response: DHS S&T Risk Assessments include both probability (likelihood) and consequences that upon combination lead to the relative risk of any given agent. Prior to 2010, DHS selected those agents that had consequences as their major risk drivers for conducting MTAs. Based on those MTAs, MTDs were issued when a threshold minimum consequence number (10,000 casualties) was surpassed based on modeling studies using a plausible, high consequence scenario. In 2010, DHS began to include the likelihood of certain agents being chosen for use instead of just the consequence numbers, which lead to the issuance of the two chemical MTDs (for Volatile Nerve Agents and Cyanide).

Question: Understanding that HHS is the department responsible for managing the procurement of CBRN countermeasures, are you aware of any ongoing or planned procurements for countermeasures based on risk assessments that have occurred more than two years ago?

Response: We are not aware of any planned procurements for countermeasures based solely on a risk assessment. MTDs were issued for Multi-Drug Resistant MDR Anthrax, Tularemia, Typhus, Glanders, Melioidosis, Viral Hemorrhagic Fever and Plague in 2006 based on the BTRA to facilitate Project BioShield procurement decisions. It is our understanding that there are ongoing efforts at HHS to address the need for countermeasures for all of these agents.

Question#:	11
Topic:	countermeasures
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony you stated that you serve on the Department of Health and Human Services' Executive Steering Committee, which reviews decisions on the procurement of biological countermeasures. You also stated that you raised concerns over the specific countermeasures proposed to combat an anthrax attack.

What was the nature of the concerns you raised regarding the proposed countermeasures for antibiotic resistant anthrax strains?

Please provide any written recommendations from you or S&T to the Executive Steering Committee, and please describe the nature of the steps taken by HHS in response to those recommendations.

Response: The decisions required of the Executive Steering Committee (ESC) regarding how HHS should invest its limited appropriations in the development and procurement of medical countermeasures against the potential array of CBRN threats are exceedingly complex.

It is widely agreed among biodefense experts that a bioterror attack using aerosolized anthrax poses a significant risk to the United States. This judgment is based on biological threat assessments which evaluate the likelihood of adversaries successfully obtaining, weaponizing and disseminating the organism and the probable consequences of such attacks – which include plausible scenarios of tens to hundreds of thousands of civilian casualties. Moreover, several nations have successfully demonstrated the weaponization of anthrax, and intelligence showed that Al Qaeda and other adversaries were interested in and actively pursued an anthrax weapon for use against the United States.

Several antibiotics are thought to be effective against exposure to aerosolized anthrax if they are administered within a short timeframe (i.e., 24 to 48 hours) after initial exposure. After this period, the bacteria have produced a lethal toxin in such quantities that antibiotics alone are not effective to cure the patient. The practical impediments to rapidly identifying that an attack has occurred and then efficiently distributing antibiotics to all the potentially exposed victims are daunting. For those victims who develop full-blown anthrax, an antitoxin product such as those developed by GSK/Human Genome Sciences Inc. and other companies might be the only possible lifesaving treatment. These products, which are useful solely in an anthrax attack, and thus of interest only to government, are expensive to develop and purchase. It should be noted that all

Question#:	11
Topic:	countermeasures
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

“biological products” are extremely expensive to develop and hence command high market prices. The antitoxin in question is not out of line with typical costs of these products, all of which expire after a shelf life of several years.

My questions during the ESC in question were not written down but pertained to the concept of use behind such products, which were to be purchased in quantities that would likely be much smaller than the number of people who might benefit from the antitoxin should an attack, or several attacks, occur. The amount of antitoxin that would be required under the most extreme credible scenario is about 3.6 times the current level of product that has been purchased and is in the stockpile. However, that current stockpiled amount is adequate to treat all individuals needing antitoxin in over 90% of all modeled scenarios. As I recall, I raised the question on what basis the government would decide who should receive these potentially lifesaving but scarce resources. These issues were being addressed at the working group level; recently, the Public Health Emergency Medical Countermeasures Enterprise issued a Clinical Guidance document that identifies for clinicians the conditions under which a patient who is diagnosed as infected with anthrax should be treated with antitoxin.

Question#:	12
Topic:	TRA and MTA 1
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: What role, if any, do non-governmental-employees play in the process of creating recommendations for the TRA and MTA?

Response: DHS, in coordination and consultation with federal interagency partners, creates recommendations for the development and execution of the TRAs and MTAs. During this process, contractor staff provides technical support to federal employees to maximize the scientific defensibility and utility of the modeling efforts. Under the direct supervision of federal program management staff, contractors perform primary execution of the modeling used to support the TRAs and MTAs. All decisions regarding finalization and dissemination for the TRA and MTA products are made by federal program management staff.

Question: Are any non-governmental employees involved in the TRA and MTA process employed by, on the board of, or do they otherwise have a financial interest in, government contractors?

Response: DHS relies on contractors for technical support in developing the TRA and MTA products. As such, by definition, they are employed by contractor organizations. In the listing of contractors with a direct role in the development of the TRAs and MTAs, the primary and any other known secondary contractor affiliations are noted. For those individuals identified as sub-contractors, it is the responsibility of the primary contractor as a DHS FFRDC to ensure any conflicts of interest, including financial interests in companies that may directly or indirectly benefit from the information shared during the course of the government-sub-contractor relationship, is protected through strict enforcement of contractor issued non-disclosure agreements.

Question: If so, please provide their names, the names of the contractor with which they have an affiliation and the relationship to that contractor.

Response:

Name	Contractor	Relationship	Program	Other contractor affiliations
Dr. Debra Anderson	Booz Allen Hamilton	Employee	Integrated Terrorism Risk Assessment (ITRA)	None
Mr. Stuart Evenhaugen	Booz Allen Hamilton	Employee	ITRA	None

Question#:	12
Topic:	TRA and MTA 1
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Dr. Rocco Casagrande	Gryphon Scientific	Employee	ITRA and Bio-Terrorism Risk Assessment (BTRA)	None
Dr. Anna Kushnir	Gryphon Scientific	Employee	ITRA and BTRA	None
Mr. Ian Whittaker	Battelle Memorial Institute	Employee	ITRA	None
Dr. Eric Tollar	Battelle Memorial Institute	Employee	ITRA and Radiological and Nuclear Terrorism Risk Assessment (RNTRA)	None
Dr. Jason Middleton	Battelle Memorial Institute	Employee	ITRA and BTRA	None
Dr. Don Stoeckel	Battelle Memorial Institute	Employee	ITRA and BTRA	None
Dr. Rachel Gooding	Battelle Memorial Institute	Employee	Chemical Terrorism Risk Assessment (CTRA)	None
Dr. Mark Whitmire	Noblis	Employee	CTRA	None
Dr. Brian Hawkins	Battelle Memorial Institute	Employee	CTRA	None
Mr. Steven Streetman	Data Architecture Solutions	Owner	RNTRA	None
Dr. Tom Bates	Lawrence Livermore National Labs	Employee	Material Threat Assessment (MTA)	None
Dr. Jason Perry	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Michael Dillion	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Danielle Poulin-Porter	Lawrence Livermore National Labs (formerly)	Employee	MTA	None
Dr. Larry Dugan	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Erik Burnett	Lawrence Livermore National Labs (formerly)	Employee	MTA	None
Dr. Brian Souza	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Doug Deder	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Michelle Alegria-Hartmann	Lawrence Livermore National Labs (formerly)	Employee	MTA	None
Dr. Dayle Daines	Lawrence Livermore National Labs (formerly)	Employee	MTA	None
Dr. Susan Allen	Lawrence Livermore	Employee	MTA	None

Question#:	12
Topic:	TRA and MTA 1
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

	National Labs			
Dr. Gayle Sugiyama	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Rich Sextro	Lawrence Berkeley National Labs	Employee	MTA	None
Dr. David Brown	Argonne National Labs	Employee	MTA	None
Dr. Woody Delp	Lawrence Berkeley National Labs	Employee	MTA	None
Dr. Jason Ellis	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Anthony Policastro	Lawrence Livermore National Labs	Employee	MTA	None
Dr. Fred Leykam	Washington Institute	Employee	MTA	None
Dr. Todd West	Sandia National Labs	Employee	MTA	None
Dr. Jo Velardo	Homeland Security Studies and Analysis Institute (HSSAI) - DHS FFRDC	Employee	BTRA	None
Mr. Mark Weitekamp	HSSAI	Employee	BTRA	None
Dr. Richard Danzig	Sub-contractor to HSSAI	Independent Consultant	BTRA	None
Dr. John Vitko	Sub-contractor to HSSAI	Independent Consultant	BTRA	None
Dr. Tom Inglesby	Sub-contractor to HSSAI	Independent Consultant	BTRA	Center for Health Security
Dr. Dave Franz	Sub-contractor to HSSAI	Independent Consultant	BTRA	None

Question#:	13
Topic:	TRA and MTA 2
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony you stated that Richard Danzig is currently being retained as a contractor with the Department of Homeland Security.

What is the nature and purpose of the contract?

Response: The contract is with Homeland Security Studies and Analysis Institute (HSSAI), a DHS FFRDC, to conduct Bio Net Assessments (BNA). The BNAs are mandated in HSPD-10, "Biodefense for the 21st Century" which identifies four pillars of national biodefense: threat awareness; prevention and protection; surveillance and detection; response and recovery. HSPD-10 tasked DHS with conducting the BNAs to provide a senior-level policy net assessment to evaluate the progress in implementing HSPD-10, identify continuing gaps or vulnerabilities in our biodefense posture, and make recommendations for re-balancing and refining investments among the pillars of our overall biodefense policy. Since inception in 2004, the BNA has completed 19 assessments evaluating both the specific progress in biodefense activities and identifying gaps in preparedness activities.

Question: What role, if any, does he play in the process of creating recommendations for the TRAs and MTAs?

Response: The BNA panel, on which Dr. Danzig participates, is currently conducting a study to evaluate the methodological approach taken by the Bioterrorism Risk Assessment (BTRA) program. The goal of the study is to examine if the probabilistic risk assessment (PRA) method of analyzing risk is 1) appropriate for bioterrorism and 2) if additional/orthogonal methodologies could enhance stakeholder utility of the BTRA products. Dr. Danzig is one of several BNA panel members contributing to the study discussion. He has not had a role in creating recommendations in either document since prior to 2006 when he disclosed his relationship with Human Genome Sciences Corporation. The Department of Health and Human Services is responsible for conducting the public health analysis that determines the need and desired quantity of any medical countermeasures.

Question: Please provide a copy of the contract as well as a description of Mr. Danzig's specific role in executing the requirements of the contract.

Question#:	13
Topic:	TRA and MTA 2
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Response: Dr. Danzig's contract with HSSAI is attached. Included in the contract language is a description of Dr. Danzig's specific roles and responsibilities in executing the requirements of the contract. His Statement of Work is as follows: As requested Dr. Danzig will provide subject matter expertise associated with the fields of bio-defense policy and public health. This subject matter expertise will be in the form of analysis and feedback.


ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.


**HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE
CONSULTANT AGREEMENT**
RICHARD DANZIG
No. C-09-078-DANZ

This Consultant Agreement ("Agreement") is made and entered into this 14th day of May 2009 by and between Analytic Services Inc., operating as the Homeland Security Studies and Analysis Institute ("HSSAI"), a California corporation, having an address at 2900 South Quincy Street, Suite 800, Arlington, VA 22206-2233 and Richard Danzig, ("Consultant") having a place of business at 3670 Upton Street NW, Washington, DC 20008.

HS SAI conducts various programs of study and research under contract with the Government and its prime contractors; HS SAI desires to obtain Consultant's specialized skills to aid HS SAI in the performance of this undertaking. In consideration of the mutual obligations specified in this Agreement, and any compensation paid to Consultant for its services, the parties agree to the following:

1. Definitions

"Firm Fixed Price (FFP)" means one price will be paid for completion of a statement of work or similar document.

"Services" means, as the context requires, the services to be performed by Consultant hereunder.

"Consultant" means the individual specified above.

"Task Order(s)" means that document issued with reference to this Agreement which describes the Services to be provided by the Consultant when specifically ordered by HS SAI.

"Time and Materials (T&M)" means the time Subcontractor spends in actual performance of a statement of work or similar document shall be paid for at a rate per hour (or per day), as defined in a Task Order, plus the actual cost of other items used or incurred in the actual performance of the statement of work.

"Work Product" means, as the context requires, any software, ideas, concepts, techniques, inventions, processes works of authorship and/or other intellectual property developed or created by Consultant during the course of performing the Services and embodied, in whole or in part, in Consultant's deliverable(s) to HS SAI or to an HS SAI client.

2. Compensation and Payment

a. HS SAI agrees to pay Consultant for performance of Services in accordance with the Task Orders issued under this Agreement. A labor rate, applicable to all Task Orders unless otherwise stated in the Task Order, is specified in Exhibit B, attached hereto. If an hourly rate is specified, Consultant's time shall be computed to the nearest one-quarter of an hour; and, if a daily rate is specified, a day shall consist of not less than eight nor more than twelve hours of work. If an estimated cost for a T&M rate agreement is specified on a Task Order, Consultant shall not exceed the estimated cost without prior written approval of the HS SAI Contract or Subcontract Representative. Further, HS SAI will not pay Consultant in excess of the estimated cost of a Task Order without prior written approval.

b. Consultant shall invoice HS SAI based on work actually performed under a Task Order either (i) within seven working days after the end of each calendar month during which work was performed; or (ii) when compensation is due and payable in accordance with a specific Task Order. One invoice shall be submitted for each Task Order under which work was performed the preceding calendar month. Each invoice shall specify, at a minimum, the Agreement number, Task Order number, unique invoice number, date of invoice, HS SAI Project Number, (if known and applicable and the address to which payment shall be submitted. If a Task Order is performed on a T&M basis, the invoice shall also specify the hourly or daily rate, the hours or days actually worked, any other direct costs incurred and



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



payable under the terms hereof (including supporting receipts for expenses claimed) and other relevant information. If HS SAI Project Numbers are noted on the Task Order, Consultant shall provide a breakdown of its costs on the basis of the project numbers. Invoices for T&M Task Orders shall also include cumulative totals in amounts and hours per labor category (if applicable). Invoices shall be signed and certified that the amounts claimed for the period of performance stated on the invoice are true and accurate for the period claimed. HS SAI reserves the right to reject any and all invoices which lack any of the above stated information.

c. Provided Consultant's invoice and supporting documentation are acceptable and approved, payment of Consultant's invoice will be made by HS SAI thirty (30) days from the date of receipt of the invoice. If the invoice and supporting documentation are not approved, HS SAI will make payment thirty (30) days after receipt of a revised invoice that is acceptable. The Consultant will submit its invoices to HS SAI as follows:

Analytic Services Inc.
2900 South Quincey, Suite 808
Attn: Accts. Payable Department
Arlington, Virginia 22206

OR

Email to: accounts payable@aniser.org

E-mail is the preferred method for invoice submission, and, if sent by e-mail, Consultant shall receive an automated confirmation of receipt.

d. Consultant's principal place of business for purposes of this Agreement shall be shown on Exhibit B. If authorized in advance of expenditure, Consultant will be reimbursed for all reasonable and necessary expenses incurred in the course of business for travel outside of the greater metropolitan area of Consultant's principal place of business. Greater metropolitan area shall mean at a radius of more than 50 miles from Consultant's place of business. Consultant is not entitled to any advances for travel expenses. Consultant shall not be reimbursed for any mileage, parking fees, meals and similar expenses for travel within a 50 mile radius of Consultant's principal place of business, unless such reimbursement has been specified in a Task Order.

(1) Consultant shall obtain air travel at the least expensive rate available consistent with meeting

the travel requirements of providing the Services in a reasonable timeframe. Unless otherwise authorized, meal, hotel and private automobile expenses shall not exceed the amounts specified on Exhibit B.

(2) Consultant shall complete a travel expense report form, either provided by HS SAI or approved by HS SAI, and shall provide supporting receipts for all travel-related expenditures. Such expense reports shall be submitted to HS SAI along with Consultant's monthly invoice.

(3) Time spent in travel shall not be considered time actually worked; no payment of any kind shall be made for Consultant's hours spent in travel.

e. Nothing herein shall be deemed to constitute a waiver of HS SAI's right to dispute and refuse to pay, in whole or in part, claims for compensation or reimbursable expenses if Consultant has materially misrepresented his or her capacity to perform an accepted assignment, failed to substantially accomplish satisfactorily the results specified, or otherwise materially breached any provision of this Agreement.

3. Term

This Agreement will become effective on the date first set forth above and shall continue in twelve (12) month increments unless written notice is provided by either party sixty (60) days prior to the end of the then-current twelve (12) month period, or until terminated in accordance with the "Termination" clause. The term of each Task Order will be stated in the Task Order and such term shall run independently of the term of this Agreement.

4. Services

Consultant agrees to provide the type of Services set forth in Exhibit A as and when specifically ordered under Task Orders referencing this Agreement. HS SAI may, at any time, increase or decrease the scope of the Services and/or Work Product specifically ordered under a Task Order, provided that any change requiring additional services shall be subject to the parties' mutual agreement regarding Consultant's compensation in connection therewith. Any such agreement regarding additional compensation shall be set forth in a signed, written amendment to the relevant Task Order; without such an amendment to the Task Order, Consultant shall not be obligated to perform the Services or provide the Work Product and HS SAI shall not be obligated



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



to pay for such additional Services and/or Work Product.

5. Task Orders

As stated under the clause entitled "Services," all work under this Agreement shall be ordered by Task Orders. An example of a Task Order form may be found in Exhibit C, but the actual Task Order form issued may be somewhat different in form and content. Each Task Order shall be bilaterally executed and shall state, at a minimum, the following information:

- a. the type of contractual arrangement for the individual Task Order—e.g., FFP, T&M etc.;
- b. the Statement of Work for the Task Order;
- c. the Period of Performance for the Task Order;
- d. the hourly rate if T&M for the work to be performed;
- e. the total price(s) if FFP, or, the total estimated cost if T&M;
- f. the payment schedule, applicable to FFP arrangements, for the work to be performed;
- g. security requirements applicable to the Task Order, if any;
- h. that the Task Order is issued under the terms of this Agreement; and
- i. any special terms and conditions for the Task Order, including the incorporation of HS SAI's client terms and conditions, if applicable.

Each Task Order shall be treated as a part of this Agreement and the terms and conditions of this Agreement shall be a part of each Task Order, but each Task Order shall be severable and segregable from this Agreement with respect to the term of the Task Order, the price or estimated cost, any special payment terms, the Statement of Work, any additional Special Terms and Conditions and any other similar terms which would clearly be applicable only to the specific Task Order in which those terms appear. If this Agreement is terminated in accordance with the "Termination" clause or the "Term" clause, this Agreement shall not be considered terminated in its entirety until the end of the period of performance of each and every Task Order which was not specifically terminated by the termination notice.

6. Method of Performance and Supervision

Consultant will generally determine the method, details and means of performing the Services. HS SAI shall not have the right to control the exact

manner or determine the precise method of accomplishing the Services; however, HS SAI shall be entitled to exercise a broad, general right of supervision and control over the results of the Services performed to ensure satisfactory performance. This power of supervision shall include the right to inspect, stop work, make suggestions or recommendations as to the details of the work, and request modifications to the scope of the Services.

7. Scheduling and Reporting

HS SAI will advise Consultant of the HS SAI employee(s) to whom Consultant will report its progress on such Services. Requirements for written reports, if any, shall be specified in the individual Task Orders.

8. Place of Work

Consultant will perform the Services at the site designated on the individual Task Order. Services may be performed at HS SAI's client's site. HS SAI agrees to arrange for working space and appropriate facilities at HS SAI's client's site on behalf of Consultant unless other arrangements have been agreed upon specifically between HS SAI and the Consultant.

9. Right to Reject

HS SAI reserves the right, in its sole reasonable discretion, to reject the Services of the Consultant and Consultant agrees that he/she shall immediately cease any work under this Agreement and leave HS SAI or HS SAI's client's facilities. Reasons for rejection may include, but are not limited to, poor performance, threatening behavior, public intoxication, drug addiction and similar behaviors which might impair the timely and professional provision of Services under this Agreement.

10. Compliance with Laws

Consultant agrees to comply with all applicable Federal, State, and local laws or ordinances, rules, regulations and orders in the performance of this Agreement.

11. Withholding of Payments

Notwithstanding any other provisions of this Agreement, failure of the Consultant to submit required reports when due, or failure to perform or deliver required work, supplies, or services, will result in the withholding of payments under this Agreement unless such failure arises out of causes



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



beyond the control and without the fault or negligence of the Consultant.

12. Non-Exclusive Relationship

This Agreement is non-exclusive. Consultant shall retain the right to perform work for other parties during the term of this Agreement, and HS SAI may have work of the same or a similar kind performed by its own personnel or other contractors or Consultants during the term of this Agreement.

13. Conflict of Interest

a. Consultant will report to HS SAI during the term of this Agreement about any and all contracts, agreements, understandings, prior employment or prior relationships applicable to Consultant, which may prohibit, restrict or limit Consultant's performance of this Agreement.

b. When requested by HS SAI, Consultant shall file with HS SAI a Statement of Affiliations in order to identify and evaluate potential organizational conflicts of interest between Consultant's services and HS SAI's, which could result in an unfair competitive advantage. Consultant will comply with HS SAI's determinations with respect to such matters.

c. Terms and conditions related to Organizational Conflicts of Interest, if any, may be found in Exhibit D.

14. Independent Contractor Status

The parties hereto acknowledge and agree that Consultant is an independent contractor to HS SAI and not an employee, agent, joint venturer or partner of HS SAI. Consultant further acknowledges and agrees that, as an independent contractor, Consultant will not be entitled to (1) make a claim for unemployment, worker's compensation or disability pursuant to this Agreement or Consultant's relationship with HS SAI, or (2) receive any vacation, health, retirement or other benefits pursuant to this Agreement or Consultant's relationship with HS SAI. HS SAI will not (a) withhold FICA from its payments to Consultant, (b) make state or federal unemployment insurance contributions on behalf of Consultant, or (c) withhold state and federal income taxes from its payments to Consultant. Consultant hereby represents and warrants to HS SAI that, except as otherwise expressly provided herein, all activities and work performed by Consultant under this Agreement shall be at Consultant's own risk and

liability. Consultant's taxpayer identification number is set forth on Exhibit B.

15. Intellectual Property

a. HS SAI owns all rights, title and interest in all Work Products provided by Consultant under this Agreement, including but not limited to all copyrights, trade secrets and other forms of intellectual property rights, and all Work Products shall be deemed "works made for hire." To the extent that any such Work Product may not be considered a "work made for hire" under applicable law, Consultant hereby grants, transfers, assigns and conveys to HS SAI and HS SAI's clients a non-exclusive, paid-up, worldwide, perpetual license to 1) use, execute, reproduce, display, perform, distribute (internally and externally) copies of, and prepare derivative works based upon, such Work Product and derivative works thereof, and 2) authorize others to do any, some or all of the foregoing, such that HS SAI and HS SAI's clients may use and copy the Work Product and/or create derivative works from the Work Product unencumbered in any fashion by claims from the Consultant or a third party of the Consultant's and/or a third party's rights, title or interest in the Work Product or its underlying intellectual property.

b. Consultant shall be free to use and employ its general skills, know-how and expertise, and to use, disclose and employ any generalized ideas, concepts, inventions, manuals, software, data files, know-how, methods, techniques or skills gained or learned during the course of the performance of any Services, so long as Consultant acquires and applies such information without the disclosure of any Proprietary Information and without any unauthorized use or disclosure of any Work Product. All ideas, concepts, inventions, manuals, software, data files, know-how, methods, techniques, skills and other intellectual property that Consultant has developed, created or acquired outside of performing the Services under this Agreement are and shall remain the sole and exclusive proprietary property of Consultant, except to the extent that rights are granted to HS SAI and HS SAI's clients as described in this clause.

16. Publication/Dissemination

No information that Consultant develops in connection with the Services hereunder shall be published or disclosed at any time in any writing, thesis, lecture, and the like without obtaining the prior written approval of HS SAI for the publication and/or release of the manuscript or material. Such



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



approval will not be unreasonably withheld but may require the approval of the Government. If Government approval is required, HSSAI and Subcontractor shall abide by the Government's decision regarding publication or release.

17. Warranties

Consultant warrants that: (1) any and all representations made in resumes and other written or oral presentations to HS SAI relating to Consultant's education, training, skills, work experience and similar matters are true and accurate; (2) all Services will be performed by Consultant utilizing the standards of care normally and customarily exercised by a professional performing comparable services under similar conditions; (3) Consultant has all requisite right and authority to enter into this Agreement with HS SAI and that by doing so Consultant will not create any conflict of interest of any type, and should such conflict of interest later arise, shall provide HS SAI with immediate notice of any such conflict of interest; (4) Consultant has no knowledge of any claims that would adversely affect Consultant's ability to assign all right, title and interest in and to the Work Product to HS SAI; (5) the Work Product does not violate any patent, copyright or other proprietary right of any third party; and (6) Consultant has the legal right to grant HS SAI the assignment of Consultant's interest in the Work Product as set forth in this Agreement.

18. Insurance

a. Consultant shall obtain and maintain in full force and effect during the term of this Agreement (1) commercial general liability insurance (including contractual liability coverage) with coverage limits of not less than One Million Dollars (\$1,000,000) per occurrence and \$2,000,000 General Aggregate, with the policy naming HS SAI as an additional insured; (2) Business Auto Liability, if any owned, hired or non-owned vehicles are used in connection with any work performed on behalf of HS SAI, with limits of \$1,000,000 Bodily Injury and Property Damage Liability for each occurrence; and (3) worker's compensation insurance as and if required by law, and, where required, including Employers Liability insurance with limits of \$100,000 /\$500,000/\$100,000 and including, if applicable, coverage for Federal Statutes; HS SAI will not be liable for any Workers Compensation benefits. Consultant shall provide HS SAI with a certificate of insurance evidencing the insurance coverage required under this clause when requested.

b. Waivers of Subrogation, on behalf of HS SAI are required on the Commercial General Liability and Workers Compensation /Employers Liability insurance.

c. Consultant agrees to provide HS SAI at least 30 days prior written notice, with a 10 day notice for non-payment of premium, of any cancellation or material change in the coverage stated herein.

19. Indemnification

To the fullest extent permitted by law, Consultant shall indemnify, defend and hold HS SAI and HS SAI's clients harmless from and against any and all claims, demands, actions, suits proceedings, losses, damages, penalties, obligations, liabilities, costs and expenses (including, without limitation, reasonable attorneys' fees) arising directly or indirectly, in whole or in part from the acts or omissions of Consultant or the breach by Consultant of its obligations under this Agreement, including, without limitation, the breach of any warranty set forth under the clause entitled, "Warranty," and including but not limited to patent and copyright infringement, contractual claims, and Governmental obligations, such as obligations under the laws pertaining to social security, unemployment insurance, workmen's compensation, income tax and deductions and other items required by state and federal law.

20. Termination

a. Termination for Convenience

This Agreement may be terminated at any time in whole or in part for the convenience of HS SAI by providing the Consultant with prior written notice. Such notice shall specify the extent to which the Agreement is being terminated, including which, and to what extent, current Task Orders are being terminated. Upon receipt of such notice, Consultant shall cease providing further Services as of the date of termination specified in the notice, advise HS SAI of the extent to which Consultant has completed the Services through such termination date, and deliver to HS SAI whatever Work Product then exists, and any physical embodiment thereof, in the manner requested by HS SAI. HS SAI shall make a final settlement payment to Consultant for all work performed through the date of such termination based on actual hours worked and actual expenses incurred if the work is being performed on a T&M basis or on a percent of completion if performed on a FFP basis.



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



a. Termination for Default

(1) If either party fails to cure any breach of its obligations under this Agreement within ten (10) days following written notice from the other party, then such other party may terminate all or part of this Agreement, effective immediately, by providing the defaulting party with written notice of termination. Such written notice of termination shall specify the extent to which individual Task Orders are being terminated.

(2) If Consultant becomes bankrupt or otherwise insolvent, HS SAI may, at its sole option and with written notice effective immediately, terminate this Agreement for default and pursue any other remedies available at law or in equity.

21. Exercise of Rights

HS SAI's failure to exercise any of its rights shall not constitute a waiver of any past, present or future right or remedy.

22. Security of Access-Restricted and Classified Documents, Materials, Information or Facilities

a. Consultant hereby covenants and agrees to: (1) strictly comply with all laws, rules, regulations and procedures of applicable governmental agencies, of HS SAI, and of HS SAI customers relating to the protection, handling and security of classified, proprietary or other restricted-access documents, materials, information or facilities; (2) refrain from obtaining access to or knowledge of such unless authorized to do so and such access or knowledge is necessary for the Services being performed for HS SAI hereunder; and, further, will not (3) intentionally or negligently disclose to any unauthorized person or any third party any information regarding same, or, if applicable, its existence; and, (4) remove from its designated place of retention any such document or material, make and/or remove any copy, reproduction, extract, picture, sketch, compilation or summary from any of said documents, materials information or facilities.

b. If the work issued to Consultant by any Task Orders involves access to information considered classified by the U.S. Government, the level of such Classified Information will be specified in the Task Order and Consultant will not be allowed access to classified information until and unless HS SAI's Security Officer has obtained certification of an appropriate Government security clearance for

Consultant. Provided such clearance is established, physical possession of classified material may be granted Consultant only in HS SAI's facility, unless otherwise authorized in writing by HS SAI. Consultant agrees to execute any and all forms related to the obtaining of and termination of security clearances hereunder and to abide by the provisions of HS SAI's Security Manual of Standard Practice Procedures, a copy of which shall be furnished to Consultant.

c. In the event that Consultant does not possess his/her own Facility Clearance (FCL), HS SAI shall hold Consultant's Personnel Security Clearance (PCL). In the event Consultant creates a partnership, corporation or other corporate legal entity to perform the work described in this Agreement prior to the termination of this Agreement, and, such new legal entity will use multiple employees with a need for access to classified information under this Agreement, then, until such time as this Agreement is either a) terminated and a Subcontract Agreement executed, or b) modified to become a Subcontract Agreement, and Consultant obtains its own FCL, HS SAI may hold up to two (2) PCLs of the employees of the new corporate entity.

23. Surrender of HS SAI Materials, Documents, and Equipment

Upon the earlier of: (1) the termination of this Agreement, (2) the completion of a Task Order, or (3) a written demand by HS SAI, Consultant shall promptly return to HS SAI or to HS SAI customers, as directed by HS SAI, all documents, writings, tools, equipment and other materials made available to Consultant by HS SAI and/or HS SAI customers, or compiled or generated by Consultant in the course of performing Services hereunder, all of which shall be deemed to be the property of HS SAI and/or its customers and for which HS SAI is the custodian.

24. Proprietary Information

a. All proprietary, confidential and business information of HS SAI and/or its customers including, but not limited to, information in tangible form marked with "Proprietary," "Confidential" or similar markings, specifications, processes, procedures, written documents, source code, capabilities, current or prospective products, services, customers or contracts, marketing strategies, research and development activities, and financial data ("Proprietary Information") shall be protected by the Consultant from disclosure to third parties. Any and all Proprietary Information shall be protected in the



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



same manner and to the same degree that the Consultant protects its own proprietary information, but at a minimum will not: (1) disclose such Proprietary Information to any person who is not an employee of HS SAI or has not been authorized by HS SAI in writing to be given same; (2) directly or indirectly use such Proprietary Information for Consultant's benefit or for that of any other business; and (3) will do all things reasonably required or requested by HS SAI and/or HS SAI's customers for the protection of such Proprietary Information. Consultant may use or disclose Proprietary Information that is or becomes publicly available, is already lawfully in Consultant's possession, is independently developed by Consultant, is lawfully obtained from third parties or the disclosing party has granted prior and specific written consent to the Consultant indicating the Proprietary Information may be disclosed to a third party. Protection of any such Proprietary Information shall continue for a period of five (5) years following the termination of this Agreement in accordance with the "Termination" clause or the "Term" clause, as appropriate. The provisions of this clause shall survive the termination of this Agreement.

b. Any additional terms and conditions related to non-disclosure of Proprietary Information imposed by an HS SAI client shall be set forth in Exhibit D.

23. Drug-Free Workplace and Workforce

The United States Government requires that defense contractors maintain a program for achieving a drug-free workplace and workforce. Testing may be required for Consultant seeking to perform work under HS SAI's Government contracts. Unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance by any Consultant is prohibited and is the basis for immediate termination of this Agreement under the "Termination for Default clause."

26. Notice of Delays/Excused Performance

a. Whenever the Consultant has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this Agreement, the Consultant shall immediately notify HS SAI, in writing, giving pertinent details. However, this data shall be informational only in character, and this provision shall not be construed as a waiver by HS SAI of any delivery schedule, or date, or any rights or remedies provided by law or under this Agreement.

b. Neither party shall be liable for, and is excused from any failure to deliver or perform or for delay in

delivery or performance due to causes beyond its reasonable control, such as acts of nature, governmental actions, fire, labor difficulty, shortages, civil disturbances, and interruptions of power or communications.

27. Assignment or Transfer/Subcontracting

a. Neither party to this Agreement may assign or transfer its interest in this Agreement to any other entity without prior written consent of the other party.

b. Consultant may not subcontract any portion of the Services to any lower-tier subcontractor of consultant without the prior written approval of HS SAI. Without such approval, no payments for Services performed by a lower-tier subcontractor or consultant will be made to Consultant.

28. Modifications

Any modifications of this Agreement shall be in writing and executed by both HS SAI and the Consultant.

29. Audit

To the extent that actual costs and/or labor hours of personnel form the basis of payment under this Agreement, the Consultant shall provide to HS SAI or to the Government or to an independent auditor supporting documentation which is adequate to perform audit and verification of such actual costs and labor hours.

30. Disputes

Any dispute not disposed of by executive management of both parties, if any shall be determined in the following manner.

a. The Parties agree to enter into Negotiation to resolve any dispute. Both parties agree to negotiate in good faith to reach a mutually agreeable settlement within a reasonable amount of time.

b. If negotiation is unsuccessful, the Parties agree to enter into binding Arbitration. The American Arbitration Association (AAA) Commercial Arbitration Rules (most recent edition) are to govern this Arbitration. The Arbitration shall take place within the Commonwealth of Virginia. The Arbitrator shall be bound to follow the applicable subcontract provisions and Virginia law in adjudicating the dispute. It is agreed by both parties that the Arbitrator's decision is final, and that no party may take any action, judicial or administrative, to overturn this decision. The decision rendered by the Arbitrator may be entered in any court having jurisdiction thereof.

**ANALYTIC SERVICES INC.**

Informing decisions that shape the Nation's future.



c. Pending any decision, appeal or judgment referred to in this provision or the settlement of any dispute arising under this Subcontract, Subcontractor shall proceed diligently with the performance of this Subcontract.

31. Incorporation of Attachments

The following attachments or exhibits are hereby incorporated into this Agreement by reference:

- a. Exhibit A "Statement of Work"
- b. Exhibit B "Prices/Rates/Other Info"
- c. Exhibit C "Sample Task Order Form"
- d. Exhibit D "Prime Contract Specific Terms and Conditions"
- e. Exhibit E "Sample Consultant Invoice"
- f. Exhibit F "Additional/Modified Terms"

32. Order of Precedence

In the event of an inconsistency in this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. This Agreement and its Attachments
- b. Task Order's Price, Payment, Period of Performance and Statement of Work Clauses
- c. Other terms and conditions added to a Task Order
- d. Terms and conditions from an HS SAI client incorporated by reference in a Task Order

33. Severability

Should any provision of this Agreement violate any law or should any provision be held invalid or unenforceable by a court of competent jurisdiction, then such provision shall be deemed to be restated to reflect as nearly as possible the original intentions of

the parties in accordance with applicable law; the remainder of this Agreement shall remain in full force and effect.

34. Non-Waiver

Analytic Services Inc. may specifically waive any failure of Consultant to comply with a provision of this Agreement, provided that no such waiver shall be binding or effective unless in writing and signed by Analytic Services Inc. and that no such waiver shall operate as or be construed to be a continuing waiver, a waiver of any other failure to comply with such provision, or a waiver of any failure to comply with other provisions of this Agreement.

35. Governing Law

This Agreement shall be construed and the legal relations between the two parties hereunder determined in accordance with the laws of the Commonwealth of Virginia.

36. Entire Agreement

- a. This Agreement, along with any attachments, is executed with the understanding that it constitutes the entire agreement between the parties and it supersedes all prior communications, representations, warranties, or agreements, oral or written.
- b. No changes in or additions to or waivers of the terms and conditions hereof shall be binding upon either party, unless approved in writing by its authorized representatives, and no modifications shall be effected by the conduct of the parties, including, without limitation, the acknowledgment or acceptance of purchase order forms containing other or different terms and conditions.

IN WITNESS WHEREOF, THE PARTIES HAVE EXECUTED THIS AGREEMENT AS OF THE LAST DATE WRITTEN BELOW:

ANALYTIC SERVICES INC.

RICHARD DANZIG

By Signe E. LiskowBy Richard DanzigPrinted Name Signe E. LiskowPrinted Name Richard DanzigTitle Director of ContractsTitle ConsultantDate 9/2/09Date SEP 11 2009



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



Exhibit A

Statement of Work

The Consultant shall perform the Services described below when and if ordered under this Agreement via Task Orders:

As requested Dr. Danzig will provide subject matter expertise associated with the fields of bio-defense policy and public health. This subject matter expertise will be in the form of analysis and feedback.

**ANALYTIC SERVICES INC.**

Informing decisions that shape the Nation's future.

**Exhibit B****Prices/Rates/Other Info**

- a) If T&M Task Orders are issued under this Agreement, the following labor rate, labor category and description shall be applicable to all work ordered under this Agreement:

[REDACTED]

- b) Consultant's principal place of business is: 3670 Upton Street NW, Washington, DC 20008

- c) If approved in advance, meals, hotel expenses and mileage while in travel status shall be reimbursed at actual cost not to exceed the limitations set forth in the Federal Travel Regulations. No travel within the Greater Washington, DC metropolitan area shall be reimbursed.

- d) Consultant's taxpayer identification number is: [REDACTED]

- e) Consultant's small business size status is: Sole Proprietor

- f) Consultant's NAICS code, if applicable: _____

ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.

**CONSULTANT AGREEMENT NO. C-09-078-DANZ
MODIFICATION NO. 01**

PURPOSE MODIFICATION: The purpose of this modification is to extend the period of performance end date for the above referenced Consultant Agreement (Changes in bold)

The Consultant Agreement end date is modified as follows.

FROM:

May 14, 2009 to May 14, 2010

TO:

May 14, 2010 to March 4, 2014

Except as provided herein, all other terms and conditions of consultant agreement remain unchanged and in full force and effect.

THIS ORDER IS ISSUED IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE CONSULTANT AGREEMENT REFERENCED ABOVE. NO CHANGES MAY BE MADE TO THIS ORDER UNLESS AGREE TO IN WRITING BY ANSWER.

Approval: Analytic Services Inc.

[Signature]
for Rene Govantes
Signature

Rene Govantes

Printed Name

Director of Contracts

Title

7/27/12
Date

Acceptance: Richard Danzig

[Signature]
Signature
RICHARD DANZIG
Printed Name
CONSULTANT
Title

July 24, 2012
Date


ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.


Exhibit D
Prime Contract Specific Terms and Conditions
Markings

All deliverables shall be submitted to ANSER and shall be accompanied by a packing list or other suitable shipping documentation that shall clearly indicate the following:

- (a) Agreement number;
- (b) ANSER's Task Order number;
- (c) Name and address of point of contact

Branding

a. The Consultant shall comply with the requirements of any DHS Branding and Marking policies. As a matter of law, Federal criminal statutes prohibit unauthorized uses of the DHS Seal. In addition, DHS policy prohibits granting authorization for certain commercial uses of the Seal. It is permissible to reference DHS in materials if the reference is limited to true, factual statements. The words DHS and/or Homeland Security should appear in the same color, font, and size as the rest of the text in the document. Moreover, such references shall not imply in any way an endorsement of a product, company, or technology.

b. Requests to use the DHS Seal shall be submitted to ANSER's Technical POC for submission to DHS. The Consultant should describe why use of the Seal is being requested and how it will be used.

Publications and Communications Concerning Work Performed Under This Agreement

No public communication referencing the work performed under this Agreement shall be made without the prior written consent of the ANSER. The Consultant will route technical communication products such as reports, journal articles, presentations, white papers and public communication products, such as brochures and flyers, through the ANSER for review and approval 45 days before any release to an external audience.

Public and technical communications shall contain the following language:

Acknowledgement

"The U.S. Department of Homeland Security (DHS) sponsored the production of this material under Contract No.HSHQDC-09-D-0003 with Analytic Services Inc."

Dissemination of Agreement Information/Advertising

a. Under no circumstances shall the Consultant, or anyone acting on behalf of the Consultant, refer to the supplies, services, or equipment furnished pursuant to the provisions of this Agreement in any publicity news release or commercial advertising without first obtaining prior and explicit written consent to do so from the ANSER. This restriction does not apply to marketing materials developed for presentation to potential Government sponsors under the Prime Contract.

b. The Consultant agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

c. The Consultant shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this Agreement, without



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



the prior written consent of the ANSER. An electronic or printed copy of any material proposed to be published or distributed shall be submitted to the ANSER.

Travel

a. Travel – General

All travel must be pre-approved by ANSER. The Consultant will provide trip reports to ANSER upon completion of travel at the level of detail specified by a Task Order or the Task Order's Point of Contact. Local travel within the greater Washington, DC metropolitan area will not be reimbursed. Other travel will be reimbursed in accordance with the *Federal Travel Regulation*.

b. Travel Outside of the United States

- (1) Approval of Foreign Travel: The cost of foreign travel is allowable only when the specific written approval of the ANSER Subcontract Administrator is obtained prior to commencing the trip. Approval must be requested at least 45 days before the scheduled departure date in order that all necessary clearances may be processed and the required approvals from DHS may be obtained. Each individual trip must be approved separately. Foreign travel is defined as any travel outside of the United States and its territories and possessions.
- (2) Travel shall take place in accordance with the Federal Travel Regulations (FTR) and will be considered reasonable and allowable to the extent permitted by FAR 31.205-46 and does not exceed the funding limitations of this Agreement. Documentation will be available upon request to the ANSER and/or the Defense Contract Audit Agency. The Consultant must notify ANSER, 45 days (for unclassified visits) or 60 days (for classified visits) before arrival of visitors from foreign countries.

Organizational Conflicts of Interest and Confidentiality

(a) Purpose. The purpose of this clause is to ensure that the Consultant (1) is not biased because of its financial, contractual, organizational, or other interests that relate to the work under this Agreement, and (2) does not obtain any unfair competitive advantage over other parties by virtue of its performance of this Agreement.

(b) Scope. The restrictions described herein shall apply to performance or participation by the Consultant and any of its affiliates or their successors in interest (hereinafter collectively referred to as "Consultant") in the activities covered by this clause. For the purpose of this clause, affiliation occurs when a business concern is controlled by or has the power to control another or when a third party has the power to control both.

(1) Use of Consultant's Work Product. (i) The Consultant shall be ineligible to participate in any capacity in Department of Homeland Security (DHS) and component contracts, subcontracts, or proposals thereof (solicited and unsolicited) which stem directly from the Consultant's performance of work under this Agreement during the term of this Agreement and for a period of two years after the completion of this Agreement. Furthermore, unless so directed in writing by the Government CO through ANSER's Subcontract Administrator, the Consultant shall not perform any systems engineering or development work under this Agreement on any of its products or services or the products or services of another firm if the Consultant is or has been substantially involved in their development or marketing. Nothing in this subparagraph shall preclude the Consultant from competing for a recompetition of this Agreement.

(ii) If, under this Agreement, the Consultant prepares a complete or essentially complete statement of work or specifications to be used in competitive acquisitions, the Consultant shall be ineligible to perform or participate in any capacity in any contractual effort which is based on such statement of work or specifications. The Consultant


ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



shall not incorporate its products or services in such statement of work or specifications unless so directed in writing by ANSER or the Government, in which case the restriction in this subparagraph shall not apply.

(iii) Nothing in this paragraph shall preclude the Consultant from offering or selling its standard and commercial items to the Government.

(2) Access to and use of information.

(i) If the Consultant, in the performance of this Agreement, obtains access to information, such as DHS plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 (5 U.S.C. 552a), or data which has not been released or otherwise made available to the public, the Consultant agrees that without prior written approval of the Government's Contracting Officer it shall not:

(A) use such information for any private purpose unless the information has been released or otherwise made available to the public;

(B) compete for work for DHS based on such information for a period of six (6) months after either the completion of this Agreement or until such information is released or otherwise made available to the public, whichever is first;

(C) submit an unsolicited proposal to the Government which is based on such information until one year after such information is released or otherwise made available to the public; and

(D) release such information unless such information has previously been released or otherwise made available to the public by DHS.

(ii) In addition, the Consultant agrees that to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 (5 U.S.C. 552a), or other confidential or privileged technical, business, or financial information of third parties under this Agreement, it shall treat such information in accordance with any restrictions imposed on such information.

(c) Disclosure after award.

(1) The Consultant agrees that, if changes, including additions, to the facts disclosed by it prior to award of this Agreement, occur during the performance of this Agreement, it shall make an immediate and full disclosure of such changes in writing to the SA for transmittal to the Government CO.

(2) In addition, the Consultant shall provide the SA for submittal to the Government Contracting Officer any disclosure of interests of itself or its affiliates that creates a real or potential organizational conflict related to the performance under ANSER's specific Task Orders.

(3) The disclosure may include a description of any action which the Consultant has taken or proposes to take to avoid, neutralize, or mitigate any resulting conflict of interest. ANSER may, however, terminate this Agreement for convenience or prohibit the Consultant from working on any individual ANSER TO if it deems such termination to be in the best interest of ANSER and the Government.

(4) In the event that the Consultant was aware of facts required to be disclosed or the existence of an actual or potential organizational conflict of interest and did not disclose such facts or such conflict of interest to the SA or the Government Contracting Officer, ANSER may terminate this Agreement for default.



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



(d) Remedies.

For breach of any of the above restrictions or for nondisclosure or misrepresentation of any facts required to be disclosed concerning this Agreement, including the existence of an actual or potential organizational conflict of interest at the time of or after award, ANSER may terminate this Agreement for default, disqualify the Consultant from subsequent related contractual efforts, and pursue such other remedies as may be permitted by law or this Agreement.

(e) Waiver.

Requests for waiver under this clause shall be directed in writing to the ANSER Subcontract Administrator for transmission to the Government CO and shall include a full description of the requested waiver and the reasons in support thereof. If it is determined to be in the best interests of the Government, the Government CO may grant such a waiver in writing.

(f) Subcontracts.

(1) The Consultant shall include a clause, substantially similar to this clause, including this paragraph (f), in subcontracts expected to exceed the simplified acquisition threshold determined in accordance with FAR part 13 and involving the performance of advisory and assistance services as that term is defined at FAR 37.201. The terms "Contract," "Contractor," and "Contracting Officer" shall be appropriately modified to preserve the Government's rights.

(2) Prior to the award under this Agreement of any such second-tier subcontracts for advisory and assistance services, in fulfilling its obligations under this Agreement, the Consultant shall obtain from the proposed subcontractor the disclosure of facts relevant to the performance of the proposed subcontract and shall determine in writing whether the interests disclosed present an actual or significant potential for an organizational conflict of interest. Where an actual or significant potential organizational conflict of interest is identified, the Consultant shall take actions to avoid, neutralize, or mitigate the organizational conflict to the satisfaction of the Consultant. If the conflict cannot be avoided or neutralized, the Consultant must obtain the approval of the DHS CO through the ANSER Subcontract Administrator prior to entering into the subcontract."

Investigating and Reporting Possible Scientific Misconduct

- a. "Misconduct" or "Misconduct in Science" is defined as fabrication, falsification, plagiarism, or other practices that seriously deviate from those that are commonly accepted within the scientific community for proposing, conducting or reporting research. It does not include honest error or honest differences in interpretations or judgments of data.
- b. Consultant shall foster a research environment that prevents misconduct in all research and that deals forthrightly with possible misconduct associated with research for which DHS funds have been provided or requested.
- c. The Consultant agrees to:
 - (1) Establish and keep current an administrative process to review, investigate, and report allegations of misconduct in science in connection with research conducted by the Consultant;
 - (2) Comply with Consultant's own administrative process;
 - (3) Inform Consultant's scientific and administrative staff of the policies and procedures and the importance of compliance with those policies and procedures;
 - (4) Take immediate and appropriate action as soon as misconduct on the part of employees or persons within the organization's control is suspected or alleged; and
 - (5) Report to the ANSER Subcontract Administrator a decision to initiate an investigation into possible scientific misconduct.
- d. The Consultant is responsible for notifying the ANSER Subcontract Administrator of appropriate action taken if at any stage of an inquiry or investigation any of the following conditions exist:



ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



- (1) An immediate health hazard is involved;
- (2) There is an immediate need to protect Federal funds or equipment;
- (3) A probability exists that the alleged incident will be reported publicly; or
- (4) There is a reasonable indication of possible criminal violation.

Security Requirements

As further described in Homeland Security Acquisition Regulation (HSAR) 3052.204-71, if Consultant requires recurring access to Government facilities, facilities operated on behalf of the Government, sensitive government information, or IT resources, Consultant is required to have a favorably adjudicated Suitability background investigation prior to commencing work at the HSSAI PFRDC.

Work under this Agreement can be classified at up to *Top Secret, SCI*. ANSER will provide specific security compliance guidance via DD Form 254. Under provisions of U.S. Law, Title 18, U.S. Code section 499 and 701, the Consultant will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, if any, included in this Agreement, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service (DSS). If the Consultant has access to classified information at a DHS or other Government Facility, it will abide by the requirements set by the agency.

Under provisions of U.S. Law, Title 18, U.S. Code section 499 and 701, the Consultant will return any expired DHS issued identification cards and building passes, and Government owned property to ANSER. If an identification card or building pass is not available to be returned, a report must be submitted to ANSER, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

Reporting Waste, Fraud, Abuse and Theft

The Consultant shall notify ANSER's Subcontract Administrator of any instances of suspected waste, fraud, abuse, loss, or theft of ANSER or Government-furnished property.

DHS Non-Disclosure

In addition to any non-disclosure or confidentiality agreements which may have been, or will be, executed with ANSER, Consultant agrees to sign DHS Form 11000-6 (08-04), "Department of Homeland Security Non-Disclosure Agreement," or a subsequent DHS form covering the restrictions on various categories of information protected by its terms, prior to performance of any work under this Agreement.

U.S. Citizenship

All personnel working under ANSER's Prime Contract are required to be U.S. citizens. Consultant's execution of this Agreement shall constitute a certification that the Consultant is a U.S. citizen.

FAR and Other Federal Terms and Conditions

The following terms and conditions from the Federal Acquisition Regulations and other Government regulations are hereby incorporated into this Agreement with the same force and effect as if set forth in their entirety. Such terms and conditions shall be interpreted to read as follows: "Government" or "Contracting Officer" shall mean "HS SAI", except where the context indicates the original meaning should be retained, and the words "Contractor," "Supplier," "Vendor," "Consultant" or similar words shall mean the Consultant as defined in the main body of this Agreement.


ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



FAR Number	FAR Title	Last Revision Date
52.202-1	Definitions	Jul-04
52.203-3	Gratuities	Apr-84
52.203-5	Covenant Against Contingent Fees	Apr-84
52.203-7	Anti-Kickback Procedures	Jul-86
52.203-13	Contractor Code of Business Ethics and Conduct	Dec-07 Dec-08
52.203-8	Cancellation, Rescission and Recovery of Funds for Illegal or Improper Activity	Jan-87
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	Jan-87
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	Jan-03 Sep-07
52.204-4	Printed or Copied Double Sided on Recycled Paper	Aug-00
52.204-9	Personal Identity Verification of contractor Personnel	Sep-07
52.209-8	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	Jan-06 Sep-06
52.215-2	Audit and Records -- Negotiation	Jun-99
52.215-8	Order of Precedence -- Uniform Contract Format	Oct-97
52.215-10	Price Reduction for Defective Cost or Pricing Data	Oct-97
52.215-12	Subcontractor Cost or Pricing Data	Oct-97
52.215-14	Integrity of Unit Prices	Oct-97
52.215-15	Pension Adjustments and Asset Reversions	Oct-04
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions	Oct-97 Jul-05
52.215-21	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data -- Modifications	Oct-97
52.216-7	Allowable Cost and Payment	Dec-02
52.216-8	Fixed Fee	Mar-87
52.216-15	Predetermined Indirect Cost Rates	Apr-98
52.219-9 Alt II	Small Business Subcontracting Plan - Alternate II	Apr-08 Oct-01
52.222-1	Notice to the Government of Labor Disputes	Feb-87
52.222-2	Payment for Overtime Premiums (insert value)	Jul-90
52.222-3	Convict Labor	Jun-03


ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



52.221-21	Prohibition of Segregated Facilities	Feb-99
52.222-26	Equal Opportunity	Apr-03 Mar -07
52.222-35	Equal Opportunity for Disabled Veterans, Veterans of the Vietnam Era and Other Eligible Veterans	Dec-04 Sep-06
52.222-36	Affirmative Action for Workers with Disabilities	Jun-98
52.222-37	Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era and Other Eligible Veterans	Dec-04 Sep-06
52.223-3 AK1	Hazardous Material Identification and Material Safety Data - Alternate I	Jan-97 Jul-95 (Alt I)
52.223-6	Drug Free Workplace	May-01
52.223-7	Notice of Radioactive Materials	Jan-97
52.223-14	Toxic Chemical Release Reporting	Aug-03
52.225-13	Restrictions on Certain Foreign Purchases	Mar-06 Jun-08
52.226-1	Utilization of Indian Organizations and Indian-Owned Economic Enterprises	Jun-00
52.227-1	Authorization and Consent	Dec-07
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	Dec-07
52.227-11	Patent Rights Retention by Contractor, Short Form	Dec-07
52.227-14 Alt II Alt III Alt IV	Rights in Data - General	Dec-07
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	Dec-07
52.227-19	Commercial Computer Software - Restricted Rights (This clause is limited to off the shelf commercial computer software)	Dec-07
52.227-16	Additional Data Rights	Dec-07 Jun-87
52.228-7	Insurance - Liability to Third Persons	Mar-96
52.230-2	Cost Accounting Standards	Apr-98 Oct-06
52.230-6	Administration of Cost Accounting Standards	Nov-99 Mar-08
52.232-17	Interest	Jun-98 Oct-06
52.232-20	Limitation of Cost	Jun-07 Apr-84
52.232-22	Limitation of Funds	Apr-84
52.232-23	Assignment of Claims	Jan-96
52.233-4	Applicable Law for Breach of Contract Claim	Oct-04
52.237-3	Continuity of Services	Jan-91


ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.



52.242-3	Penalties for Unallowable Costs	May-01
52.242-4	Certification of Final Indirect Costs	Jan-87
52.242-13	Bankruptcy	Jul-85
52.243-2	Changes – Cost Reimbursement (Aug 1987) – Alternate V	Apr-84 Aug-87
52.243-8	Change Order Accounting	Apr-84
52.244-2	Subcontracts (Aug 1988) – Alternate II	Aug-88 Jun-07
52.244-5	Competition in Subcontracting	Dec-06
52.244-6	Subcontracts for Commercial Items	Dec-04 Feb-08
52.245-1	Government Property	Jun-07
52.247-1	Commercial Bill of Lading Notations	Apr-84 Feb-06
52.247-83	Preference for U.S. Flag Air Carriers	Jun-03
52.251-1	Government Supply Sources	Apr-84
3052.204-71	Contractor Employee Access	Jun-06

52.204-2	Security Requirements	Aug 1996
52.215-19	Notification of Ownership Changes	Oct 1997
52.222-39	Notification of Employees Rights Concerning Payment of Union Dues and Fees	Dec 2004
52.227-23	Rights to Proposal Data (Technical)	Jun 1987
52.243-7	Notification of Changes	Apr 1984

52.246-6	Inspection of Services—Cost-Reimbursement	APR 1984
52.246-9	Inspection of Research and Development (Short Form)	APR 1984
52.246-16	Responsibility for Supplies	APR 1984
52.246-20	Warranty of Services	MAY 2001
52.242-15	Stop-Work Order (AUG1989) – Alternate I (APR 1984)	APR-1984 AUG 1989


ANALYTIC SERVICES INC.

Informing decisions that shape the Nation's future.


Exhibit E
SAMPLE INVOICE FORM

[DATE]

[CONSULTANT'S NAME]

[ADDRESS]

Client: Analytic Services Inc. (HS SAI)

Consultant Agreement No.: [X-XX-XXX-XXXX]

Task Order No.: [NUMBER]

Agreement No.: [NUMBER]

Invoice Number:

HS SAI Project Number: [XXXX-XXX]

Period of Performance Invoiced: [DATE] to [DATE]

		Current Month		Cumulative	
Rate	Hours	Total	Hours	Total	

Labor Cat.

Description of Services:

"I certify the above charges are true and accurate for the time period stated."

Signed:

Name/Title

Question#:	14
Topic:	acquisition
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: As a member of the Acquisition Review Board, S&T has a significant role in ensuring that acquisitions at DHS are technologically and scientifically feasible and necessary, and proceed with all necessary documentation. On May 9, 2013, the Office of the Under Secretary for Management at DHS issued a memorandum that absolved components from acquisition documentation requirements for 42 programs because they were already in the sustainment phase. However, as much as 60% of a procurement's lifecycle costs come in the sustainment phase.

As a member of the Acquisition Review Board, including S&T, are you aware of any cost-benefit analysis that was conducted before reaching the decision to absolve these programs of the documentation requirements? If so, please provide the analysis.

Response: Acquisition Review Boards (ARBs) are chaired by the Acquisition Decision Authority (ADA) who considers many elements such as cost, schedule, performance, etc. prior to making an acquisition decision. S&T's independent Director, Operational Test and Evaluation (DOT&E) as a member of the ARB, is responsible for reporting on the system performance specifically the system's operational effectiveness and suitability in meeting the requirements contained in the system's Operational Requirements Document (ORD). The DOT&E does not assess the cost-benefit of deployment and has not reviewed any cost-benefit analysis for projects listed on the May 9, 2013 memorandum. The Under Secretary for Science & Technology is also as a member of the ARB but S&T has not reviewed any cost-benefit analysis. The Department is developing the Integrated Investment Life Cycle Model (IILCM), which will link Departmental strategy to resource decisions for major acquisitions. The IILCM will evaluate requirements, programmatic needs, and program costs, including life cycle costs, to ensure the Department is capable of meeting its mission in the most efficient way possible.

Question: Are you aware of any projects not listed on the May 9, 2013 memorandum that have proceeded without all members of the ARB signing off on all Acquisition Decision Memoranda related to those projects? What were S&T's recommendations with respect to those programs? Please provide documentation of S&T's recommendations.

Response: Per DHS Management Directive 102-01 the Under Secretary for Management, through the Office of Program Accountability and Risk Management, is responsible for drafting and vetting Acquisition Decision Memoranda (ADMs).

Question#:	14
Topic:	acquisition
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Individual ARB members do not sign ADMs but do concur with the content during ARBs and review and concur with the ADM prior to final signature. Concerns with ADM's are addressed during the ARB and review phase.

S&T concurred with the decision of the ARB for the programs reviewed and documented in ADMs. However each of the programs listed were well into sustainment at the time MD 102-01 was implemented.

Additionally, by DHS T&E policy all major acquisition programs that require T&E must complete Operational Test and Evaluation (OT&E) prior to deployment. The acquisition program's T&E is documented in the Test and Evaluation Strategy (TEMP), Operational Test and Evaluation Plan (OTP), Operational/System Test and Evaluation Report and the DOT&E Letter of Assessment (LOA). The LOA includes an assessment of the adequacy of the operational test, a concurrence or non-concurrence on the Operational Test Agent evaluation of operational suitability and operational effectiveness, and any further independent analysis. The DOT&E submits each LOA to the ADA. The ADA considers many elements including the DOT&E LOA prior to making an acquisition decision.

Question#:	15
Topic:	GAO
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The S&T Test and Evaluation Program is in a position to assess the feasibility of the science behind acquisitions. A recent report from GAO was published regarding unreliable results from a pilot on the Transit Work Identification Credential (TWIC) Program. GAO has stated that DHS S&T developed a testing plan for the TWIC pilot but the test plan was not followed.

What was the reasoning by TSA for not using the test plan provided by S&T?

Response: In June 2007, S&T Director, Test and Evaluation and Standards Division (TSD) now Director, Operational Test and Evaluation (DOT&E), worked with the TWIC program office to develop and approve a Test and Evaluation Master Plan (TEMP) which is the overarching program test strategy. The TSD sponsored the conduct of environmental testing on several commercially available TWIC card readers to determine if they would operate in the coastal port environment. Since the TWIC programs mission was to develop and implement the TWIC Card, the test and evaluation (T&E) work supported TWIC program rule making. While TSA performed testing of the TWIC card and readers in various scenarios, there was no rule that required the individual Port Security sites to implement infrastructure or a standard operating procedure. Additionally, the TEMP required readers used in the pilot to complete formal testing prior to implementing field reader tests. TSA determined that waiting for TWIC readers to go through lengthy, formal laboratory testing would cause unacceptable delays to Reader Pilot progress. To alleviate this, TSA implemented an informal reader evaluation process to quickly make readers available for testing. Formal testing was completed concurrently with field tests. Therefore, the complete testing strategy as documented in the TEMP was not executed.

Question: Do you believe that DHS components should be required to consult S&T and use its testing plans? If not, why not?

Response: S&T supports Department policy as documented in Management Directive 102-01 and Management Directive 026-06 requiring major acquisitions to get a Test and Evaluation Master Plan (TEMP) approved prior to Acquisition Decision Event 2B (permission to proceed to the obtain phase). Individual programs develop specific test plans as required by the TEMP.

Question#:	15
Topic:	GAO
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

DHS Acquisition Policy was implemented in November 2008 and T&E Policy was implemented in May 2009. By DHS T&E policy all major acquisition programs that require T&E must complete Operational Test and Evaluation (OT&E) prior to deployment. The acquisition program's T&E is documented in the Test and Evaluation Strategy (TEMP), Operational Test and Evaluation Plan (OTP), Operational/System Test and Evaluation Report and the DOT&E Letter of Assessment (LOA). The LOA includes an assessment of the adequacy of the operational test, a concurrence or non-concurrence on the Operational Test Agent evaluation of operational suitability and operational effectiveness, and any further independent analysis. The DOT&E submits each LOA to the Acquisition Decision Authority (ADA). The ADA considers many elements including the DOT&E LOA prior to making an acquisition decision.

Question#:	16
Topic:	Best Places to Work
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In the 2012 rankings of the “Best Places to Work” across the Federal Government the Department of Homeland Security ranked last among large departments and S&T ranked last among 292 agency subcomponents. During the hearing you mentioned several possible reasons for this, including the effects of sequestration, the frequency of the survey, the temporary freeze on travel and conference spending, and issues with the civil service system. However, these are issues that are affecting every agency and subcomponent.

Have you solicited feedback from S&T employees about this ranking?

In your opinion, what are the specific issues with S&T have led to this ranking?

What is the Science and Technology Directorate doing to resolve the morale issue with its employees?

Response: I am deeply committed to the overall well-being of the S&T workforce and take the results of the Federal Employee Viewpoint Survey seriously. However, it is important to note that the methodology for the “Best Places to Work” survey utilizes only three of the 84 questions in the Federal Employee Viewpoint Survey (FEVS):

- I recommend my organization as a good place to work.
- Considering everything, how satisfied are you with your job?
- Considering everything, how satisfied are you with your organization?

Selecting only these three questions artificially distills the breadth of the survey and overlooks the areas where S&T scored strongly such as dedication to the mission, employee satisfaction with supervisors, a strong offering of training and development opportunities, and robust work-life balance options. Nevertheless, I was concerned about the overall survey results and wanted to explore the underpinnings in a more detailed, S&T-specific manner. Therefore, S&T commissioned our own internal survey.

One of the primary issues we identified was employees felt that they were lacking in resources (specifically, budget) to meet their mission. In my opinion, this reflects the 56% reduction in R&D funding to the Directorate from 2010 to 2012. Due to the cuts, S&T program managers saw many promising projects eliminated or paused due to funding constraints. Having a project in the middle of the R&D cycle be canceled not

Question#:	16
Topic:	Best Places to Work
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

only harms the DHS mission by preventing that technology from reaching fruition, but is also extraordinarily frustrating for the program manager. Some S&T staff were reassigned to new duties as a result of the funding reductions, resulting in additional dissatisfaction. In addition to the many challenges facing the federal workforce, having one's funding cut further impacts the ability to perform the mission which only decreases morale.

Survey results further revealed that employees felt a lack of personal empowerment with respect to work processes. During my tenure, S&T has undergone significant changes in organization (i.e. establishment of the Group Structure) as well as process (e.g. Portfolio Reviews). Employee dissatisfaction may be linked to the level of organizational change that has occurred within the S&T as a result of these actions. It is my belief that these changes were necessary and will be beneficial to the organization going forward, reflecting a leaner and more focused S&T.

Also of note, the survey indicated challenges associated with improving day-to-day information sharing and communication. Employees also cited dissatisfaction with recognition/reward programs, as well as policies and practices of senior leaders. Some of this dissatisfaction is rooted in the impacts of the sequester on the work force. The inability to offer awards and other fiscal restraints imposed by the sequester limits the tools available for management to improve the workplace environment. Despite this, we are aggressively pursuing "no cost" recognition options and other tools that are still available to us, but challenges remain in the current fiscal environment.

In response to the survey results, we instituted numerous actions. S&T implemented new awards and recognition events, including peer awards, in order to address the concerns around acknowledgement and recognition for work. I asked senior leaders within the Directorate to take a look at their individual organizations and identify actions they could take to improve overall morale, with a focus on communication. S&T leadership now routinely hold meetings to discuss organizational identity and strategic planning, include Q&A sessions in All Hands meetings, convene brown bag sessions on technical matters, and conduct weekly or biweekly meetings to discuss strategy and share information.

I personally dedicate time to promoting employee engagement and addressing employee morale; I routinely host "Tara Bytes" luncheons where employees are able to meet with me directly to discuss both successes and opportunities for organizational improvement. The Chief of Staff Monthly Outreach Session (COSMOS) meetings, "Ask Tara" email box, and S&T All Hands meetings are proving fruitful avenues to solicit input and ideas directly from staff. We have also implemented a new Alternative Work Schedule Policy

Question#:	16
Topic:	Best Places to Work
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

to provide greater flexibility for staff, and have projects underway to build more on-site collaboration spaces to improve the work environment.

These programs, policies, and engagement efforts contribute to the S&T workforce reaching its productivity and work-life balance goals, aim at improving morale, and support the development of a high-performing technical workforce.

Question#:	17
Topic:	SETA
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony you stated that the contractors at S&T are different than Systems Engineering and Technical Assistance (SETA) support contractors at other federal agencies.

Can you describe the differences between S&T SETA contractors and SETA contractors at other federal agencies?

Please provide a list of the current SETA contracts at S&T with the amount obligated against those contracts for FY09 through FY13.

What percentage of the non-management and administration (M&A) funds appropriated to the directorate for research and development are spent on contracts?

What is the ratio of federal employees to SETA support contractors at on-site at S&T?

How many Contracting Office Technical Representatives (COTRs) or Contracting Office Representatives (CORs) are designated to monitor the SETA support contracts?

How much has S&T spent on SETA support contracts between FY2009 and FY2013?

Response: Our SETA contractors are similar to the SETA contractors at other R&D organizations. They are mostly scientists and engineers with advanced degrees that provide support and technical assistance, usually on site with our federal program managers. The technical SETA support contractors are paid for out of the Research, Development, Acquisition, and Operations (RDA&O) appropriation and account for about 7% of the appropriation, ~\$50 million of the \$674 million appropriated in RDA&O. The vast majority of the RDA&O appropriation is placed on Interagency Agreements, contracts and grants with the Federal/National Laboratories, the private sector, or Universities where S&T oversees research and development, standards test and evaluation, operations and systems analysis, laboratory management and construction, and other work such as the SAFETY act to meet the mission requirements of the Homeland Security Enterprise.

The current SETA contracts at S&T include Booz Allen Hamilton; Acquisition, Research and Logistics Inc; Analytical Research LLC; SRA International; BAI Inc. and Teracore Inc.

Question#:	17
Topic:	SETA
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

The following is a table providing funding spent on SETA, FY13 is as of 14 August.

Contractor	FY09	FY10	FY11	FY12	FY13	TOTAL
Analytical Research, LLC	\$2,706,449.80	\$3,974,166.74	\$3,393,948.09	\$2,734,520.06	\$3,042,716.59	\$15,851,801.28
Acquisition, Research and Logistics, Inc.	\$0.00	\$0.00	\$0.00	\$2,377,509.31	\$4,393,607.43	\$6,771,116.74
BAI Inc	\$2,331,892.51	\$2,190,266.00	\$2,227,975.00	\$2,548,677.80	\$2,242,925.00	\$11,541,736.31
Booz/Allen/Hamilton	\$64,558,590.97	\$60,175,146.62	\$63,441,461.71	\$45,869,179.52	\$30,416,173.18	\$264,460,552.00
SRA INTERNATIONAL	\$20,167,648.51	\$9,133,597.00	\$9,575,765.56	\$5,939,474.52	\$6,832,277.68	\$51,648,763.27
Teracore, Inc.	\$0.00	\$4,425,051.26	\$4,182,507.66	\$3,222,253.56	\$2,689,000.00	\$14,518,812.48
TOTAL	\$89,764,581.79	\$79,898,227.62	\$82,821,658.02	\$62,691,614.77	\$49,616,699.88	\$364,792,782.08

The Decrease in the SETA funding is a result of position conversions. S&T continues to hire Federal Employees into areas where a federal employee is a more suitable match for the position. Booz/Allen/Hamilton (BAH) has been the main and largest SETA contractor at S&T. The main SETA contract was recompleted this year (FY13) as an indefinite delivery/indefinite quantity (IDIQ) contract. The award has been made to three companies, BAH, Noblis, and Mantech. The first task orders on that contract will be competed and awarded in early FY14.

The Percentage of Research, Development, Acquisition, and Operations (RDA&O) (non M&A) funds spent on contracts, interagency agreements, or grants with private industry, universities Federal/National laboratories for both research and development and SETA is 96% with the other 4% going to Federal employees at the S&T laboratories.

Federal employees to on-site SETA support contractors ratio as of 30 June 2013 is 261 contractors to 459 federal employees, slightly more than one SETA to every 2 Federal employees.

There are 22 CORs monitoring the SETA contracts listed above.

Question#:	18
Topic:	contractors
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony you stated that S&T is using contractors to manage travel for DHS S&T employees. Your specific reasoning for the use of contractors to manage travel was that it is saving the directorate money.

Please provide the cost benefit analysis that was done by the Science and Technology directorate to determine the financial savings of contracting out the management of the travel process.

Please provide a copy of the current contract as well as the annual cost of maintaining the contract.

How much has the Science and Technology Directorate spent on travel for the years FY 2009 through FY 2013?

Response: In 2010, one of the major complaints I received from S&T employees was the time required and difficulty in using and the inflexibility of the electronic travel system and the labyrinth of Federal travel regulations. To address this issue, S&T established an office staffed with experts in the electronic travel system and Federal travel regulations to address the concerns expressed by employees throughout the directorate. This new team addressed the following issues:

- Usability of a new travel system FedTraveler.com
- Lengthy processing times (for travel and reimbursement)
- Lack of knowledge of travel regulations, policies, and processes

With travel processing as their focus, they know and understand the travel system and understand travel regulations and policies. The team is a mix of five contractors and six and a half full time Federal employees; they support 279 employees. Since inception the team has achieved the following:

- Reduced Electronic Travel document failure rates from 17% to less than 2%;
- Reduced travel document processing times from start to finish by 50%;
- Achieved cost savings through increased online adoption rate, resulting in lower transaction fee expenses in support of the Department Travel Efficiency Initiative.

Question#:	18
Topic:	contractors
Hearing:	The Department of Homeland Security at 10 Years: Harnessing Science and Technology to Protect National Security and Enhance Government Efficiency
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

- Increased communication and collaboration amongst travelers and senior management participating in the program.
- Created an accurate travel reporting structure streamlining the process required to generate data; and minimizing the use of manually prepared reports to achieve accuracy.
- Helped reduce travel expenses from \$3,741,000 in FY 2011, \$2,939,000 in FY 2012 to currently \$1,553,000 as of August 6, 2013, and projected by year end to be under \$2,000,000 for FY 2013.

The new travel team was established to facilitate travel authorizations but it also ended up saving money.

Current contract is attached.

S&T Funding spent on Travel for each Fiscal Year

<i>Year</i>	<i>Total</i>
2009	\$4,162,958
2010	\$4,808,248
2011	\$3,741,875
2012	\$2,939,195
2013	\$1,971,000
	\$17,623,276

FY13 funding as of 6 August

Attachment 1 – HSHQDC-12-J-00352

**DEPARTMENT OF HOMELAND SECURITY (DHS)
STATEMENT OF WORK (SOW)
FOR**

FINANCIAL SERVICES SUPORT

**Science and Technology Directorate
Finance and Budget Division**

1.0 GENERAL**1.1 BACKGROUND**

The Science and Technology (S&T) Directorate's mission is to improve homeland security by working with partners to provide state-of-the-art solutions and/or technology that helps them achieve their missions. S&T partners and customers include the operating Components of the Department, other government agencies, State, local, tribal, and territorial emergency responders and officials.

The purpose of this acquisition is to acquire financial services for the Science and Technology Directorate, Finance and Budget Division.

The Finance and Budget Division provides the S&T Directorate with high-quality, efficient, and cost-effective financial management services through five branches. The Budget Branch develops long-term plans for resource allocation, execution plans, Congressional Justifications, and management of financial resources within the S&T Directorate, as well as, develops and implements internal and external performance metrics for S&T Directorate programs, as well as risk assessment methodologies to help inform programming decisions. The Acquisition Branch develops the S&T Directorate's acquisition strategy and manages and prepares S&T's interagency agreements. The Financial Services Branch manages the travel and purchase card programs and the validation and verification program within S&T. The Financial Operations Branch is dedicated to sound fiscal stewardship of the S&T Directorate's appropriations and reimbursable funding; timely and accurate budget execution, financial management and financial reporting. The Internal Controls Branch monitors programs and activities to provide assurance about the adequacy of internal controls within the S&T Directorate.

1.2 SCOPE

The Scope of this work is under Functional Category 1 Program Management. The scope of work for this acquisition includes labor, materials, equipment, and supplies necessary to supply financial support services to the Science and Technology Directorate's Finance and Budget Division's five branches: Budget Branch, Acquisition Branch, Financial Services Branch, Financial Operations Branch and Internal Controls Branch. The financial services support will be in accordance with the task requirements outlined in this Statement of Work.

1.3 OBJECTIVE

The objective of this acquisition is to provide the Science and Technology Directorate, Finance and Budget Division with essential support services that is not inherently governmental and may require a level of effort that is not sufficiently consistent to warrant additional staffing with federal employees. Our mission is to maximize the efficient use of Science and Technology Directorate assets in support of the Homeland Security mission by improving business processes and tracking costs more effectively.

1.4 APPLICABLE DOCUMENTS

The Contractor shall comply with requirements of the following documents, updated as required, to meet the requirements of this contract:

- OMB A-123 http://www.whitehouse.gov/omb/circulars_a123_rev
- OMB A-11 http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc
- FAR <https://www.acquisition.gov/far/>
- FTR (Federal Travel Regulation) <http://www.gsa.gov/portal/content/104790>
- DHS IT Security Program Publication DHS MD 4300.Pub
<http://www.uscg.mil/acquisition/nais/RFP/Section1/DHS-MD-4300-1.pdf>
- DHS Acquisition Planning Forecast System Quick Reference Guide (Office of the Chief Procurement Officer/Acquisition Systems Branch), Version 1.0, April 14, 2011
http://www.dhs.gov/xlibrary/assets/opnbiz/cpo_hsam.pdf
- Economy Act (31 U.S.C. 1535 et seq.) as implemented in subpart 17.5 of the Federal Acquisition Regulation <http://www.casu.gov/authority/uscl535.html>
- Public Law 108-330 "The Department of Homeland Security Financial Accountability Act"
<http://www.hsdl.org/?view&did=467854>
- Section 309 (a) (1)(c) of the Homeland Security Act of 2002, Public Law 107-296 (116 Stat. 2135 (2002)) <http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf>
- DOE Order 484.1, Reimbursable Work for the Department of Homeland Security (August 17, 2006), including its attachments
<https://www.directives.doe.gov/search?Title=%22DOE+o+484.1%22&Subject:list=status+current&submit=Search>
- Interagency Acquisition Guide, Office of Federal Procurement Policy, OMB, June 2008
Intragovernmental Business Treasury Bulletin 2011-04
<http://www.fins.treas.gov/factsi/manuals/ifin-bulletin-2011-04.pdf>

2.0 TASK REQUIREMENTS

The drafting of official agency proposals for legislation, Congressional testimony, responses to Congressional correspondence, or responses to audit reports from an inspector general, the Government Accountability Office, or other Federal audit entity is prohibited; as these types of services are inherently governmental.

- 2.1 Task 1 – Acquisitions/Assembling Interagency Agreements - Processes documents needed for award, administration, and close-out of all Interagency Agreements. Requires knowledge of legal and regulatory authorities allowing the transfer of Federal funds. Requirements

involve highly technical research and development specifications with a standardized set of Terms and Conditions agreeable to the Federal entities. Requires a working knowledge of change order authority and knowledge of contract administration principles and practices to monitor contractor performance and to solve problems relating to administration of the agreement, contract modifications, payments and prevailing statutes or directives effecting the agreement are required as well as a general working knowledge of business and industry practices related to a contractor's ability to perform work for the government is beneficial. Additionally, requires knowledge of procurement monitoring and management control techniques necessary to monitor the contractor's financial and business conditions, to detect indicators having an adverse impact on contract performance (e.g., impending bankruptcy or severance of vendor support), and to recommend appropriate remedial action. To support the Acquisition Branch in this business need, the contractor shall provide support in:

- 2.1.1 Perform recurring assignments in support of assembling Interagency Agreements which can be either an inter or intra governmental transaction.
- 2.1.2 Process each agreement primarily through the use of information technology but is required to prepare an official hardcopy record of the official file.
- 2.1.3 Review requisitions and all necessary supporting documentations to ensure: requirements, deliverables, and schedules are clear and concise.
- 2.1.4 Initiate communications with technical, financial and support personnel to resolve questions concerning ambiguities, conflicts, and omissions within the documentation.

2.2 Task 2 - Budget Execution –The budget execution team provides timely and accurate budget execution and financial reporting support and liaise with OCFO, OPO, OGC, S&T Divisions and Program Offices, and performers to coordinate and conduct the planning, programming, budgeting, and execution of the President's budget for DHS Science and Technology. To support the Acquisition Branch in this business need, the contractor shall provide support in:

- 2.2.1 Originate Procurement Requisitions (PR) packages and collaborate with Program Managers (PMs) and Contracting Officers (CO) to collect all required hard-copy documentation such as Statements of Work, Determinations & Findings, Analysis of Alternatives, Sole Source Justifications, Independent Government Cost Estimates, etc. PR packages include new procurement actions, modifications to existing actions, no-cost period of performance extensions, de-commitments, and de-obligations of funds.
- 2.2.2 Create corresponding PR electronic records in FFMS, PRISM, and the OCFO Execution Performance Invoice Consolidation (EPIC) database.
- 2.2.3 Prepare and process PRs to recover funding for the rescission, if any.
- 2.2.4 Route PRs for approval, fund certification, fund commitment, and award through appropriate Program Office/Divisions, S&T Chief Financial Officer (CFO), and COs in hard copy and electronic format through FFMS, PRISM.
- 2.2.5 Monitor and ensure funds control for each procurement action by project level for each Division's execution plan.
- 2.2.6 Provide support and guidance to PMs and division staff on PR processing and documentation requirements, preparing current and prior FY Program Project Database Tracking Sheets and associated documents.
- 2.2.7 Monitor prior-year budgets and coordinate with the execution of these funds with PMs.

- 2.2.8 Collaborate with COs to provide guidance to program offices about procurement requirements and existing contract vehicles available to DHS.
 - 2.2.9 Monitor all awarded and un-awarded open commitments and coordinate with OPO and/or awardee to obtain countersigned agreements.
 - 2.2.10 Monitor and provide financial analysis on project-level budget execution activities and provide issue resolution as required.
 - 2.2.11 Reconcile financial and procurement data from FFMS, PRISM, and EPIC.
 - 2.2.12 Analyze program and division spending against allotments and other benchmarks required by CFO, and provide status reports to CFO and divisions quarterly or on a periodic basis.
 - 2.2.13 Compile and review PR Status Reports, Status of Funds, and current and prior FY Execution Reports from the EPIC Database for completeness and accuracy. Submit these financial reports to divisions on a weekly basis.
 - 2.2.14 Compile, review, and distribute the monthly Contract Status Report to OCFO and Division personnel.
 - 2.2.15 Prepare for, attend, and provide budget execution updates at weekly division and program office staff meetings.
 - 2.2.16 Respond to daily inquiries from program and division staff regarding status of PRs.
 - 2.2.17 Respond to Headquarters, Congressional inquiries, and S&T Leadership data calls as required.
 - 2.2.18 Provide additional ad-hoc financial analysis for division and program offices as necessary.
 - 2.2.19 Identify and continue to develop reporting requirements for divisions as necessary.
 - 2.2.20 Assist in the development of Standard Operating Procedures (SOPs) for OCFO operations.
 - 2.2.21 Manage emerging and changes to existing requirements as they relate to Budget Execution and Financial Reporting.
- 2.3 Task 3 – Financial Operations (Fin Ops) – Fin Ops is responsible for Funds Control, funds certification of commitments and obligations, processing of Intra Governmental Payment and Collection (IPACs) and commercial invoices, accounting of capital assets, reimbursable program financial management and the generation of internal and external reports. To support Fin Ops in this business need, the contractor shall provide support in:
- 2.3.1 Distribute IPACs and commercial invoices to the proper Contracting Officer (CO) and/or Contracting Officer Representative (COR) for certification.
 - 2.3.2 Perform certification follow ups with COs and/or COR's as necessary.
 - 2.3.3 Update WebView's process flow status location for each IPAC and/or invoice.
 - 2.3.4 Post required documentation in Webview for each IPAC and/or invoice.
 - 2.3.5 Research and resolve each IPAC placed into suspense status.
 - 2.3.6 Post required documentation in Webview to support suspense status resolution.
 - 2.3.7 Assist in the accepting and establishing new reimbursable agreements.
 - 2.3.8 Maintain reimbursable agreement log.
 - 2.3.9 Assist in ensuring reimbursable agreements are properly established in the accounting system.

- 2.3.10 Review open reimbursable agreements quarterly to determine if any can be closed.
 - 2.3.11 Assist in resolving any billing and/or collecting discrepancies between S&T and reimbursable customers.
 - 2.3.12 Assist in closing out reimbursable agreements.
 - 2.3.13 Assist in developing reimbursable budget authority estimates.
 - 2.3.14 Assist in maintaining reimbursable standard operating procedures.
- 2.4 Task 4 – Verification and Validation (V&V) – The verification process requires the identification and review of all available supporting documentation to verify that there is a bona fide contractual relationship between the performer and DHS S&T and that the amount of the unexpended obligation is reflected correctly in FFMS. This process also includes reviewing original obligating documents, subsequent modifications and amendments, invoices, and any other related transactional documentation. The validation process includes analyzing the supporting documentation associated with an obligation to determine whether the obligation should remain open or be de-obligated. If there are still goods and services to be delivered or pending Intra-Governmental Payment and Collection (IPAC) funds transfers or invoices, the obligation will remain open. However, if the obligation is no longer necessary, the contract has been fulfilled, all goods and services have been provided, and all IPACs or invoices have been received and paid, the obligation is processed for de-obligation in FFMS, permitting funding to be recovered and made available for other S&T priorities. To support Verification and Validation in this business need, the contractor shall provide support in:
- 2.4.1 Generate quarterly report of Unexpended Obligations.
 - 2.4.2 Generate/Distribute/Monitor/Record Open Obligation Certification Letters.
 - 2.4.3 Generate/Distribute/Monitor/Record Closeout and Follow-Up Closeout Letters.
 - 2.4.4 Perform reconciliation/analysis of any and all financial documents needed to de-obligate and/or close out any S&T obligation.
 - 2.4.5 Generate de-obligation PR packages as requested by PMs/COs/Customers/Other to include but not limited to FFMS reports, Customer reports, PRISM documentation, EPIC reports, Office of Procurement Operation (OPO) mandatory COR Checklist, V&V Forms, and other as required.
 - 2.4.6 Create corresponding PR electronic records in FFMS, PRISM, and the OCFO Execution Performance Invoice Consolidation (EPIC) database.
 - 2.4.7 Route PRs for approval, fund certification, fund commitment, and de-obligation through appropriate Program Office/Divisions, S&T Chief Financial Officer (CFO), and COs in hard copy and electronic format through FFMS/PRISM.
 - 2.4.8 Analyze Open Commitment Report, Log of Obligations, Recoveries of Prior Year Obligations, and Status of Funds reports as needed.
 - 2.4.9 Generate Recovery Reports and perform Recovery Report Reconciliation
 - 2.4.10 Review/Analyze/Complete Undelivered Obligations Head Quarters Data Call Report.
 - 2.4.11 Generate/Distribute/Monitor Performance Burn Rate Report and answer questions from S&T staff.
 - 2.4.12 Generate V&V Summary Reports.

- 2.4.13 Maintain working relationship with OPO and provide requested services and documentation as needed.
 - 2.4.14 File Verification and Validation documents.
 - 2.4.15 Generate/Update/Maintain Standard Operating Procedures.
 - 2.4.16 Provides analysis and support in the Department-wide annual A-123 internal controls assessment.
- 2.5 Task 5 – Travel Management and System Support – The Travel Management Office (TMO) is responsible for developing, implementing, and managing travel processes and several integrated and non-integrated systems used by federal and non-federal travelers for both domestic and international travel in compliance with the Federal Travel Regulations (FTR), departmental policies and S&T processes and procedures. The purpose of this work is to support the Travel Program Manager administering the E-Gov Travel Service Program and other operational needs related to the conduct of official travel for the Directorate and other miscellaneous financial expenditures (i.e. official employee expenses, tuition reimbursement). To support the TMO in this business need, the contractor shall provide support in:
- 2.5.1 Provides the full range of financial functions for major system development and implementation.
 - 2.5.2 Defines established financial business practices for integration into the clients financial business system.
 - 2.5.3 Works with functional specialists, automation specialists, contractors, vendors, and clients to effectively translate the client's requirements into an automated application.
 - 2.5.4 Performs substantive investigative, fact-finding, data acquisition, data compilation, data analyses, issues analyses and recommends solutions to potential problems.
 - 2.5.5 Reports generation assignments supporting complex financial and budget operations activities, related studies, and implementation of internal controls as it relates to travel program administration and system support.
 - 2.5.6 Uses automated databases such as the Execution Performance and Invoice Consolidation (EPIC) and web-based systems such as Fedtraveler.com to perform outline assignments and produce internal and external reports and analysis.
 - 2.5.7 Provides assistance in preparing responses to data calls and audit requests from the agency and external regulatory bodies (i.e. OIG, USM, OMB, GSA, etc.).
 - 2.5.8 Provides assistance in preparing reports, issue papers, and correspondence pertaining to financial management of S&T travel program.
 - 2.5.9 Re-engineers, develops and implements processes, procedures and systems as necessary for employees for both domestic and international travel.
 - 2.5.10 Ensures quality control and compliance to the Federal Travel Regulations (FTR) and departmental policy for all travel authorizations and expense reports.

- 2.5.11 Ensures accurate financial data in various financial and subsidiary systems, reconciles accounting and transaction data, and executes corrective action to assure data quality and consistency of the travel program.
 - 2.5.12 Processes documentation to re-allocate funds to correct imbalances and to deploy funds to meet changes in programs.
 - 2.5.13 Submits data for specific items of external monthly reports on program budget execution for review and final submission.
 - 2.5.14 Conveys established program and procedural guidance to stakeholders for dealing with standard financial and budgetary issues, and for preparing and submitting reports.
 - 2.5.15 Serves as a travel liaison for S&T travel program stakeholders.
- 2.6 Task 6 – Bankcard Program Management and Support –The purpose of this task is to support the Program Manager responsible for the implementing, managing, and administering of the GSA SmartPay Card Program for all three business lines (fleet, travel, and purchase) in accordance with regulations, policies, and procedures. To support the Bankcard Program in this business need, the contractor shall provide support in:
- 2.6.1 Provides the full range of financial functions for major system development and implementation.
 - 2.6.2 Defines established financial business practices for integration into the clients financial business system.
 - 2.6.3 Works with functional specialists, automation specialists, contractors, vendors, and clients to effectively translate the client's requirements into an automated application.
 - 2.6.4 Performs substantive investigative, fact-finding, data acquisition, data compilation, data analyses, issues analyses and recommends solutions to potential problems.
 - 2.6.5 Uses automated databases such as the Execution Performance and Invoice Consolidation (EPIC) to perform outline assignments and produce internal and external reports.
 - 2.6.6 Provides assistance in preparing responses to data calls and audit requests from the agency and external regulatory bodies (i.e. OIG, USM, OMB, GSA, etc.). Provides analysis and support in the Department-wide annual A-123 internal controls assessment.
 - 2.6.7 Provides assistance in preparing reports, issue papers, and correspondence pertaining to financial management of S&T travel program.
 - 2.6.8 Re-engineers, develops and implements processes, procedures and systems as necessary for employees for both domestic and international travel.
 - 2.6.9 Ensures accurate financial data in various financial and subsidiary systems, reconciles accounting and transaction data, and executes corrective action to assure data quality and consistency of the travel program.
 - 2.6.10 Processes documentation to re-allocate funds to correct imbalances and to deploy funds to meet changes in programs.
 - 2.6.11 Reviews and edits standardized operating procedures for financial management of credit card programs.

- 2.6.12 Provides guidance to credit card program stakeholders regarding execution of appropriated funds through the charge card program in accordance with Federal Acquisition Regulations and departmental policies.
 - 2.6.13 Develops analyses and projections for program managers, recommendations for general funding and budgetary changes, and enhanced documentation.
 - 2.6.14 Uses established techniques to analyze trends in receipts, obligations, and expenditures of funds to ensure efficient and effective program operations.
 - 2.6.15 Advises program manager of funding imbalances, negative projections, or indications of improper utilization of travel funds or credit cards.
 - 2.6.16 Monitors and reconciles expenditures daily, monthly, quarterly, and annually using existing systems to meet invoice processing timelines and internal control objectives.
 - 2.6.17 Applies internal control techniques and utilizes the appropriate systems to detect and report fraud, waste, and abuse to the program lead.
- 2.7 Task 7 – Travel Execution and Reporting Support (TOPS) - The Travel Operations, Policy, and Support Program (TOPS) centralizes travel preparation and support by travel experts in the CFO shop (FBD). TOPS primary goals are to. Improve the overall travel experience for the Federal Traveler. Improve fiscal oversight of S&T travel activity and operations. Support the Secretary's Travel Efficiency Initiative which targets the elimination of non-mission critical travel and the reduction of travel costs and implement streamlined processes that document these costs savings. Improve communications and policy awareness related to the conduct of official travel. To support TOPS in this business need, the contractor shall provide support in:
- 2.7.1 Prepares a manual and electronic Travel Authorization (TA) and Expense Report Requests submitted by program office travelers and invitational travelers conducting travel on behalf of a program office for both domestic and international travel.
 - 2.7.2 Submits and monitor Emergency Ticketing Requests.
 - 2.7.3 Submits and monitor Centrally Billed Account Use Requests.
 - 2.7.4 Maintains and reviews travel card status/balance/credit limit information in bank system as necessary to carry out travel support functions.
 - 2.7.5 Submits and monitor travel card limit increase requests on behalf of the traveler when necessary.
 - 2.7.6 Provides guidance to travelers regarding execution of appropriated funds through the charge card program in accordance with Federal Travel Regulations and departmental policies.
 - 2.7.7 Establishes and maintains a task tracking system to ensure business/programmatic action items and suspense dates are maintained.
 - 2.7.8 Posts actions items and suspense dates on tracking system in a SharePoint-type environment for program management review, tracking, monitoring, and reporting.
 - 2.7.9 Ensures has staff access to current processes and procedures via a SharePoint-type environment.

- 2.7.10 Ensures processes and procedures reflect industry best practices for centralized travel support services and are compliant with the latest guidance provided by the department.
 - 2.7.11 Works with functional specialists, automation specialists, contractors, vendors, and clients to effectively translate the client's requirements into an automated application.
- 2.8 Task 8 – Conference/Event Planning, Management, Execution Support - The Conference Support Role is defined as primary support to the Federal Conference POC who serves as a single point of contact for all S&T divisions for conference policies and processes, planning, approval, and data capture and analysis. To support conference and event planning in this business need, the contractor shall provide support in:
- 2.8.1 Assists S&T with implementing the federal regulations on conferences at S&T.
 - 2.8.2 Assists S&T with implementing Department conference approval process at S&T, including reviewing the process to identify areas for streamlining and efficiency in our application of the process.
 - 2.8.3 Draft communications for distribution by FBD Conference POC on conference processes and procedures, approvals, policies, etc.
 - 2.8.4 Assists S&T Division conduct market research on available conference venues, costs, a/v capabilities, etc.
 - 2.8.5 Identifies and document possible cost reductions.
Coveys DHS conference policies and procedures to S&T divisions and follows appropriate guidance for all conference, workshops, and reviews.
 - 2.8.6 Drafts conference approval process forms, and conference estimates.
 - 2.8.7 Assists S&T Divisions attain all necessary conference approvals, as per DHS Conference Approval policy.
 - 2.8.8 Liaise with Financial Analysts and Financial Officers to help answer funding questions, track PR approval process, and identify conference funding execution figures.
 - 2.8.9 Develops process, tools and system to capture estimated conference costs
 - 2.8.10 Analyzes data monthly, quarterly, and yearly to identify trends and assist with further process/policy streamlining
 - 2.8.11 Assists with preparation of response to internal and external data calls related to S&T conference activity.
 - 2.8.12 Conducts and provide ad hoc reporting and analysis.
 - 2.8.13 Develops process, tools and system to manage conferences records.
 - 2.8.14 Ensures conference files and records are current and well organized.
 - 2.8.15 Ensures records are disposed of in accordance with established policies and guidelines.
- 2.9 Task 9 – Internal Controls/Financial Audit - The Internal Controls/Financial Audit provides professional expert analysis and advice, for the management of the internal controls program, the financial audit and ensuring compliance with regulations. Regulations include (but are not limited to): OMB Circular A-123, Management's Responsibility for Internal Control (including Appendices A, B, and C), Federal Managers Financial Integrity Act (FMFIA), Improper Payments Information Act (IPIA) and Improper Payments Elimination

and Recovery Act (IPERA). Work under this task will take place seasonally from April 1 to September 30.

- 2.9.1 Assist financial managers in conducting internal assessments of internal controls of operational processes (e.g. asset management; plant, property and equipment; internal use software; and environmental financial liabilities) and producing written documentation (Test of Design (TOD), Test of Effectiveness (TOE) and a summary of aggregated deficiencies) of the assessment.
 - 2.9.2 Provide analysis and support in the Department-wide annual A-123 internal controls assessment.
 - 2.9.3 Evaluate documentation and/or statistical financial data developed in response to requests from the auditors conducting the Department's consolidated financial statement audit.
- 2.10 Task 10 - Performance - Manages the overall process for developing, monitoring, reporting, tracking, and using performance information to evaluate effectiveness and continuous improvement efforts for S&T. Serves as the liaison to the DHS Performance Team and as the Performance Improvement Officer for S&T.
- 2.10.1 Provide Performance Management SME support to S&T PPAs and programs with the creation of performance measures, milestones and targets that align to the DHS QHSR and S&T Missions, Goals and Objectives as stated in the S&T Strategic Plan.
 - 2.10.2 Provide direction/guidance to S&T PPAs and programs with regard to implementing and integrating performance measures and milestones into their programs and projects to ensure that the measures are being used to gauge program success and areas in need of improvement.
 - 2.10.3 Establish and maintain quarterly and annual status of performance measures, milestones and targets.
 - 2.10.4 Establish and maintain tracking mechanisms for updates, changes and retirement of measures at all levels (GPRA, Management, and internal) as well as milestones and targets.
 - 2.10.5 Collect complete, accurate and reliable performance data.
 - 2.10.6 Assist with the reporting on the following internal and external findings.
 - 2.10.6.1 Internal:
 - 2.10.6.1.1 Performance and Resource Review (PRR) - high-level snapshot review of current program performance information for each Division in the Science and Technology Directorate. This information includes funding status, performance metrics/targets, risk discovery, and to highlight Division achievements and any issues/challenges that the Division is currently experiencing with regard to funding, contracts, performance, etc.
 - 2.10.6.2 External:
 - 2.10.6.2.1 Quarterly Performance Updates – data call sent to all Divisions in the form of spreadsheets that track the Division(s) performance measures and targets for each

quarter progress toward their annual target. This information is entered into the FYHSP system at the end of the quarter.

- 2.10.6.2.2 Annual Performance Updates - data call sent to all Divisions in the form of spreadsheets that track the Division(s) performance measures and targets for end of year results for meeting their annual target established the beginning of the fiscal year. This information is entered into the FYHSP system at the end of the fourth quarter.
- 2.10.6.2.3 QFRs – Provide input or review material for S&T leadership including presentations, testimony, Questions for the Record, etc. for Hearings, briefings, or meetings with Congressional Members and/or staff with regard to S&T Performance.
- 2.10.6.2.4 Strategic Context – Provide DHS with a strategic overview of S&T's organization of Divisions and how its resources and performance contribute/align with the DHS Missions, Goals and Objectives.
- 2.10.6.2.5 Congressional Justification (CJ) – Provide input to the S&T CJ with regard to established measures and milestones captured and maintained in the system of record for DHS, FYHSP.
- 2.10.6.2.6 APR – Provide input to the DHS APR with regard to all S&T measures, milestones, targets for the fiscal year. Provide review of information and updates as necessary.
- 2.10.6.2.7 ~~AFR~~ – Review all portions of the AFR for accuracy and completeness with regard to S&T's data and submissions.
- 2.10.6.2.8 DHS Summary Report (formerly Citizen's Report) – Provide input and review of the DHS Summary Report for accuracy and completeness with regard to S&T's data and submissions.
- 2.10.6.2.9 Statement of Assurance – Complete and submit the S&T Statement of Assurance on behalf of S&T to the Budget Formulation Team as well as DHS PA&E. This purpose of this form is for each component in DHS to ensure the reliability and accuracy of all the performance data, for that component, that is published in the APR. These along with a Memo signed by each component head is sent to S1 with the APR submission.

2.10.7 Coordination/Liaison:

- 2.10.7.1 Provide management and maintenance of the Performance Team Mailbox. Ensuring that all emails that come in are answered and filed appropriately.
- 2.10.7.2 Attend the monthly DHS Performance Team meetings.

- 2.10.7.3 Provide input and guidance to the open government working group on efforts and data that is available for release to the public that fits the needs of the working group.
- 2.10.7.4 Provide assistance and guidance within the CFO to other Branches/Divisions when requested or warranted.
- 2.10.7.5 Prepare and present performance workshops for senior executives within S&T.

2.10.8 Training

- 2.10.8.1 Provide assistance and guidance on Performance Management within the Directorate.
- 2.10.8.2 Provide performance training and guidance within the CFO to other Branches/Divisions when requested or warranted

2.11 Task 11 – Front Office Support - To support the front office in this business need, the contractor shall provide support in:

- 2.11.1 Provide routine administrative support to the FBD senior management team and branch chiefs.
- 2.11.2 Provide analytical and program support to FBD by preparing financial reports, presentations, graphs, tables and charts.
- 2.11.3 Review and edit documents for grammar and content.
- 2.11.4 Provide additional program support to all FBD offices as required during peak performance periods.
- 2.11.5 Serve as Share Point Administrator for FBD, posting service bulletins, calendar items, Director's newsletters, and other documents, as needed.

2.12 Task 12 – Task order management and Surge - To support FBD in this business need, the contractor shall provide support in:

- 2.12.1 Provide on-site contract management.
- 2.12.2 Provide surge personnel on as needed basis to support FBD offices as required during peak performance periods.

3.0 KEY PERSONNEL

The contractor shall provide resumes of all key personnel designated in this SOW. The contractor shall notify the CO and COR prior to making any change in the individuals identified in the proposal and/or assigned to this contract. All substitutions must be submitted in writing to the CO and COR at least fifteen (15) days in advanced of the proposed substitution. All requests for substitution must include a detailed explanation of the circumstances necessitating the proposed substitution. Requests for substitution shall include a complete resume of the proposed substitute and any other information required by the CO or COR which is necessary to approve or disapprove the proposed substitution. The contractor shall demonstrate that the qualifications of the substitution are equal to or better than the qualifications of the personnel being replaced. The CO and COR will evaluate such requests. The COR will recommend and the CO will approve or disapprove substitutions and promptly notify the contractor of the Government decision in writing. Note: The Government may designate additional Contractor personnel as Key at the time of award.

As identified by the requirements in section 2.0 above, key labor categories needed to support the Finance and Budget Division requirements include:

Key Personnel - Program Manager

4.0 CONTRACTOR PERSONNEL

4.1 Quality Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this PWS. Historically, successful completion of these tasks have been achieved with the below personnel.

Labor Category	Task	Proposed Hours
Subject Matter Expert (Senior)	2.1	2080
Subject Matter Expert (Junior)	2.1	1040
Subject Matter Expert (Junior)	2.1	1040
Analyst (Intermediate)	2.2	2080
Analyst (Intermediate)	2.2	2080
Analyst (Junior)	2.3	2080
Analyst (Intermediate)	2.3	2080
Analyst (Intermediate)	2.3	2080
Analyst (Senior)	2.4	2080
Analyst (Junior)	2.4	2080
Analyst (Intermediate)	2.4	2080
Analyst (Senior)	2.5	2080
Analyst (Intermediate)	2.5	2080
Analyst (Intermediate)	2.6	2080
Analyst (Intermediate)	2.7	2080
Analyst (Intermediate)	2.7	2080
Analyst (Senior)	2.7	2080
Analyst (Junior)	2.7	2080
Administrative Clerk III	2.7	2080
Administrative Clerk III	2.7	2080
Administrative Clerk III	2.7	2080
Analyst (Intermediate)	2.8	2080
Analyst (Intermediate)	2.9	1040
Analyst (Senior)	2.10	2080
Analyst (Senior)	2.11	2080
Analyst (Intermediate) Surge	2.12	2080
Analyst (Intermediate) Surge	2.12	2080
Task Order Project Manager (Intermediate)	2.12	1040

4.2 Employee Identification

4.2.1

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

4.2.2

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

4.3 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

4.4 Removing Employees for Misconduct or Security Reasons

The Government may at the discretion of the Contracting Officer direct the contractor to remove any contractor employee from DHS facilities for misconduct. Removal of a contractor employee does not relieve the contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the contractor with a written explanation to support any request to remove an employee.

4.5 Non-Disclosure Agreements

All contractor personnel are required to sign non-disclosure agreements (DHS Form 11000-6) upon starting work and as deemed necessary under this contract to protect proprietary and/or source selection information.

4.6. CONTRACTOR MANAGEMENT

The contractor shall apply the management, human resources, and organizational skills, techniques, practices, and methodologies required to support and effect highly successful performance of this effort.

The contractor shall provide a Contract Management Plan at time of award that, at a minimum, describes the overall approach to management as well as the specific approaches to transition in and out of this effort (including bringing on board fully cleared staff in a timely manner). This

plan shall also address recruitment and retention, risk management, and subcontractor management.

The Contract Management Plan shall identify what subcontractors will be part of the offeror's team, what tasks each subcontractor will perform, and what percentage of the total effort each subcontractor will be responsible for.

5.0 OTHER APPLICABLE CONDITIONS

5.1 SECURITY

Contractor access to classified information is required under this SOW. The maximum level of classification is SECRET. Details will be provided in a Department of Defense (DD) Form 254.

The contractor shall have a facility security clearance up to SECRET level. All personnel supporting this PWS shall be required to obtain and maintain a SECRET level clearance. The Government reserves the right to approve or deny suitability of the contractor's individual employees based on security risks, unsatisfactory performance, or disruptive influence to mission accomplishment.

DHS has and will exercise full control over granting, denying, withholding, or terminating unescorted Government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and make a favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the contractor to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full suitability authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order. No employee of the contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the DHS Office of Security. Contract employees assigned to the task order not needing access to sensitive DHS information or recurring access to DHS facilities will not be subject to security suitability screening. Contract employees waiting and EOD decision may not begin work on the task order. Limited access to Government buildings is allowable prior to the EOD decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend briefings, non-recurring meetings, and begin transition work.

Classified information is Government information which requires protection in accordance with Executive Order 12958, National Security Information (NSI) as amended and supplemental directives. If the contractor has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. If the contractor is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

Contractor shall comply with all government facility and security requirements while on government property, including obtaining and displaying identification badges, obtaining vehicle decals and proper vehicle operation.

All services provided under this task order must be compliant with DHS 4300B DHS National Security System Policy and the DHS 4300B National Security System Handbook. Additionally, where there is a requirement for encryption, all encryption shall be FIPS 197 Advanced Encryption Standard (AES) that has been FIPS 140-2 certified.

Requirements for Handling Sensitive and/or Proprietary Information. The contractor shall comply with all government standards for handling sensitive and/or proprietary information, as listed on the DD254 and briefed by S&T.

5.2 PERIOD OF PERFORMANCE

The period of performance for this contract is a one-year base period with one one-year option period and one six month option period as follows:

Base Period	Date of Award to 12 months from date of award
Option Period One	12 months from end of Base Period
Option Period Two	End of Option Period One through February 6, 2015.

5.3 PLACE OF PERFORMANCE

The work will be performed at a Government site as directed by the CO and/or the Contracting Officer's Representative (COR). Audits, assessments, attendance at meetings and symposia will most likely require travel to S&T sites and other locations both federal and private. Classified work will be done at the government location only.

5.4 HOURS OF OPERATION

When working on Government sites, normal duty hours are 8:00 am - 5:00 pm, Monday through Friday (except Federal holidays). Overtime will not be permitted under this task order, unless authorized in writing by the COR.

In the event of a shutdown for any reason (including, but not limited to, Government closures due to inclement weather or other public emergency, building closures due to lack of power or water, and additional Government holidays granted by the President), the Government will not be liable for Contractors' costs incurred during this period except to the extent agreed in advance and in writing by the COR or CO.

5.5 TRAVEL

Domestic and international travel may be required in connection with this task order. All domestic and international travel requires the advanced written approval of the Task Order Contracting Officer's Representative (COR). Travelers are required to submit a summary trip report to the TO COR within five working days following the completion of travel. Travel shall be in accordance with the Federal Travel Regulation.

5.6 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 7 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract.

The Post Award Conference will be held at the Government's facility, located at 1120 Vermont Avenue NW, Washington, DC 20005, or via teleconference.

5.7 DELIVERABLES

5.7.1 Reports

5.7.1.1 Monthly Progress Reports - The Contractor Project Manager shall provide a monthly progress report to the Contracting Officer and COR via electronic mail and two hard copies to the COR. This report shall provide monthly cost and performance reporting of all assigned tasks. The contents and formats of the reports shall be specified in the Contract Management Plan. At a minimum, these reports shall include: highlights of support provided, expenditures, projected expenditures for the next reporting period and to term, and major issues affecting cost and performance. The costs portion of the report shall be structured to enable ready discernment of cost trends, projections, and variances. The Program Manager shall be qualified to act as the Contractor's single point of contact for all technical and administrative matters related to this task order. If more than one task order is awarded, the reports will be consolidated. This report shall also include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

5.7.1.2 Transition In plan - The Contract Project Manager shall provide a transition in plan to the Contracting Officer and COR via electronic mail and two hard copies to the COR. This plan shall address the contractors plan for minimizing impact such that continuity of services will be maintained without disruption. The contractor shall describe how it will achieve full staff support levels within 60 days of award. This report is due 7 business days after award of contract.

5.7.1.3 Transition Out plan - The Contract Project Manager shall provide a transition out plan to the Contracting Officer and COR via electronic mail and two hard copies to the COR. This plan shall address the contractors plan for minimizing impact such that continuity of services will be maintained with disruption. The contractor shall describe how it will transition work to the new contractor. This report is due 120 days before the expiration of the contract.

5.8 PROGRESS MEETINGS

The Contractor Project Manager shall be responsible for keeping the COR informed about Contractor progress throughout the performance period of this contract, and ensure Contractor activities are aligned with DHS objectives. At a minimum, the Project Manager shall review the status and results of Contractor performance with the COR on a monthly basis at scheduled meetings. These meetings shall be both working and formal sessions to review overall program efforts.

5.9 GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications) in accordance with Deliverables Table cited in Paragraph 10.0.

5.10 PROTECTION OF INFORMATION

Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6). Additionally, contractors must comply with FAR 9.505-4(b) and provide the Contracting Officer with copies of any company to company agreements for the contracting officer to ensure that they are properly executed.

5.11 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then “1194.21 Software” standards also apply to fulfill functional performance criteria.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 – Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional

Performance Criteria", they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards.

When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

5.12 Limitation on Contractor Data Rights

The Contractor shall not use, release to others, reproduce, distribute, or publish the data deliverables or any data first produced in the performance of this contract without first receiving approval from the COR.

For the purposes of paragraphs (b)(2)(i) and (d) of the Rights in Data-General (FAR 52.227-14) clause of this contract, the Contractor shall not use, release to others, reproduce, distribute, or publish any data first produced or specifically used in the performance of this contract for private purposes without the prior, written approval of the Contracting Officer.

5.13 Advertisements, Publicizing Awards, and News Releases

All press releases or announcements about agency programs, projects, and contract awards need to be cleared by the Program Office and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the Program Office and the Contracting Officer.

6.0 GOVERNMENT TERMS & DEFINITIONS

- 6.1 AQL – Acceptable Quality Level
- 6.2 AFR – Annual Financial Report
- 6.3 APR – Annual Performance Report
- 6.4 PRR – Performance and Resource Review
- 6.5 PPA – Program Project Activity
- 6.6 CO – Contracting Officer
- 6.7 COR – Contracting Officer's Representative
- 6.8 DHS – Department of Homeland Security
- 6.9 DOE – Department of Energy
- 6.10 EOD – Entry on Duty
- 6.11 EPIC – Execution Performance Invoice Consolidation database
- 6.12 FAR – Federal Acquisition Regulation
- 6.13 FBD – Finance and Budget Division
- 6.14 FFMS – Federal Financial Management System
- 6.15 FIN OPS – Financial Operations
- 6.16 FMFIA – Federal Managers Financial Integrity Act
- 6.17 FOUO – For Official Use Only
- 6.18 FTE – Full Time Equivalent
- 6.19 FTR – Federal Travel Regulation
- 6.20 FY – Fiscal Year
- 6.20 FYHSP – Future Year Homeland Security Plan
- 6.22 GPRA – Government Performance Results Act
- 6.23 GOTS – Government Off-the-Shelf
- 6.24 GSA – General Services Administration
- 6.25 IA – Interagency Agreement
- 6.26 ICE – Immigration and Customs Enforcement
- 6.27 IPAC – Intra Governmental Payment and Collection
- 6.28 IPERA – Improper Payments Elimination and Recovery Act
- 6.29 IPIA – Improper Payments Information Act
- 6.30 IT – Information Technology
- 6.31 MD – Management Directive
- 6.32 OCFO – Office of the Chief Financial Officer
- 6.33 OFM – Office of Financial Management
- 6.34 OGC – Office of General Counsel
- 6.35 OIG – Office of the Inspector General
- 6.36 OPO – Office of Procurement Operations
- 6.37 POC – Point of Contact
- 6.38 PI – Performance Institute
- 6.39 PIC – Performance Improvement Council
- 6.40 PM – Program Manager
- 6.41 PR – Purchase Request
- 6.42 PRS – Performance Requirements Summary
- 6.43 RFP – Request for Proposal
- 6.44 R&D – Research & Development
- 6.45 RDT&E – Research Development Test & Evaluation
- 6.46 PA&E – Program Analysis and Evaluation
- 6.47 PWS – Performance Work Statement
- 6.48 SF – Standard Form
- 6.49 S&T – Science and Technology Directorate

- 6.50 SME – Subject Matter Expert
- 6.51 SOP – Standard Operating Procedure
- 6.52 SP2 – Standardized Policies and Procedures
- 6.53 SSI – Security Sensitive Information (Sensitive but Unclassified Information)
- 6.54 TA – Travel Authorization
- 6.55 TMO – Travel Management Office
- 6.56 TOE – Test of Effectiveness
- 6.57 TOD – Test of Design
- 6.58 TOPS – Travel Operations, Policy and Support Program
- 6.59 USM – Undersecretary for Management
- 6.60 V&V – Verification and Validation

7.0 GOVERNMENT FURNISHED RESOURCES

DHS will provide information, materials, and forms unique to DHS to the vendor to support certain tasks under this PWS. These will be task specific and issued upon task commencement or as needed during task performance.

The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this contract, and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear. Government resources to be provided are as follows:

- Office spaces, computers, telephone, equipment, and supplies deemed necessary by the Government to execute this work.
- Hardware, software, database, and documentation support deemed necessary by the Government to execute this work.

The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract, and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the period of performance. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

7.1 MATERIALS

Contractor purchased materials shall be required to support this requirement. All materials required in the performance of this contract by the Government will be for the marketing and presentation needs of the FBD.

8.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in SOW 7.0 and SOW 8.0.

9.0 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

9.1 The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have an opportunity to correct the rejected deliverable and return it per delivery instructions.

9.2 The COR will have 5 business days to review deliverables and make comments. The Contractor shall have 5 business days to make corrections and redeliver.

9.3 All other review times and schedules for deliverables shall be agreed upon by the parties. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

10.0 DELIVERABLES SUMMARY TABLE

DELIVERABLES	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	5.7.1.1	Monthly Progress Report	By the 15th of each month.	Two hard copies shall be provided to the Contracting Officer's Representative (COR) and one electronically submitted copy shall be provided to the COR and CO. Delivered to: Jennifer Hatten, COR, Science and Technology Directorate 1120 Vermont Ave. Washington, DC 20005. Room 5-131 (Jennifer.Hatten@hq.dhs.gov) and (Janice.Brinkly@hq.dhs.gov)
2	5.7.1.2	Transition In Plan	7 days after award of contract.	Two hard copies shall be provided to the Contracting Officer's Representative (COR) and one electronically submitted copy shall be provided to the COR and CO. Delivered to: Jennifer Hatten, COR, Science and Technology Directorate 1120 Vermont Ave. Washington, DC 20005. Room 5-131 (Jennifer.Hatten@hq.dhs.gov) and (Janice.Brinkly@hq.dhs.gov)
3	5.7.1.2	Transition Out Plan	120 days before expiration of period of performance.	Two hard copies shall be provided to the Contracting Officer's Representative (COR) and one electronically submitted copy shall be provided to the COR and CO. Delivered to: Jennifer Hatten, COR, Science and Technology Directorate 1120 Vermont Ave. Washington, DC 20005. Room 5-131 (Jennifer.Hatten@hq.dhs.gov) and (Janice.Brinkly@hq.dhs.gov)

11.0 POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

11.1 The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process background investigations and suitability determinations, as required, in a timely and efficient manner.

11.2 Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

11.3 Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security/PSD. Prospective Contractor employees shall submit the following completed forms to the DHS Office of Security/PSD. The Standard Form (SF) 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Office of Security/PSD no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- a. Standard Form 85P, "Questionnaire for Public Trust Positions"
- b. FD Form 258, "Fingerprint Card" (2 copies)
- c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
- d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon award of the contract.

11.4 DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

Contractor employees waiting for an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings in order to begin transition work.

11.5 The DHS Office of Security/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be

returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

11.6 When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

11.7 Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.

11.8 DHS S&T Security Office POC:

DHS S&T Security

Washington DC 20005

Telephone: (202) 254-XXXX

12.0 SURGE RESPONSE

The Contractor shall provide additional support under the task areas described in this Statement of Work (SOW) during emergency/critical operations as described in Section 2.12, Task 12. This task shall be reimbursed on a Labor Hour basis subject to the labor categories and hourly rates contained in the pricing schedule and the terms of the modification authorizing the work.

The Government may exercise the surge CLIN optional tasks by written notice to the Contractor within 5 business days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 5 business days before the contract expires. The preliminary notice does not commit the Government to an extension.

If the Government exercises this optional surge, the extended contract shall be considered to include this option clause.

13.0 TRANSITION IN

The transition-in phase shall identify those actions, plans, procedures, and timelines necessary to ensure a smooth transition from contract start date to full operational status by the Contractor. The Contractor shall continue to perform contract requirements during the period between the initial decision date and completion of the phase-in transition period. The Government will provide the Contractor office space and telephone access as available. The phase-in transition period shall begin at date of contract award and shall conclude 60 days later. Upon completion of the phase-in transition period, the contractor shall assume full operating accounting and responsibility. The transition-in period may be extended in order to ensure an orderly draw down of outgoing personnel and ramp up of incoming personnel.

14.0 Contract Clauses**14.1. FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This task order incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. These clauses are in addition to clauses already in the PACTS contract. The full text of a clause may be accessed electronically at this address:
<https://www.acquisition.gov/far/index.html>.

14.2 FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSES AND PROVISIONS INCORPORATED BY REFERENCE.

- a) FAR 52.203-16, Preventing Personal Conflicts of Interest (Dec 2011)
- b) FAR 52.204-2 Security Requirements (Aug 1996)
- c) FAR 52.217-9 Option to Extend the Term of the Contract. (Mar 2000) [insert "5 days" in both blanks in para. (a) and "29 months" in para. (c)]
- d) FAR 52.222-54, Employment Eligibility Verification (Jul 2012)

14.3 U. S. DEPARTMENT OF HOMELAND SECURITY ACQUISITION REGULATION (HSAR) CLAUSES INCORPORATED IN FULL TEXT.**HSAR 3052.204-70 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)**

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include—

- (1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
- (2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).
- (d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.
- (e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

**HSAR 3052.209-72 Organizational Conflict of Interest
(JUN 2006)**

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting is that contractors working onsite at the Government facility may have access to non-public information regarding an upcoming solicitation.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

HSAR 3052.209-73 Limitation of Future Contracting (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict is that contractors working onsite at the Government facility may have access to non-public information regarding an upcoming solicitation.

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

HSAR 3052.215-70 Key Personnel or Facilities (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract:

Program Manager, Marcel Winner

(End of clause)

HSAR 3052.242-72 Contracting Officer's Technical Representative (Dec 2003).

The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract, such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the Contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

COTR

Name: Jennifer Hatten
Phone No: 202-254-8245
E-mail Address: Jennifer.Hatten@hq.dhs.gov

(End of clause)

EXAMINING CHALLENGES AND ACHIEVEMENTS AND ADDRESSING EMERGING THREATS

WEDNESDAY, SEPTEMBER 11, 2013

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:30 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senators Carper, Pryor, Baldwin, Coburn, Johnson, Ayotte, and Chiesa.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. Well, welcome one and all to this important hearing.

Today marks the 12th anniversary of September 11, 2001. Coming down on the train today, Dr. Coburn and colleagues, I was reminded that 12 years ago exactly to this day, to the hour, to the minute, what was going on in our lives. So it is a very poignant day, a sad day, but a day that is not without hope. But it is a day for reflection—not only a day that we lost a lot of our fellow Americans, but a day that brought with it a sense of unity that we do not often see in this town and in this country in the wake of a terrible tragedy.

There is going to be a moment of silence a bit later, I think observed here in the Capitol. I am going to ask us just to start this hearing with a moment of silence, and then I will introduce our witnesses and make some statements and begin. But if you will just pause now for a moment of silence, please.

[Moment of silence.]

Thank you.

One of the things that our chaplain—some of you know our chaplain, Barry Black, a retired Navy Admiral. He always encourages us to pray for wisdom, each and every one of us in our own way, and that is probably a good thing for us to remember on this day.

This anniversary also provides us with an important opportunity to think about all the efforts we have taken to secure our country since that fateful day, as well as the challenges that lie ahead.

With us today we have just a remarkable group of witnesses that will share their thoughts, their counsel, on what we have accomplished since September 11, 2001, and the future of homeland secu-

city. We are just honored that each of you are here and delighted that you would come, and thank you so much for joining us and really for your service, your extraordinary service, to our country.

This year, the Department of Homeland Security (DHS) turned 10 years old. And while I am sure we can all agree that the Department can do a better job in certain areas, we should not forget about the remarkable progress that has been made in keeping Americans safer since Tom Ridge helped to open the door of that new Department those many years ago. There is no doubt, in my view, that we are safer today than we were 10 years ago in spite of greater threats to our Nation and to our well-being.

I want to take a couple minutes to highlight some of the more significant accomplishments, if I could.

We have enhanced aviation security through a more risk-based, intelligence-driven system that begins screening passengers against national security databases roughly 4 days before they ever board an aircraft.

We have improved our preparedness for and our ability to respond to disasters while cutting red tape at the Federal level.

We saw the fruits of these efforts in the response following the Boston Marathon bombings and also the natural disasters that struck my part of the country, including Hurricane Sandy.

We have increased the security of our Nation's borders with historic levels of manpower and resources.

And we have built up cybersecurity capabilities to work with the private sector and Federal Government agencies in preparing for, responding to, and mitigating against the ever-growing number of cyber attacks.

But is there still room for more improvement? And I would just say you bet there is. One of my favorite sayings is, "The road to improvement is always under construction." And that is true in this venue as well. One way the Department can improve is by doing a better job of preparing for tomorrow's threats today.

We do a pretty good job in this country at fighting the last war and preparing for the last type of attack, but to secure our homeland we must do an even better job at anticipating the next kind of attack that we will face. Ten years ago, for example, relatively few people were even talking about or thinking about cybersecurity. Some were, but a lot were not. Today we can hardly go a day without reading about a cyber attack or hearing about a cyber attack in the news, oftentimes many attacks.

To respond to the challenge of ever-changing threats, we need a Department of Homeland Security that is flexible and ready to adapt when necessary. And sometimes we just need to use some common sense. If a program is not working, we should not just keep throwing good money after bad. Rather, we must work smarter with our limited resources and find ways to get even better results for less money or for the same amount of money.

That is why Dr. Coburn and I are holding this hearing and a series of others. Actually, at the beginning of this year, he suggested that we focus on reauthorization. We have never done a reauthorization of the Department of Homeland Security. He suggested that maybe a good way to do that would be to do a year-long series of hearings that are relevant to the Department and its functions and

looking forward. And this is one of those hearings, and a really important one.

We are doing this top-to-bottom review of the Department so we can learn from instances where the Department succeeded and where it came up short. And this information will help us to better focus our scarce resources on what works.

As the Committee conducts this review process, we will be looking to ensure that the Department is making smarter acquisition decisions, developing an even more agile and capable workforce, and improving its financial management systems. This review will also look at how we can strengthen the defenses of our homeland against very sophisticated and highly agile threats.

One of the most important things we can do to improve homeland security is to come together to pass cybersecurity legislation, either in pieces or together as a comprehensive policy, a comprehensive approach for our country. The threat is too great and the consequences of inaction are too severe to do nothing. Enacting a thoughtful, comprehensive cybersecurity policy has not been easy, as we know. But we have a shared responsibility—both Democrats and Republicans, House and Senate, government and industry—to get this legislation across the goal line and into the end zone hopefully this year.

We already saw many of the different parties come together to pass comprehensive immigration reform in the Senate a few months ago.

I do not agree with everything in that bill, and I know my colleague here, Dr. Coburn, and I suspect Senator Johnson do not agree with everything either. But I believe the approach that we have taken in the Senate is vastly preferable to our current immigration system, the failings of which undermine both our national and economic security. It is my hope that the House will pass its own version of immigration reform so we can go to conference, make it even better, and pass the kind of historic piece of legislation that our country needs.

So as we remember 9/11 and discuss the challenges that lie ahead, we must seek to recapture that spirit of unity that prevailed 12 years ago today, and we need that if we are going to succeed in making not just the Department of Homeland Security stronger over the next 10 years but our Nation stronger going forward into the future.

So I look forward to working with Dr. Coburn and with our colleagues, even Senator Johnson over here, who is so good at coming to our hearings. He is always faithful in attendance and asks good questions. And we look forward to working with the Administration, with our witnesses, and a whole lot of other folks that are going to help us figure out how to do this job of shared responsibility better.

So with that having been said, let me turn it over to Dr. Coburn for any comments he wants to make. Thank you.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Thank you, Senator Carper. I have a statement that I will place in the record.

I have a lot of concerns with Homeland Security. One of the editorials that was in the New York Times today talked about the lack of focus on multiple committees—the focus on multiple committees instead of single committees of jurisdiction, and I know it is difficult for Homeland Security to answer all the questions from the 88 different committees and subcommittees that they have to answer to. And that is one of the things that we ought to be about changing because our frustrations are we cannot ever get answers. And I am sure it is not always intentional that we do not get answers. Sometimes it is, but it is because we are asking so much information all the time where the people who actually have responsibility at Homeland Security cannot do their job because they are busy answering questions of Members of Congress. So the disorganization.

The other concern I have with Homeland Security is it has turned into an all-hazards agency, which was never its intent. And it has abandoned risk-based policies to put money where risk is rather than money where risk is not. And the politicians in Washington have very much accounted for that.

In my opening statement that I will put in the record, there are a large number of areas where we are incompetent, whether it is in terms of either metrics or effectiveness, and we have not held the hearings that are necessary to straighten that out.

I would welcome all of our panelists. Thank you for your service in multiple areas for our country. And I hope that you can give us some wisdom—I have been through your testimonies. I hope that you can give us some wisdom how to streamline and not undermine the goal and the long-term changes that need to be made in Homeland Security to get us back to a risk-based agency instead of a grab bag of political benefits agency.

The final point I would make is that transparency is important, and the difficult job you had, Governor Ridge, in terms of bringing all these agencies together. We have had good Homeland Security Directors and Secretaries, but the idea that you can effectively manage this—and we have all the data to say that we are not effectively managing it. And so my hope today out of this hearing is that we will hear some great ideas on how you change the structure.

And the final point I would make is we have 15 of the top 17 positions at Homeland Security open, and to my knowledge, we only have two nominees pending in that area. And I may be wrong. That is my guess. I think we have two.

So leadership matters, and having people in positions instead of acting people in positions is very different in terms of accomplishing the goals that need to be accomplished at Homeland Security.

So I welcome you, thank you, and look forward to your testimony.

Chairman CARPER. Thank you. Thank you, Dr. Coburn.

Before I introduce our witnesses, I will just note, if I could, that at 11 o'clock there is going to be a gathering of Members of Con-

gress and former Members of Congress, I think on the east steps of the Capitol, for an observance. And my hope is that we would work right up to just before that time, and hopefully we will be in a position to conclude, to adjourn; and if not, I may ask to adjourn fairly briefly but come back in about half an hour. Hopefully we can be done. I know at least one of you has a tight schedule herself.

All right. I want to just briefly introduce our first, or not so briefly, the first witness. Tom Ridge and I came to the House together in 1983, 30 years ago today. We were both in our mid-twenties, maybe early twenties. But we both served in the Vietnam War together, he with real distinction, as just a hero, and very modest about it. But we ended up on the Banking Committee together, and I think in the 102nd Congress, I think we ended up leading—on the Banking Committee, we had a Subcommittee on Economic Stabilization, and people said to me in the past years, “Tom, what did you accomplish in those 2 years that you and Tom Ridge led that Committee?” I said, “We laid the foundation for the longest-running economic expansion in the history of the country.” And we stepped down from our responsibilities in 1993 and we were on our way to 8 glorious years. He went on after that to become Governor of Pennsylvania, our neighbor to the north, and the first Secretary of the Department of Homeland Security.

Since stepping down as Governor, he has not only led the Department, but he has also served as chairman of the National Security Task Force at the Chamber of Commerce and on boards of the Institute of Defense Analysis, the Center for Studies of the Presidency and Congress, and chairman of the National Organization on Disability. Meanwhile, he travels the world as head of his firm, Ridge Global, and any number of other entities. Somewhere along the line, he found time to convince a woman named Michele to marry him, and they have two wonderful kids that we have been privileged to know, Leslie and Tommy.

We are delighted to see you and thank you for your friendship and thank you for your extraordinary service to our country.

Next I want to welcome Jane Harman, former Congresswoman from California’s 36th District. During her tenure in the House of Representatives, Congresswoman Harman distinguished herself as one of the top national security voices in the House, serving on the House Armed Services Committee and the Intelligence and Homeland Security Committees. She was also one of the principal authors of the Intelligence Reform and Terrorism Prevention Act of 2004. Congresswoman Harman now serves as the Director of the Woodrow Wilson Center. She is also a member of the External Advisory Board for the Department of Defense (DOD), State, and the Central Intelligence Agency (CIA), and does a million other things. So it is great to see you. We welcome you warmly.

Our next witness is in his civvies today, with facial hair, and I was kidding him earlier. I would not have recognized you had I not known it was you and that you were coming today. But it is great to see you. You are a hero in this country, a hero in the Coast Guard, and in the Department of Homeland Security. I have enormous respect and affection for you, as you know. Thank you for all that service. I wish you well as, I understand, the executive vice president at Booz Allen Hamilton, and we are happy for you for

that opportunity, well deserved. But in the Coast Guard, Admiral Allen led the effort to respond to and recover from Hurricane Katrina after the first couple of weeks of the initial response as well as the Deepwater Horizon oil spill. And for that service and a million other things that you have done and continue to do, we welcome you. I want to thank your family for allowing you to serve our country and share you with all of us.

The final witness is Stewart Baker battling cleanup, former Assistant Secretary for Policy at the Department of Homeland Security, a partner—are you partner now?—at Steptoe & Johnson here in D.C. I understand you have a book out. You are the author of a book. I love this title: “Skating on Stilts: Why We Aren’t Stopping Tomorrow’s Terrorism.” Good luck with that.

In his position, Mr. Baker established the Department’s Policy Office. He led successful negotiations with foreign governments over data sharing, privacy, and visas, and established a secure visa-free travel plan. What years did you serve in the Bush Administration?

Mr. BAKER. 2005 to 2009.

Chairman CARPER. OK. Thank you for that. And I want to again thank all of you for being here. Your entire statements will be made part of the record, so feel free to testify. We are going to lead off, I believe, with Governor Ridge, and I just want to say to Senator Chiesa, nice to see you. Welcome. Always a pleasure. He is the Senator from New Jersey whom you may or may not know. He is a great addition to this Committee and to this body.

Governor. Congressman.

TESTIMONY OF THE HON. TOM RIDGE,¹ PRESIDENT AND CHIEF EXECUTIVE OFFICER, RIDGE GLOBAL, AND FORMER SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. RIDGE. Thank you very much. Good morning to my former colleague and my friend, Tom Carper. It is a great pleasure to appear before you and Senator Coburn.

As they say, let me associate myself with the gentleman’s remarks with regard to a risk-based approach, with regard to consolidating the incredible labyrinth of the jurisdictional maze that the Secretary and his or her Department have to continually respond to up here on the Hill. It was one of the recommendations of the 9/11 Commission, and 10 years later, that one and the other recommendation they made was with regard to a broadband public safety network. That is 10 years in the making. There is some legislation. We are a long way from execution. So I really appreciate your words in those regards. And to the other Members of the Committee, it is a great pleasure for me to spend this morning with you on this very historic and very important day.

I appear before you in my wonderful personal capacity as a private citizen as well as the chairman of the U.S. Chamber of Commerce’s National Security Task Force. The task force is responsible for the development and implementation of the Chamber’s homeland and national security policies. Frankly, it is a voice for businesses across America. It certainly informs my perspective on

¹ The prepared statement of Mr. Ridge appears in the Appendix on page 492.

many issues, but it does not dictate it because my work there is strictly voluntary. I am neither a lobbyist nor a paid advocate, but we do have certain views that we share, and I am happy to advocate when we share them.

I welcome the opportunity to appear here to examine ways in which we can secure America's future. Since we have limited time, I would ask permission to revise and extend my remarks.

Before I begin I want to, on this anniversary, acknowledge the families that lost loved ones on September 11th. We all know where we were. I had the opportunity to visit Shanksville a couple of hours after the plane went down.

So the reason we are here is to work together and to do our best to ensure that such events do not happen again and that other families do not have to suffer like the families of our 9/11 heroes.

With your indulgence, I would like to make a few general observations first and then focus on what I believe is a cross-cutting issue that both DHS and the broader Federal Government has faced in the past and has the potential to complicate our security forevermore.

First of all, briefly, it is becoming clear that members of this body intend to pass some form of immigration reform. I think that is relevant to homeland security. DHS components can be expected to play a significant role in implementing these reforms. My position is that the time has come to grant status to those who wish to enter to our country legally, to work lawfully, to pay taxes, and deal with the issue that we have talked about for 10 years, and that is, the undocumented individuals who are here. I think it can be done. I hope this Congress does it. But I also think Congress has to balance this responsibility with providing adequate resources to the Department of Homeland Security in order to affect the outcomes that the broader American public want to achieve. We can talk about reaching consensus in Washington, but unless any reforms are resourced appropriately, DHS components will be saddled with an impossible mission in the critical area of border security.

I am not going to discuss my deep and abiding concern about the number of critical senior-level vacancies at DHS. It has been addressed. It is disconcerting that an agency, if it is perceived by our government, the U.S. Government, to be as important as I believe it is, to have 15 vacancies, or whatever the number is, at any time. And yet these vacancies have lasted for quite some time. You are aware of it. I just urge the administration to fill the vacancies quickly and the Senate in a judicious manner and timely manner to exercise the advice and consent responsibilities and fill these positions.

Let me spend the rest of my time discussing the challenges of information sharing, which I think goes to the heart of Homeland Security's responsibility. We do not generate intelligence. We are assigned from the get-go the enabling legislation to share it and provide whatever defensive measures we need to protect America.

Information sharing is an issue that has been with us since September 11, 2001, and cuts across a range of challenges that have and will continue to confront the dedicated men and women of Department of Homeland Security. We all know the nature of the ter-

rorist threat has changed. As we have seen in Iraq, Afghanistan, and today in Syria, our enemy is no longer just al Qaeda, but like-minded organizations and nation states that are willing to ally themselves in order to harm their common enemy—the United States. In my opinion, this will require the intelligence community to renew its commitment to work more closely with one another than ever before. Congress in its oversight role should ensure that DHS specifically remains plugged into the Federal intelligence community horizontal across the board. For if intelligence indicates a physical or cybersecurity threat against the homeland, DHS by enabling legislation is the agency required to work with our partners along the vertical—required to work with the State and locals, required to work with the private sector. That is embedded in the enabling legislation. Further, we should ensure that the great progress that has been made for information sharing with our State and local partners—such as the establishment of fusion centers—continues to be nurtured.

No discussion of the DHS threat environment or about information sharing can be complete without discussing cybersecurity in greater detail. There is no part of our national economy, infrastructure, or social fabric that is not in some way connected to the Internet backbone—our critical power and communications, transportation, product supply chains, and financial systems. And DHS owns many of these sector-specific relationships.

Let us face it. The cyber threat is not new or emerging. In fact, when I was Secretary, in 2003, a full decade ago, the first U.S. National Strategy to Secure Cyberspace was released. Greater awareness of this threat may be emerging, but the threat itself has been with us and will be with us for the rest of our lives. As the first Secretary of Homeland Security, I have a particular perspective on this issue.

We learned after September 11, 2001, and we learned after Hurricane Katrina and we keep learning after all these incidents that information and coordination sharing could have been better, and some people refer to a digital cyber Pearl Harbor. Well, at least in that instance, historians say that we did not have notice of the emerging threat. Well, I do not think this is the cyber Pearl Harbor, because we have notice, and it is not an emerging threat. It is a constant and ever-changing dynamic threat. So I am more inclined to say that it may end up being a cyber Hurricane Katrina where we had notice but we were not as prepared as we should have been until Thad Allen got there and cut through the Gordian knot of problems and began to address the situation that he confronted on the ground.

I have several more pages of testimony. I see my time is running out. But I hope we get to this area in the question and answer (Q&A). At the end of the day, the sharing of information between the U.S. Government and the private sector specifically—and I can refer to the enabling legislation that says that is where DHS has a very significant legislative role—is absolutely critical, and not in a prescriptive form. It cannot be in a prescriptive form. We cannot mandate regulations. There are plenty of standards out there, and, frankly, the President's Executive Order (EO) asking the National Institute of Standards and Technology (NIST) to set the standards

is something that we all welcome and we engage, but we hope we give it a chance to work and assure that the private sector is involved and engaged, because it is that kind of collaboration that is absolutely essential. And you are never going to defeat the cyber enemy, whether it is a nation state, organized crime, any organization, by having the private sector check the compliance box. We did all that Congress wanted us to do. That is not enough. That is inadequate. It is grossly ineffective. There has to be timely and continual information sharing horizontally within the Federal Government, particularly to DHS, and then vertically down to the State and locals, and particularly to the private sector. After all, the Federal Government relies on the private sector in order to function.

So as I said before, we have some lessons to be learned about the inadequacy of what the Federal Government is doing to protect its own information. I think it would be helpful not only when we repair that, but we also make sure that we facilitate the day-to-day engagement and sharing of information with the private sector.

I thank my colleagues who are on the panel, distinguished patriots as well, for the opportunity to appear with them, and I thank the Chairman and the Committee for the opportunity to share these remarks with you this morning.

Chairman CARPER. Thank you for those remarks very much. Congresswoman Harman, please proceed.

TESTIMONY OF THE HON. JANE HARMAN,¹ A FORMER REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. HARMAN. Thank you, Mr. Chairman. As I think every Member of this Committee knows, I have great affection for this Committee. I worked very closely with your prior management during 8 years on the House Homeland Committee and another 8 years, some of them overlapping, on the House Intelligence Committee. Later today, at the invitation of Colorado Governor John Hickenlooper, I am flying to Denver where Senator Lieberman and I are appearing on a 9/11 panel in Denver this evening.

Chairman CARPER. Well, I hope you will give them our best.

Ms. HARMAN. I shall. And as my youngest daughter would say, your former Ranking Member, Susan Collins, is one of my “besties.” And we stay close friends, and we all worked together on the intelligence reform law of 2004.

I also have great affection for all of us testifying before you today, worked very closely with everyone on this panel on homeland topics, and we continue to stick together, which I think is a good thing.

Twelve years ago today, as the towers were falling and the Pentagon fire was burning, I was walking toward the U.S. Capitol. My destination was the Intelligence Committee rooms in the Capitol dome—the place most consider was the intended target of the plane that went down in Shanksville. My staff called to alert me that the Capitol had just been closed, as were the House and Senate office buildings. So most of Congress, including me, milled

¹ The prepared statement of Ms. Harman appears in the Appendix on page 501.

around on the lawn in front of the Capitol. There was no evacuation plan. We had no roadmap for a response.

Part of the solution which some of us recommended was to create a dedicated homeland security function, and that function we thought should be in the White House, and Tom Ridge became its first coordinator.

Along the way, the White House proposed a much more ambitious concept, and in order to get this function as part of law, we embraced that concept, and then there became the Department of Homeland Security.

Now in its tenth year, I am proud of my role as one of the Department's "founding mothers," and I think we should acknowledge today the thousands of DHS employees who serve us daily around the country and the world. As we speak, Customs and Border Patrol (CBP) agents are in mega ports like the port of Dubai, and they are screening U.S.-bound cargo for dangerous weapons and materials. Specially trained homeland security investigation agents are in diplomatic posts everywhere in the world, and they are reviewing suspicious visas, and the Transportation Security Administration (TSA) screeners are daily depriving al Qaeda and other terror groups of the ability to turn more aircraft into weapons—a tactic we know they are continuing to attempt.

Today, as Tom Ridge said, DHS remains a work in progress, but the efforts of its people are its backbone—and our backbone. We have a safer country because of them.

A year ago, I testified here, and I noted some of the things that were going well at DHS. But I also noted challenges, and they include: An anemic intelligence function, something Tom Ridge just touched on; the need for DHS to focus more on its relationships with critical infrastructure owners and operators, something that is now happening because the cyber threat is increasing; and as mentioned by you, Mr. Chairman, the failure of Congress to reorganize its committee structure.

Today, as you mentioned, there is a very good op-ed in the New York Times—I actually buy the print edition, called "Homeland Confusion" but Tom Kean and Lee Hamilton, our good friends, and Lee preceded me as the president and Chief Executive Officer (CEO) at the Wilson Center, and we served as colleagues many decades ago in the House.

I do not want to touch on all of this, but let me just briefly scope the bad news and the good news since last year.

The bad news: We failed to thwart the Boston Marathon bombing; an exponential increase in cyber attacks; Edward Snowden; and the fact that the bomb maker, Ibrahim al Asiri, who belongs to al Qaeda, is still alive in the boonies of Yemen, despite our good efforts to retire his service.

But there is significant good news. One is information sharing is improving. I know there is much to continue.

Second, resilience. We showed resilience after Boston in particular, after the Boston Marathon bombing, and common sense is emerging in the way we approach homeland security. And to Senator Coburn's point, I think there is more support, and there should be, for a risk-based approach.

Collaboration with the private sector on cyber, that is happening, and credit should go to—I guess she has just retired—the Secretary of Homeland Security Janet Napolitano for personally working on this issue.

And we are getting ahead of privacy concerns.

Let me just touch on these very briefly because my time is running out, too.

Information sharing, Tom Ridge talked about it, but the Committee should take credit for the fact—and so should the Department—that homeland security grant money was critical. According to the Boston Police Department (PD), it helped make sure that the city was trained to share information rapidly during the emergency. DHS also participated in something called the Multi-Agency Coordination Center (MACC), that was operational before and during the marathon. And the MACC was critical in coordinating communications once the bombs exploded.

Resilience—a very important factor in our country's ability not to be terrorized. It is not that we will not have future attempts and maybe even successful attempts at attacks. But if we fail to be terrorized, the terrorists lose. And DHS, again, and this Committee distributed almost \$11 million to Boston, just to pick Boston, through its Urban Area Security Initiative (UASI). The money was used in part to upgrade over 5,000 portable radios for first responders, install a communication system inside the tunnels of the Boston T, and conduct two citywide disaster simulations in coordination with DHS. This is a very good news story.

Similarly, in Hurricane Sandy, which went fairly well, the Federal Emergency Management Agency (FEMA) activated in advance a National Response Coordination Center (NRCC), which was critical in terms of preventing more damage and speeding the recovery.

Collaboration with the private sector on cyber.

DHS will never “own” the cyber mission, but it is responsible for a central piece, which is critical infrastructure protection. And in the past year, DHS has tracked and responded to nearly—get this number—200,000 cyber incidents, a 68-percent increase from the year before. We will never get ahead of this problem if there is not a total lash-up with the private sector. And as Janet Napolitano and some of her team explained at the Wilson Center about 6 weeks ago, that is exactly what is happening. Kudos to the Department.

Finally, getting ahead of privacy concerns. The Department itself has a Privacy and Civil Liberties Office. That office has trained many in the fusion centers—68 out of 78 fusion centers have received some training. There is enormous complaint out in the boonies about the invasion of privacy, and it is important that we do two things: One is protect the American people, and two is protect the American people's privacy. It is not a zero-sum game. It can be handled with proper training.

And, finally, the Administration has fully populated the Privacy and Civil Liberties Oversight Board (PCLOB), which was created by the 2004 law and which was never functioning until May, and that should be helpful, too.

Let me just conclude by saying DHS will continue to face difficult challenges, including al Qaeda's enormous ability to evolve, the rise of lone wolf-terrorists, the constant increase in the type and sophistication of cyber attacks, especially the risk of exploits in software, and privacy issues. But most attempts to attack us since September 11, 2001, have been thwarted, for which thousands of selfless DHS people deserve our thanks, and so do our former Secretaries of Homeland Security, starting with Governor Ridge over here, and so do Members of this Committee.

Thank you very much, Mr. Chairman.

Chairman CARPER. Congresswoman, thank you so much.

Admiral Allen, please proceed. Your whole statement will, again, be made part of the record. Feel free to summarize as you see fit.

TESTIMONY OF THAD W. ALLEN,¹ ADMIRAL, U.S. COAST GUARD (RETIRED), AND FORMER COMMANDANT, U.S. COAST GUARD

Admiral ALLEN. Thank you, Mr. Chairman, Ranking Member Senator Coburn, and Members of the Committee. Thank you for the opportunity to testify this morning.

Like Secretary Ridge, for the record, I am testifying in my personal capacity today and am not representing any particular entity. I would note, however, that the op-ed piece that was published this morning by Lee Hamilton and Tom Kean was the result of an Aspen-sponsored task force on congressional oversight of the Department of Homeland Security, and I am a member of that task force, for disclosure.

I am also pleased to be here with comrades Jane Harman and Stewart Baker. These are people that I have worked with over the years and I hold with great respect and consider them friends and role models. I am glad to be here with them.

As you mentioned earlier, Mr. Chairman, it is hard not to sit here this morning and not recall the events of 12 years ago and what has transpired in the interim. I was the Coast Guard Atlantic Commander on 9/11, and what happened that day was something I thought I would never see in my career, and that was a Coast Guard cutter stationed off the tip of Manhattan with its guns uncovered. It was a chilling site. We closed the port of New York. We closed the Potomac River north of the Woodrow Wilson Bridge and then used Coast Guard vessels to resupply Ground Zero because there was such a problem getting vehicles in and out. So this was a consequential event for the Coast Guard as well, and I, like the members of the panel here, pass on our best regards to the families that were impacted by that terrible event.

I have testified before this Committee on several occasions since my retirement, and in each of the testimonies, including today, I have done a little bit of a retrospective on where the Department is at. I am not going to go into that today. I would say that I was the Chief of Staff of the Coast Guard when the Department was established and led the transition out of the Department of Transportation (DOT) into the Department of Homeland Security, and I have spoken over the years on many occasions about the conditions under which the Department was formed, which was bu-

¹ The prepared statement of Admiral Allen appears in the Appendix on page 505.

reaucratic light speed, just a little over 3 months. And the issues associated with trying to bring all that together, including—it was in the middle of an appropriations year. It was between sessions of Congress. I think Secretary Ridge was confirmed the day before he became the Secretary, if I remember correctly.

Mr. RIDGE. Correct.

Admiral ALLEN. That is a lot of stuff going on at the same time, but I think we have to move beyond the aggregation of entities that came into the Department and the conditions under which the Department was created and kind of get beyond that. You can talk about that as a means for why the Department kind of is the way it is. But I think 10 years later we have to actually sit down and say what is going on here and where do we need to go.

So I would like to associate myself with the remarks that were made by Secretary Ridge and Jane Harman. They have talked about the what. I would like to talk a little bit about the how, because ultimately we need to know, moving into the future, how we are going to attack these problems and what is the best way to do that. And the central part of all of us and a recurring theme you are hearing is information sharing, because information sharing is the precursor to unity of effort and more integrated operations in the Department of Homeland Security, not only in mission execution but in mission support, all the back-room operations that actually enable folks to put boarding teams on, to have TSA inspectors screen people, and that is financial operations, human resource (H.R.) operations and so forth. So I would like to talk in general about the border, resiliency, counterterrorism, law enforcement, and cybersecurity, as has been previously referred to.

Regarding the border, there is a lot of talk right now about the southwest border in relation to comprehensive immigration reform. And while we move forward and define what the policy is going to be and what we are going to do in relation to the number of illegal immigrants that are in the country right now, I think we need to remember that we have a border that is very complex and goes well beyond what I would call a geographically and physically described border. It is a functional border that also includes the analysis of data and the movement of cargo that are never touched by human hands but are virtually carried out and we have to carry out our functions as a sovereign government in a global commons in a variety of ways, including air, land, sea, and cyber domains.

So when we look at border security, I would just urge the Committee to try and understand that it is a combination of functions and it is a system of systems. And it cannot be reduced to oversimplistic fixes like fences or more Border Patrol agents. We have to figure out what is the nature of the problem and what is the best way to deal with it with all the tools we have available, including the aggregation of data on all border functions into a fused picture that senior leaders can take a look at. And I am talking about all the different license plate reader programs, passenger information, information on private arrivals of aircraft and vessels and so forth, bringing that together and putting that where there can be coherent analysis done against it.

I think sharing and fusing of sensor information across all domains is incredibly important. We need to build an architecture

that allows us to do that so we can understand the current conditions and the threats and how to react to them on the border.

We need to visualize that knowledge for our leaders so that they can understand what we would call a common operating picture, and that in turn can be discussed with folks here in the Congress regarding oversight.

And I think we need to look at, along the southwest border, not every part of the border is the same, and boots on the ground and fences are not the way to control the border. We need to look at areas where, say, there is no traffic, and conversations that I have had with some folks in the Department, we are actually using satellite imagery and going back and taking several runs at a time. And if there are no movements, you can pretty much say that is a low-risk area and start concentrating on where you think there is a risk involved there. I think in that way we could probably do a better job of looking at how we are managing the border.

Congresswoman Harman talked about national resiliency. I think this is extraordinarily important. And I think it is important because we need to start looking at resiliency as something that resides way beyond natural disasters and what FEMA does for a living inside the Department.

I am in favor of regionally based risk assessments that focus on the most likely and consequential events that occur, either natural or the man-built environments, and that includes understanding what population densities and critical infrastructure do and what kind of risk they present. And we need to figure out how to reduce those risks, including looking at building codes, land use, going beyond current floodplain legislation and regulations associated with that and try and look at the behaviors that need to be influenced to change how we think and act at a local level.

I think we need to improve our incident management doctrine. Homeland Security Presidential Directive (HSPD)-5 is a general framework for the Secretary to manage incidents, but, frankly, when you have these large, complex incidents, it is very hard to support one Cabinet to another in an overarching way to understand incident management, especially in complex hybrid events, I think is extremely important.

If you look at the possibility that we could have a combination of events that starts with a cyber attack, then gets into industrial control systems that produces a consequential kinetic effect, all of a sudden you have FEMA, the National Protection and Programs Directive (NPPD), the Federal Bureau of Investigation (FBI) through the National Cyber Investigative Joint Task Force (NCIJTF) there because it is a potential crime scene, and then you have the overall incident management, we do not have a coherent doctrine how to move forward on that.

And, finally, we need an integrated national operations for Homeland Security. The National Response Coordination Center at FEMA is an excellent operation for what they do. The Coast Guard has an operations center. One of the big challenges in the absence of being able to consolidate on a campus at St. Elizabeths is the inability to create a coordinated operations center with every component there to be able to coordinate in direct operations.

I have some other points, but I see my time is out, so I will submit that for the record. I will be glad to answer any questions you may have.

Chairman CARPER. Thanks. You crammed a lot into 5½ minutes. Thank you. That was a lot of wisdom.

Mr. Baker, please proceed. Welcome.

TESTIMONY OF THE HON. STEWART A. BAKER,¹ FORMER ASSISTANT SECRETARY FOR POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BAKER. Thank you, Chairman Carper, Ranking Member Coburn, and Members of the Committee. It really is an honor to be here with Members of the Committee and members of the panel. All of us made promises to ourselves and to the country 12 years ago and it is a pleasure to be here to have an opportunity to continue and rededicate myself with the rest of the panel to those promises.

There have been a lot of achievements in those 12 years, and DHS has contributed to many of them. It has many successes that we have heard about from other panel members that could not have been possible without the Department. It also has had some failings that I think you are talking about addressing quite directly. Reauthorizing legislation is an excellent idea. The idea of reducing the number of committees that provide disjointed oversight to portions of the Department would be an excellent approach, as would be building the equivalent of the Defense Department's Office of the Secretary of Defense.

We have had three great leaders of the Department who, when they are focused on a problem, have the entire Department sing like a chorus. But when they have had problems that they cannot spend 1 day a week on or one meeting a week on, the components tend to drift off. And there is no institutional mechanism for keeping the Department in tune when the Secretary is pulled off or the Deputy Secretary is pulled off in another direction. So finding ways to build the Office of Policy, the Office of Management, into effective managers of many of those second-tier issues would be very valuable.

I want to talk mainly about an issue where I think the most opportunity for progress is offered, and that is in cyber. This is a terrible crisis. We are not solving it. We are falling behind. Many of the ideas that have been proposed are rather divisive, but it seems to me that there are at least three issues where the Department of Homeland Security could contribute to and that may form a basis for less divisive solutions.

What seems clear to me is that, while we are falling farther behind, we also have more information about the people who are attacking us than we actually expected to have 5 years ago. We know what their girlfriends look like. We know what blogs they write. They are no more able to secure their communications than we have been able to secure our networks, and that offers some opportunity for actually bringing deterrence to bear, not simply defense. We cannot defend ourselves out of this cyber crisis. That is like

¹ The prepared statement of Mr. Baker appears in the Appendix on page 515.

telling people that we are going to solve the street crime problem by making pedestrians buy better body armor. That is not the solution. We have to find a way to actually capture and deter and punish the people who are attacking us.

How do we do that? Law enforcement is very familiar with the idea of deterring and punishing attackers, but prosecuting the people who are attacking us, many of them overseas, many of them associated with governments, is probably not the most effective measure. What we need is new ways of bringing sanctions to bear on the people that we can actually identify, and DHS can lead that.

If we used the law enforcement capabilities that the Department has at the Immigration and Customs Enforcement (ICE), at the Secret Service, integrated them in a smaller group, maybe on an experimental basis with NPPD and its defensive capabilities and its understanding of the attacks, we could gather much more intelligence about these people and then bring to bear new forms of sanctions—again, something DHS could take the lead in developing. Many of the companies that support these hackers by hiring them after they have finished their service for government, the universities that train them—need and want visas to come to the United States. I do not know why we are giving them visas if we know who they are. We should impose sanctions of that sort or, frankly, sanctions of the sort that Treasury uses today to deal with conflict diamond merchants or the Russian officials who oppressed the human rights of Mr. Magnitsky.

We face attacks on the human rights of advocates right in the United States, cyber attacks on Tibetan activists and the like. We should be treating attacks on human rights that occur in the United States every bit as seriously as we treat the Russian Government's abuses inside Russia. And, again, DHS could be authorized to go looking for ways to bring those sanctions to bear.

And then, finally, with respect to the private sector, it seems to me the private sector knows more about the attackers inside their networks than government will ever know. They are more motivated to find their attackers and to pursue those attackers, who often end up as their competitors. What is being stolen is competitive information. It is fed to competitors, and those competitors are operating in our markets. If we can gather intelligence and close the loop to find the beneficiaries of cyberspying, we can bring to bear criminal and other penalties on the beneficiaries of these attacks.

That is not something we are doing now because there is not enough integration between the people who have the resources and the incentive to do that, the individual companies who are under attack, and the law enforcement agencies that are totally swamped by the nature of the task. If we experimented with giving the companies that are under attack more authority to investigate their attackers under the guidance and supervision of the government, we could make more cases and impose more sanctions on the people who are attacking us.

So those are three pretty concrete ideas. There are plenty more in my testimony, which I ask that you read into the record. Thank you.

Chairman CARPER. Your full testimony will be made a part of the record. Thank you very much for your testimony today.

I want to return to a comment of Dr. Coburn's. Several of you, as well as, I think, Governor Ridge, and the issue—I call it “executive branch Swiss cheese.” It is not just DHS. It is not just the Department of Homeland Security. We have too many vacancies throughout the Federal Government. The Administration I think has released just in the last couple of days an extensive list of nominees. We welcome that. A lot of them are in the Department of State. One or two are in this Department. We are still looking for an Inspector General (IG). We need someone to fill that position in this Department, and a bunch of other IG positions that are vacant. This is a shared responsibility. The Administration has a responsibility to vet and give us names of excellent people, capable, honorable people, hard-working people. We have an obligation to hold hearings, to vet those nominees, and, to the extent that we feel they will do a good job, to move them promptly. And the Administration needs to do their job. We need to do our job. And we will keep focused on that.

Governor Ridge, we're wearing different uniforms, him in the Army, me in the Navy. There was a popular movie called “Five Easy Pieces.” Some of you are old enough to remember the Jack Nicholson movie. A great movie. And I think comprehensive cybersecurity policy is not five easy pieces, but maybe six. And I just want to mention them, and then I want to ask a question of each of you about one of those.

One of the pieces is critical infrastructure, how we best protect our critical infrastructure. That is a shared responsibility, as we know.

Another piece is information sharing. I think almost every one of you has touched on that in your testimony.

A third we call the Federal Information Security Management Act (FISMA), but it is really protecting the Federal Government's networks.

A fourth piece is workforce. Governor Ridge and I have talked about this recently and Dr. Coburn and I have talked about this a lot. How do we make sure that DHS is able to attract and retain the kind of people that they need to do their job in this arena.

Research and development (R&D) would be a fifth piece.

And another one that falls outside of our jurisdiction but an important one is data breach. How do we respond to data breaches? What are the expectations of those who breach data? That affects a lot of people's lives.

So those are sort of the six not so easy pieces that we are dealing with.

Over the past couple of years, the Department of Homeland Security has been playing an important role in protecting our Federal networks and working to try to secure our critical infrastructure. Unlike the specific statutory authority that defines the Federal Bureau of Investigations or the National Security Agency's (NSA) work in this arena, the Department of Homeland Security's authority comes really from a patchwork of Presidential Directives. It comes from policy memos. It comes from vaguely written laws.

In fact, one way I have heard it described is this: As far as cyber capabilities go, if the NSA has a Doberman, if the FBI has a German Shepherd, then DHS has a Chihuahua. Nothing against Chihuahuas, but they need a bigger dog because this is a big fight. And we want to make sure that we figure out what to do and give them that capability.

While I would say that DHS is much further along in developing cyber capabilities than some people give the Department credit for, I do think that we ought to provide the Department with clear statutory authority to carry on their current activities so that it can be compared to something a lot stronger, a lot more formidable than a Chihuahua.

Let me just ask each of you, do you believe that it is important for the Congress to empower the Department, this Department, with clear and explicit statutory authority to carry out its current cyber activities? These activities include working voluntarily with the private sector to protect against, to prepare for, and recover from cyber attacks. And would a better defined statutory mission of the current cyber activities—help to strengthen the Department's cyber capabilities? Governor Ridge, do you want to lead it off, please?

Mr. RIDGE. Senator, I think the enabling legislation that created the Department of Homeland Security, embraced in a strong bipartisan way by the House and the Senate, basically set up conceptually that very idea that DHS would really be at the epicenter of engagement down to the State and locals as well as the private sector. So, No. 1, I think it is certainly consistent with the original intent of Congress in terms of the role that DHS plays.

Second, I think any gray that exists in the alignment of DHS' relationship with the private sector particularly, probably creates a great deal of confusion. Right now I know the private sector is reluctant to cooperate, for many reasons even to share information because of the absence of liability protection or those sorts. I realize you are not asking that, but I think if there is a gray area that can be cleaned up and there is a direct line of responsibility—and, by the way, you also have the opportunity then to hold them accountable for not doing the job consistent with what Senator Coburn said. You have been assigned some tasks. We do not think you are providing those very well. You can hold them accountable that way.

Third, I would only say, however, that it will be important to do two things. One, I think it will be important to resource the Department appropriately. The men and women in DHS right now that are working on cyber, and government generally, let us face it, there are probably a lot more potential lucrative opportunities out there in the private sector. So we have some real patriots. R's and D's, Independents, it is immaterial. They are working hard on cybersecurity matters because they believe it is their contribution to their family's security and their country's security as well. But we are probably going to need to take a look at some kind of compensation adjustment to keep some of the best and brightest with us for some time. So, one, I think it is consistent with the enabling legislation.

Two, I think clarity would enhance the kind of voluntary collaboration that I think is absolutely critical between the private sector and the Federal Government vis-a-vis DHS. And then if it is going to be the mandate, I think they need to be properly resourced.

Chairman CARPER. Good. Thanks very much.

Again, the same question, if I could, for Congresswoman Harman. Would a better defined statutory mission of DHS' current cyber activities help to strengthen the Department's cyber capabilities?

Ms. HARMAN. My answer is absolutely yes. The Administration did issue an Executive Order last year, which is somewhat helpful, but it will take legislation, and Secretary Ridge outlined a lot of the issues. There has been a difference of opinion among people up here about how robust DHS' authorities have to be. But the bottom-line problem is that the private sector does not trust DHS. That has been overcome to some extent by the really impressive efforts that Secretary Napolitano has made in the recent months to reach out for industry, and now there literally is a floor in the DHS headquarters where the private sector and appropriate DHS representatives are working together on cyber threats. So that is a good start.

I just want to add a robust endorsement to your point about Swiss cheese. There are a couple of nominations that have been made by this Administration, and one of the nominees I know very well. She has been nominated for Under Secretary for NPPD, which is in charge of the cyber function, and I just mention her to all of you. Her name is Suzanne Spaulding. I hired her to be the staff director of the Minority on the House Intelligence Committee and worked with her for years. And before that, she was the Executive Director of the National Commission on Terrorism (NCT) on which I served, which was then chaired by L. Paul Bremer, Jerry Bremer, whom many of you know, a bipartisan commission that predicted a major attack on U.S. soil, one of three commissions that was not paid a lot of attention to. But we need nominees, and I would recommend, if anyone cares, the guy to my left as the new Secretary of Homeland Security.

Thank you.

Chairman CARPER. I will not ask if anyone wants to move that the nominations be closed. [Laughter.]

But we could do a lot worse. I do not know that we could do a whole lot better. But there is no shortage of, I think, really good candidates. We just need for the Administration to pick one and send us a great name. For Suzanne Spaulding, I think we have a hearing—I believe, Dr. Coburn, we have a hearing for her next week, and my hope is that we will be able to move that nomination quickly. She is an impressive candidate.

Admiral Allen, same question.

Admiral ALLEN. That is a tough statement to follow, but I will try. I think there are three things we have to look at. I do not think you can look at just the DHS authorities in isolation. And if I could just enumerate them, because I think it is really important.

The first one is the current status of FISMA, which is basically a regulatory compliance tool to try and ensure that proper information security is being carried out in the government. There is a

major step being taken right now to go move away from a compliance checklist mentality to continuous mitigation and measurement at the gateways so we actually know what is going on. That will be enhanced shortly by a dashboard which will pull that information up and allow it to be shared across the agencies. That is a phenomenal step forward, but it has been largely done through the congressional and appropriations process where money was provided to actually go out and solicit for that work to be done. So I think we need to move forward and figure out how we are going to transition from FISMA, which is a compliance program, to continuous monitoring of our circuits and how to move that information around.

Second, as Jane mentioned, the Executive Order (EO) on cybersecurity and infrastructure protection has laid out a number of very important steps, including a voluntary framework for the private sector that is being developed by NIST right now in cooperation with all the parties. But we need to go beyond the EO, as Secretary Ridge said, and start looking at the issues regarding liability and what are the prohibitions that keep the private sector from being involved.

So you have the FISMA revision; you have the EO on cyber, which is going to take legislation to completely solve that, and I think both of the other panelists have said that. And then, finally, what are the authorities and the jurisdictions that DHS would need to do that? If we put all three of those together, I think you have the complete package, and I think legislation is needed. But it should not be separate from legislation that addresses the issues with the private sector as well.

Chairman CARPER. Good. Thank you for those comments.

Last, Mr. Baker, would a better defined statutory mission of the current cyber activities at DHS help to strengthen that Department's cyber capabilities?

Mr. BAKER. Yes, I think in a couple of ways.

First, the technology is always evolving, and yet the law that we are operating under is 10 years old at least. In many cases authorities were simply transferred. And FISMA is a great example. FISMA envisioned doing security checks that would occur on paper and take months to accomplish. Yet the Department is now actually rolling out technology that will perform much of the FISMA checks in 3 days. And it is important to revise the law so it takes account of those capabilities and all of the other security measures that are being developed in this area.

I would certainly support the idea that working with the appropriators is the best way to do this. Having a single unified appropriations process for the Department is the saving grace for the Department, and the more that can be done, the better.

Similarly, the second point that I will close on is that in many cases the authorizing legislation needs to make clear that, while the National Security Agency has a big dog, it is an important participant—I used to work there, am very supportive of it, but everyone in the country needs to be reassured that when we are talking about cybersecurity, it is DHS that is setting the policy and dealing with the data, not the National Security Agency.

So what I would say is maybe DHS does not need so much a bigger dog as a leash, and authorizing legislation can provide that kind of reassurance to the American people.

Chairman CARPER. Thank you all for those responses.

I consulted with Dr. Coburn. We are talking about how do we better honor the loss of all those lives 12 years ago this morning. Do we honor it by recessing and going to join some of our colleagues on the steps of the Capitol for an observance? Or do we really better honor their lives and their loss by continuing to do our work here today? And we believe that the best way to honor them is for us to continue doing that. We are going to continue going through the 11 o'clock hour, and that will give us a chance to really drill down on some of these important issues.

With that having been said, let me just yield to Dr. Coburn. Thank you.

Senator COBURN. Well, thank you, Mr. Chairman. A couple of points based on what I have heard here today. The Homeland Security budget is twice what it was when you had it, and everybody knows we are resource poor right now. And the question is: How do you put metrics on what Homeland Security is doing?

I would suggest, No. 1, there are 45 open areas from the Office of the Inspector General (OIG) that have not been addressed by the Department of Homeland Security on recommendations that they essentially agree with but they have not acted on. I do not know if that is a priority problem or a resource problem. But that list is growing.

The second thing, on FISMA, Bobbie Stempfley is a great leader at Homeland Security. If we had a hundred Bobbie Stempfleys, we could all sleep great at night. But the fact is FISMA is going backward, according to the last Office of Management and Budget (OMB) report, not forward. So I am very hopeful, based on what you said, Admiral, on what we are going to see and what you said, Mr. Baker, in terms of improving that.

The other point I would make is I asked the Congressional Research Service (CRS) to give us what statutory authorities Homeland Security has, and they have most of the authorities they need for everything. As a matter of fact, when Secretary Ridge was Secretary, he had them start all these things under these authorities. So we need to ferret out what we actually really need to do to give increased authority.

The things that I am concerned about is I do not—first of all, we cannot afford to duplicate things that we are doing at NSA. And we heard from all of you, every time we have seen a problem since September 11, 2001, it is because of either a stovepipe or an individual judgment that was made in the wrong direction. Even with Boston, if you go to the intel on all that, what we know was we had some errors made by individuals or by process rather than have flat, good, horizontal communication that was real time.

So Tom Carper and I do not disagree about what the goals are. The question is or the disagreement is: How do you get there and how do you hold people accountable?

So information sharing is the key for us to be flexible and highly responsive when it comes to threats for our country, and how we do that is important.

And I think, Jane, you said something that I think is really important. The confidence level by the public and the private sector in terms of DHS' capability to handle all this is a key hurdle we have to get over. And what we have to do is we have to walk before we run. And we have been crawling, and now I think we are walking, and I would attribute some of that to the most recent Secretary, but also to Bobbie Stempfley and her crew and some of the other things that are going on there.

The other thing is privacy is a big deal. We have seen that. But we had a lot of problems at fusion centers with privacy. We put out a report that showed that, and they responded. They were starting to respond before that. But there is no privacy policy associated with the drones with DHS right now. We have an open letter that has not been answered. What are you doing about it? And yet there was no consideration of privacy as they made the policy for the use of drones. So there are big problems for us to address.

I guess what I would ask is—and, by the way, I do need to make a correction. The President has nominated four positions out of the 15, not two, so I stand corrected on that: Office of General Counsel, NPPD, Customs and Border Protection, and Mr. Mayorkas.

So I guess the question I would ask is: How do we incentivize to make sure we have real-time sharing across all the branches, one? No. 2, how do we reform Congress' oversight of DHS to where we limit the committees? Tell me how we do that so that we can make them react in a positive way and not spend so much time up here on the Hill but have good, clear communication and single authority coming out? We have most of the authority for Homeland Security, but that is not true in terms of a lot of other subcommittees. So your comments on those, and I would like each of you to address that, if you could.

Mr. RIDGE. Well, I would be happy to volunteer to begin the conversation. I must tell you, Senator, that I think your frustration with the growth of the Department in terms of personnel and dollars is something that I share a little bit. More is not necessarily better.

I remember my first year as Secretary. A well-intentioned Congress on both sides of the aisle wanted to give me more money, and I said, "Before you give me more money, I think I better take a look at it and see if we are doing an effective job with the money we already have." And I thank you and Senator Carper for bringing that mind-set.

Someone told me that we have gone from 180,000 basically to 240,000. I do not know what the number is, but, I mean, I just have no idea where the additional bodies are needed, notwithstanding some increase in personnel down at the border, CBP and ICE, like that.

So I must tell you, I think at the epicenter of all the concerns you have addressed is the failure of this institution of the Congress of the United States to consolidate jurisdictions so that there are no end runs to protect vested interests that have been existing in silos for a long time. And I think the only answer to that is the will of this body to effect a change. Unless you can consolidate jurisdictional responsibilities so that a small group of Republicans and Democrats in both chambers have exclusive jurisdiction or

nearly exclusive jurisdiction, you are going to see through the process—because we all know that it is a little byzantine, it is—everybody has allies on all these other committees, both on authorization and appropriation levels. We really need to do that. And I think if you can consolidate that responsibility, I think you can affect the kind of change that you are talking about.

It is amazing to me that the Congress would ask two of America's great public servants—Lee Hamilton and Tom Kean—to spend about a year and a half or 2 years, take all that testimony, and say, "We as a Congress want to know how we can help this new Department mature and how we can make our country safer," and two of the most obvious and needed recommendations made 10 years ago, consolidate jurisdiction on the Hill and private sector, a public safety broadband network so that police and fire and emergency responders can handle future crises and all that, and we are not there.

Senator COBURN. The third one is risk based rather than all hazards.

Mr. RIDGE. Exactly, and the third one is risk based. I mean, clearly—but I must say, they are starting to do it at TSA. I mean, I like the pre-clear program. I know John Pistole has done a great job. They are moving in that direction. But I am going to say to my friends on both sides of the aisle here, quit arguing about a fail-safe border security platform; you will never make an absolutely secure border. What we want to do is reduce the risk. So we have to risk-manage the border, we have to risk-manage commercial aviation, we have to risk-manage everything across the board. But I think at the end of the day, Senator, if you are looking to achieve the outcomes that I think are generally shared on both sides of the aisle, the commitment is that strong, then I think the Republican and Democrat leaders in both chambers have to sit down before the next Congress and say, "Enough is enough."

One final anecdote, and I say this with the greatest respect for my 12 years here on the Hill. I cannot tell you the number of times we have been walking over to a vote, and we would be leaving a committee or subcommittee hearing, and there would be lament among the members: "Geez, we got five or six committee hearings and subcommittee hearings today, and we have to run from here to there." And everybody decries the pressure on legislators to do their job effectively and all these committees and subcommittees, but nobody wants to relinquish the seat on the committee or subcommittee. It may not be voluntarily relinquished, but if the leaders in both chambers say, "As of this Congress this is done, we are making these changes, Homeland Security does not report to 100, it reports to 5 or 10," it will be done.

So I think the answer to that is you have to get the leaders in both chambers and both parties to agree, because I think it is at the epicenter of solving the problems that you have just addressed. A strong letter to follow.

Ms. HARMAN. Mr. Chairman, let me apologize in advance. I have to leave at 11 because I serve on a foreign policy board to the State Department, which has been rescheduled three times, but it is today, and the meeting with—

Chairman CARPER. We understand. We are just delighted you—we will make the next 17 minutes count.

Ms. HARMAN [continuing]. At 11:30 on my way to the airport. All right. So I apologize.

Let me just address reorganizing Congress, which I think is absolutely essential and will be very difficult to do. I was in the painful conversations with—I am not sure if it was the Democratic Caucus; Maybe Senator Baldwin remembers back in the day—about the need for more jurisdiction for the House Homeland Committee, and the pitch was made and people nodded, and then someone from the House Commerce Committee stood up and said, “Oh, no, but this notion of an interoperable emergency broadband network is central to our jurisdiction.” And so, of course, read: No change. And people in this institution on both sides earn their power through their committee positions. And giving up power in this institution is not something people will do voluntarily.

So I agree with Tom Ridge that the leadership will have to basically require it. However, the leaders earn their power through the loyalty of their members, and making members shrink their own power is not really helpful to leaders holding power. So I do not know how the thing changes, but until it changes, we will not have the robust homeland function that we should have.

Just one other comment, as I kind of implied, 10 years ago, the concept for the Homeland Department was more ambitious than maybe some of us would have wished. It was the White House’s proposal to put 22 departments and agencies together. Some of us had thought about a more modest function directed by the Homeland Coordinator in the White House, a job Tom Ridge originally had. But we took it because the Administration was behind it.

So it is a daunting task to make this thing work. At this point I do not think we should rearrange the deck chair in the Administration. But if there is a way—and maybe the members here have more power than members that I observed back in the day. If there is a way to reorganize Congress to give this Committee and the House Committee more power, I think our country will be safer for it.

Chairman CARPER. Admiral Allen, do you want to——

Admiral ALLEN. Thank you, Mr. Chairman.

Chairman CARPER. And then Mr. Baker. Go ahead.

Admiral ALLEN. As I stated earlier, I spent several days out at the Sunnylands Estate at the Annenberg Foundation site in Rancho Mirage with Lee Hamilton and Tom Kean as part of the Aspen task force that produced the report that was sent out today. My proposal would be that be submitted and attached to the record because there is a detailed discussion of that rather than take the Committee’s time here.

I would say that I would not have served on that task force if I did not subscribe to the concept that we need to make this simpler.

The Coast Guard’s authorizing committee is Transportation and Infrastructure (T&I), and there is a subcommittee for the Coast Guard there. I spent 4 years as the Commandant of the Coast Guard without an authorization bill. There were significant issues that we needed to deal with, anywhere from fishing vessel safety

to unregulated small boats that never were able to be addressed, and then if they were, committees would assert jurisdiction that had to be sent over to those committees for review. Very time-consuming. And if you look at some of the issues we have not been able to address—and a lot of those areas are addressed in the Aspen report¹—I would direct the Committee just to take a look because I think there are a lot of issues on the record that have been raised. The issue of security for general aviation aircraft is another one moving forward.

The only other point I would add in response to Senator Coburn's comments on risk based, if you look at what we are trying to do right now with flood insurance, it is very instructive, because we have a problem right now, and those that bear the risk do not pay for the risk. We have an extraordinary amount of liabilities that have been built up trying to pay off the flood insurance claims for Hurricane Katrina that still exist today, and there is no clear way to how those books are going to be balanced moving forward.

On the other hand, if you start to let those flood insurance fees rise, you have issues with local communities. And what you really need to do in the long run, in my view, is get out ahead of all this by starting to change behaviors on building codes, land use, and zoning out there, which is a much more strategic way to deal with this. But you cannot do that if you have four or five committees asserting jurisdiction over the problem.

Mr. BAKER. I fully support the idea of reducing the number of authorizing and oversight committees. Let me, though, talk about two ways that we can address Senator Coburn's concerns about the budget and some of the other issues.

It seems to me that proper authorizing legislation can set the framework for actually saving money in the budget, and I will give you two examples. In fact, you raised one. The question of duplicating NSA's capabilities, it makes no sense for DHS to try to do that. NSA has built capabilities over 50 years, carrying out a mission that has been funded in ways that DHS's mission will never be funded. They have enormous capabilities.

At the same time, both the American people and I think the Department of Homeland Security want some reassurance that if they lean on DHS to use those capabilities, they will not discover that policies are being made de facto, privacy policy in particular, by the people that they are leaning on. And so language that could create a set of authorizing legislation that sets aside DHS' authorities and leaves it in control of its area, drawing on NSA for talent and for tools and technologies that it already uses, you will end up saving money by relying on existing capabilities and creating at the same time reassurances for people about how that reliance will work.

The same thing, it seems to me, is true if you can build a planning process, a budgeting process that uses integration, Office of Secretary of Defense type capabilities, to say how can we reduce the budget effectively, how can we eliminate redundancies by looking at the authorizing language? And if we do that, we will be building the capabilities at what I described as the second tier so that the Secretary does not have to sit down and get out the eye-

¹ The report to which Mr. Allen refers can be found on page 523.

shade and start asking about the 14th line on individual components' budgets, but that is being done by a centralized staff that is trying to eliminate redundancies. So by creating the right kind of authorization for those central staffs, you set the framework for reducing the budget.

And, last, tied to that, it seems to me that until the day comes when we have eliminated many of the authorizing issues, one of the things that this Committee can do is build a relationship with the appropriators so that when the appropriators are asked about legislation that arguably is authorizing on appropriations, they know that this Committee has looked at those ideas, has thought about them, has vetted language, creating authorization language that may in a pinch end up in an appropriations bill, is worth considering in at least the short run until we get to the promised land.

Chairman CARPER. Good. Thanks. I apologize to Senator Baldwin and Senator Chiesa, and Senator Ayotte has just left, too, to attend the observance. We have gone well beyond our 5 minutes, as you know, and I thank you for your patience. I just thought it was really important for us to allow this panel to answer these questions in the kind of thoughtful way that they have done. We spend so much of our lives here just going from one place to the other and in and out, as some of you know, and this was just a very helpful series of questions and responses.

Senator Johnson, if he comes back, is next. Senator Chiesa is going to be recognized next, then Senator Baldwin. Senator Pryor was here. I think he has made the same decision that Senator Ayotte has made. But this is just an excellent hearing, and I am just very pleased with the way it is going. Jane, after Jeff asks his question, we will give you maybe the first rights, the first shot at that, if you want, and I know you have to leave.

OPENING STATEMENT OF SENATOR CHIESA

Senator CHIESA. Thank you, Mr. Chairman, and thanks to this panel for being here today.

Mr. Chairman, I join everybody in remembering the families, many from my State, who were so tragically impacted by the events of 9/11. We all remember where we were that day, certainly in New Jersey, watching this go on.

I have prepared some remarks that I would ask you to make part of the record rather than reading them here today.

Chairman CARPER. Without objection.

Senator CHIESA. Thank you.

The most recent events that we have seen that really get to the issue we are talking about today are the bombing at the Boston Marathon. And at the time—and I have raised this issue before when we had Commissioner Davis here and others to talk about those events, and I was serving as Attorney General at the time, and I remember in real time being in my office and learning that there were contacts, potential contacts to what was going on there in my State. And I remember—our State police and everybody just did an unbelievable job and turned that around in a way that makes everybody proud. It really does. And I understand that we want to work hard so that we do not have the event actually occur.

So I have the same question, and, Congresswoman Harman, I would invite you to answer first because of your time constraint. Do you think we currently have the appropriate climate among the people that are responsible for having, developing, and sharing the information necessary so that information is flowing appropriately, to get to Secretary Ridge's point, we are not overly siloed? Because of all the things we are talking about, be it from a cyber perspective, be it from a terrorism perspective, be it from whatever these perspectives are, it is all about making sure the information is getting where it needs to get. And I would ask each of you to talk to us about your thoughts on the current climate of the way that information is shared among the people responsible for sharing it?

Ms. HARMAN. Well, thank you, Senator. I would give us, as I just said, an F for reorganizing Congress. I think it is really sad that Congress has a 19th century structure to deal with 21st century evolving threats against our country. But on information sharing, I would give us a B, and that is not an A, and I am looking at Tom Ridge. I do not think—

Mr. RIDGE. Did you say B or D?

Ms. HARMAN. B. It is not an A, but the challenge was to break down silos and to create opportunities for people to actually know each other, which is one of the ways you build trust and enable information sharing.

Yes, there were mistakes in the Boston Marathon case. The Terrorist Identities Datamart Environment (TIDE) list did not get to the right folks, and the FBI did not followup, and a little of this and a little of that. However, once the event occurred, Boston—the surrounding police departments, the State of Massachusetts, and all of our Federal law enforcement agencies and Homeland came together in almost a seamless way; and using video, including people's handheld phones, they were able to piece together the identity of the folks and to close in on them quickly. So that is why I say it is a B. After action we were an A; before action we were probably a C. But this is improving.

I just want to mention something that we have not talked about but it is something I know a lot about based on my role on the Advisory Committee to the Director of National Intelligence (DNI) and some of these other intelligence places that I stay connected to, and that is that information—the dark side of information sharing is that it enables a Snowden or others to get too much information and to use it for nefarious purposes. So our goal has to be to build the trust, to build the horizontal arrangements, but then also to put in safeguards so that people with bad motives inside our system or outside our system cannot abuse it. And I do not think we mentioned that, and I do think it is part of the challenge going forward.

Senator CHIESA. Thank you. Secretary Ridge.

Mr. RIDGE. Well, I had the great pleasure of working with Congresswoman Harman back then. I think she is grading on a higher curve than I would by giving everybody a B. I am not going to give them a grade, but I want to address something that I found and I still find troubling, and it goes to the perception that DHS has not done its job.

I remember doing some TV after the Detroit bomber, and DHS was criticized for letting the individual on the plane. And I think Secretary Napolitano has taken some heat, and I had to remind everybody that DHS does not gather information. They rely on the alphabet agencies to provide it. And if the State Department did not give the information to DHS and Customs and Border Protection and give them reason not to put the person on the plane, then DHS should not be held accountable. But it seems from time to time they are.

I think back to Fort Hood. There has been public revelation that the FBI in two different venues were aware that Hasan was e-mailing the radical cleric in Yemen, and DHS takes a little hit on that. Why didn't they do more? Well, frankly, that was not in DHS' spot. Somebody has to ask a couple of the other agencies why they did not do more.

Now let me go to your question with regard to Boston. I do not think that the FBI is on a speed-dial arrangement with the Kremlin, and I would like to know personally how often the Kremlin picks up the phone and says, "We think you have a couple terrorists in your midst." So I do not know how thorough the examination of that revelation was within the FBI. I am not faulting the FBI. I just do not know whether or not the Federal Government generally, including the FBI, took Russia, Russian intelligence, communication as seriously as it should have. There may have been other agencies that should have been involved.

I think the response, as Congresswoman Harman said, to that incident was phenomenal. DHS did not get the credit—I mean, there were grants that went out; a training program went out. All that was done under DHS. But that is triage after the incident, and that is why information sharing is so critically important.

Let me just take this a little step further. Let us assume that you break down the silos and there is more and better information sharing conceptually. I think somebody has to take a look at classification. The easiest way for an agency, I do not care what the agency is, to deny access to—and I am concerned about State and locals and private sector—is to say it is top secret, top secret sensitive compartmented information (SCI). Well, nobody wants to touch it. So I think somebody has to take a look at classification. I have seen a lot of things that were classified top secret that I know you could have shared with folks that would not do harm to sources and methods. And so I think classification is very important, particularly if we are serious about information sharing down to the State and locals and the private sector.

Finally, I think Attorney Generals have to know more information about what is going on in their State. I am just one of those folks—you cannot secure the country from inside the Beltway, and at some point in time, Federal agencies, the alphabet agencies, have to entrust and trust high-level law enforcement members in all 50 States and territories with information about what is going on in their respective States. I venture a guess that you have no idea, as all the investigations did not when you were Attorney General, into potential terrorism activity in your State.

I think it is a huge mistake. People say, well, somebody may reveal that information that was shared. Well, then, there would be

consequences. But I just think we need to expand the network with fellow Americans who have responsibilities for safety and security in this country. We have to start to trust them. You cannot just keep all that information in here.

So that is my response to that inquiry, and I do think we need to take a look at classification because it is overly classified, which is reason not to share, and safety and security is the ultimate concern. You have to trust fellow Americans outside this city to help keep the country safe and secure.

Senator CHIESA. Thank you, Secretary, and I know that my experience was——

Chairman CARPER. Congresswoman Harman, as you leave, thank you very much. Godspeed.

Senator CHIESA. Mr. Chairman, I know I am out of time. We had the opportunity to be briefed, and every Attorney General's jurisdiction is a little bit different. Mine included a lot of those things. But I think to get to your point, others have made these relationships. The first time you are talking cannot be after an event. Right? And talking before and having some trust and having seen somebody is invaluable once the event starts so that there is no hesitation, because that information has to get to the decision-makers and to the rescuers and to whomever else is involved. So I appreciate your thoughts on that.

Mr. Chairman, I am over my time, and I do not want to hold up Senator Baldwin, but at some point I would love to hear from the other panelists, too.

Chairman CARPER. Senator Baldwin, are you OK if the other panelists respond to his question? Are you OK with that? Let us just do that. We have a good flow. Thanks.

Senator CHIESA. Thank you.

Admiral ALLEN. Rather than repeat some of the points, which I think are very valid, that Jane and the Secretary have made, let me take a little bit of a different spin on this. When you look at counterterrorism and the great expansion of transnational organized crime and illicit trafficking, we know there are growing linkages there. Whether you are a terrorist or you are a criminal, you have to do a couple of things that are visible. You have to talk, you have to move, and you have to spend money. And every agency operates basically on a case doctrine and how you manage it, and in that case there are usually confidential informants, and there are sources and methods. That usually is the route of classification, as Secretary Ridge referred to, because they are trying to protect that.

The problem is that our law enforcement structure in this country has evolved over the last century against business lines of the bad guys—drugs, alcohol, tobacco, firearms, counterfeiting, intellectual property, all managed by a law enforcement agency that manages as a case.

The fact of the matter is we are dealing with networks, illicit networks, that generate cash however they need to to perpetuate their regime. And what you need to do is attack the network with a network. And I think the greatest case for information sharing and the greatest case for more and better integration, not only in the Department of Homeland Security but domestically and internationally, is to move to a way to look at these challenges as net-

work challenges and how do we move across dealing with their business lines, which means you are only taking down one franchise. You are not dealing with the root of the problem, which is how the network managed itself, threat financing, how the money moves, how they move, and how they communicate. That is the No. 1 cause for action on information sharing in my view.

Mr. BAKER. Three thoughts on this, one that I offer only tentatively because I do not know all the details. But I do remember that when the older Tsarnaev brother came back from Russia, he entered the United States, we had the chance to interrogate him; we had the chance to look at his electronics as he crossed the border. We did not do it. My impression is we did not do it because at that point the FBI had closed its case. And one of the questions I wonder about is whether DHS and CBP have deferred too much to the FBI. We have an independent responsibility to protect the United States, and the fact that the FBI closed its case is not necessarily a reason not to ask questions of somebody who has gotten the kinds of intelligence reports that Tsarnaev earned.

Second, one of the things—

Senator COBURN. Let me correct the facts on that. Your statement is in error.

Mr. BAKER. All right.

Senator COBURN. The information was sent to the Joint Terrorism Task Force in Boston, but it was not relayed to Customs and Border Patrol at Kennedy.

Mr. BAKER. OK. So then there clearly were failures of information sharing that cost us something, and something significant.

Second, we learned after Boston how valuable cameras can be. They are not valuable in stopping crimes. They are valuable in catching the people who carry them out. That is also true—we learned that in the Tube bombings in London. And yet for a variety of reasons, including privacy campaigns, a lot of cameras have not yet been installed inside the city centers. We do not actually need them hooked up, we do not actually need to be watching them, but they need to be recording so that if something bad happens, we can go back and figure out what events led up to that. We should be encouraging the installation of those cameras, and if people have privacy worries, we should just have them continually write over their hard drives as opposed to send the data anywhere.

And, third, on the information-sharing point, I thought that Jane Harman was exactly right. Information sharing creates risks. It creates the risk of Snowdens or Mannings. But on the network Snowdens and Mannings look a lot like Chinese hackers who have also compromised computers on the networks and are gathering suspicious amounts of data, and the same tools that help us to provide better cybersecurity will also provide better audits of who is on the network, what they are doing, and will protect privacy as well because we will be able to tell who has accessed information improperly.

And so one of the things that this Committee could do, that DHS could do, is to make it a little clearer to the State and local entities that get grants, that they can use that money for cybersecurity audit technology that will allow them to meet all of those requirements.

Senator CHIESA. Thank you.

Thank you, Mr. Chairman.

Chairman CARPER. You bet. Thank you.

Senator Baldwin, thank you for your patience here today. You can take as much time as you want.

Senator BALDWIN. Thank you, Mr. Chairman, Ranking Member, for holding this hearing, and I want to thank all of our panelists, including Congresswoman Harman in absentia, for your service to our country. I appreciate each of your sharing your analysis and appraisal of where we have come in these last 10 years and where we still have to go.

I want to focus my questions on the larger issue of cybersecurity and the incredible increase in cyber attacks that we are experiencing. And I would like, if you could—and I will start with you, Mr. Baker—to sort of talk about any distinctions that we should appropriately make with regard to economic cyber attacks versus the threat of cyber terrorism where the goal might be to take out part of the power grid, for example. And I would like to have you focus—you ended your testimony a little bit with the private sector being in a position where they have more intel on their potential competitors, but I think you were talking about economic cyber attacks in that arena. So the question I have is: What can we do better with existing authorities?

And then the second question that I would like to hear from all of you about is, you know, I do not know how long the journey will be until Congress actually passes legislation on this topic to supplement the Executive Order and to respond to many of the issues that have been raised. But there have been lots of comments about—and, Secretary Ridge, you talked about do not make this prescriptive, do not make this regulatory. Again, I wonder whether there is a distinction we need to make when we are talking about critical infrastructure because the people of America depend upon that critical infrastructure for daily life, and it may be private, but it is to the public benefit without question. And should there not be some additional obligation, some prescription, if you will, because of the level of importance of that critical infrastructure?

If you do not mind, Mr. Baker, I would like to start with your reflections on those questions.

Mr. BAKER. So there are two big worries in cyber. One is what you might call economic espionage or espionage generally, in which all of the attacks are aimed at stealing information. And we have seen enormous amounts of attacks aimed at practically everybody who might be of interest to any foreign government with any capabilities in this area, and probably everybody on this panel and certainly everybody on this Committee has been attacked in an effort to gather that information. So that is a serious pandemic problem right now.

Second, sabotage or cyber war or cyber terrorism designed to break systems is a very serious possibility. I am not so sure about terrorism. I do not think it has been very healthy for al Qaeda leaders to use the Internet in the past. But state-aided terrorism is a concern. If we actually did attack Syria, I think you would have to worry that Iran or Hezbollah or some organization assisted by them would engage in cyber attacks on the United States de-

signed to cause failures in financial or industrial control systems, and those could be very serious.

All of those attacks tend to actually use the same basic techniques. You break into a standard commercial network, and then you try to hop to an industrial control network that you can break and cause serious damage. And so stopping the espionage attacks, making it much more expensive to break into systems to steal secrets, is probably our first and highest priority.

First, companies know a lot about who is in their network. I represent a lot of them, and the experts that they hire say, "Oh, yes, this is a unit of the People's Liberation Army or some criminal gang. We know, by the things they are doing, the code they are leaving behind, who it is, and we can tell you what their tactics are going to be for the next 24 hours or 48 hours. We can tell you what they are trying to steal and why."

So companies know a lot just from looking at the activity on their network, information that may not be available to law enforcement. What they cannot do is go to the command and control servers that are being used to steal the information or to the attackers headquarters computers. For that you often need law enforcement authorities. But law enforcement does not have all of the background information. So we need to find a way to use existing law enforcement authorities and the existing resources and information that individual companies have to actually track those guys back home and then begin looking for reasonably creative penalties that can be applied. Again, using existing authorities, we can deny visas for any good reason. The President and Congress can impose financial sanctions on individuals who have committed this kind of crime. We have lots of authorities we have not yet used.

Admiral ALLEN. I think the progress that has been made with the Executive Order that was signed by the President regarding cybersecurity and infrastructure protection has taken a major step forward. I think, though, as was mentioned earlier, until you start dealing with the issues about proprietary data, antitrust issues, and liability, there is going to be a hesitancy of the private sector to want to fully get on board with that.

Now, I think the conversation that has been started in the last 2 weeks with the release of the draft voluntary framework by NIST is going to advance that discussion further. There are some critics that have said that is too general and not detailed enough to be effective. My position would be that you need to start out with the 1.0 version and go to the 2.0 version, and having that conversation and moving forward and involving the private sector in that is really what is needed.

But if you look at this problem, this is a classic case of macroeconomics. What is the inherent governmental role here? What should the private sector be doing? And I think that there is not a consensus in the country about what those roles are. Are the markets going to clear security? Or is the government going to provide there will be a command and control regulatory system?

I think to figure out a way, No. 1, to share the information that is currently held classified within the government and get that out to the people that need it; on the other hand, when they are attacked, to get that information out of them so it can be used when

they are concerned about regulatory oversight of potential civil or criminal penalties associated with that.

I will just say this: There are a lot of people out there that are trying to work this problem. I have had the opportunity over the last couple years to work with an organization in Pittsburgh called the National Cyber-Forensics & Training Alliance. It is a 501(c)(3) organization that was developed with the local folks at the Software Engineering Institute at Carnegie Mellon and the local FBI office, and they actually have kind of developed a way to create what I would call a metaphorical Switzerland where they are collocated in the same place, so it is capable of just walking across the hall and exchanging information, understanding the protocols, building trust and so forth. But we are going to have to figure out a way for both of those parties to come into an area where they are free of risk, organizational risk, to provide that information and exchange it. If we cannot do that, it does not matter what the role of the government is or what the role of the private sector is. It is not going to work. And of all the conversations I have had in the last 2 or 3 years regarding this very complex problem, the National Cyber-Forensics & Training Alliance has come closer to trying to figure out exactly how that works in the organization I have run into, and I would suggest the Committee may want to reach out and talk to them.

Mr. RIDGE. Senator, I think——

Senator COBURN. Turn your microphone on.

Mr. RIDGE. I believe quite a bit of progress has been made since the establishment of the Department with regard to addressing cybersecurity, although I think we all have to honestly admit in 2003, when the enabling legislation was created, there was no one, I do not think, that was as totally concerned about—some may have been—the emerging threat of cyber incursions as we all are today. It has accelerated. It is pretty remarkable if you think that we commercialized the Internet in 1992 or 1993, and now it is the backbone of absolutely everything we do. And so the sensitivity and concern with regard to distinguishing between what is an economic event and what is actually a more defense-directed or offense-directed security incursion is a legitimate one. We know who the actors are. You have nation States. You have terrorists. You have hackers employed by nation States and terrorists. You have organized crime. There are multiple challenges in dealing with this.

Even if we can attribute, if we can actually attribute who the attacker was and make a determination of the consequences, what do we do about it? What do we do about it? I mean, that again speaks, I think, to the kind of collaboration that focuses on information sharing in a true public-private partnership with the private sector rather than compliance, because with due respect to my profession, as an attorney, I do not see compliance lawyers as being the best means of assuring that we have enhanced our security in this country, because a regulation means there will be a block, it will be a check block, and you will check, and they said, OK, you did what the Federal Government wanted to do. And, frankly, the technology available today, offensive and defensive, as we speak, is changing, and it will be different tomorrow and the years ahead.

So I think the best insurance right now is to take, frankly, the embrace of—I think it is Pat Gallagher running NIST, who I think testified perhaps in this Committee previously about, look, let us continue down this path of setting voluntary standards that both the Federal Government and the private sector agree upon, and let us see how well they do about taking those standards and devising the kind of defensive infrastructure that they need before we start thinking about regulations, because I am afraid we will never be—I am going to say this: Congress 4 or 5 years ago appropriately gave to DHS chemical facility antiterrorism standards and regs. I think we are 3 or 4 years later; there are a lot of people working really hard on it. But that delegation of authority does not mean it was executed in the appropriate way. And I am simply saying, for the time being I think we ought to let this—I think President Obama set it up with his Executive Order. I think we ought to let that come to fruition before we even think about standards—before we think about regulations.

I might add the three or four critical sectors—and I think you were alluding to them in your comment—you have financial services, you have energy, you have transportation. I must say from my experience these sectors have spent and will continue to spend hundreds of billions of dollars, sometimes on their own, sometimes in cooperation, in collaboration with Homeland Security. But we have evolved a long way. I remember we created a Computer Emergency Response Team at Carnegie Mellon because this was an emerging problem back in 2001 and 2002. Now it is a fact of life. We are going to be dealing with forevermore. Forevermore. And so I do not think we are ever going to have a regulatory compliance scheme that is going to be able to keep up with the dynamic environment.

So my recommendation based on the purpose of this hearing, even though I think your question is a very important one, I think we need to let the NIST standards play out and really push for far more collaboration between the public and private sector.

One anecdote. My company deals with some significant private sector companies that deal with the cyber issue, and one of them, which is a multinational corporation, walked into one of the alphabet agencies and said, “We have been hacked into,” and the alphabet agency said, “We know.” And they said, “Well, we are a tax-paying group of folks. Did you ever think it might be helpful if we sat down and worked together on it?”

So I think, again, focusing on collaboration and sharing rather than compliance is the best approach for the time being.

Chairman CARPER. Do you want some more time?

Senator BALDWIN. No. Thanks.

Chairman CARPER. All right. We made good use of that.

As we start a second round, I want to preface—let me just say, you mentioned Pat Gallagher, who did testify here before our Committee earlier this year—from NIST, and he said—every now and then witnesses show great wisdom. And in his testimony before us, I think he said, and I will paraphrase, he said, “We will know we are on the right track when good cybersecurity policy and good business policy are one.” That is what he said. I thought that was

pretty good advice. We have gotten a lot of good advice here today as well.

Let me also preface my next question by saying that here we are, it is the anniversary of 9/11. Here we are, maybe days before the United States could launch limited Cruise missile attacks at some targets in Syria. Here we are, knowing that we are under attack on the cyber front 24/7. And we have an Acting Secretary of Homeland Security, and we have an Acting Deputy Secretary of Homeland Security. And that just cries out for the Administration and for us to do our jobs, to make sure we have in place the kind of confirmed leadership that we need, capable confirmed leadership.

OK. That having been said, let me turn to a topic that I just mentioned, that is on our minds, and that is the potential for military action, limited military action, in Syria unless that country relinquishes its chemical warfare supply and dismantles their capability to create more chemical weapons.

The prospect of our using military force is a serious matter. It weighs on us all, certainly the President who came and visited our caucuses yesterday in the Senate, both Democrat and Republican.

I want to ask, as we prepare to make whatever decisions we need to make in the days ahead in conjunction with the President, I think it is important for us to get answers to a few more questions, and I would like to ask this seasoned panel of national security experts for some of your thoughts.

If the President does choose to take limited military action against the Assad regime, what impact do you think that might have on homeland security? What should DHS be doing to prepare for some potential consequences that would flow from U.S. action, even on a limited basis, against Syria? Mr. Baker, if you would like to lead off, that would be great.

Mr. BAKER. Sure, I will be glad to. We absolutely need to prepare here. By taking on Syria, we are also taking on Hezbollah and Iran, their backers in that regime. And if they choose to make the United States regret the sanctions it imposes, they have very substantial capabilities. Hezbollah has its own cruise missiles. And a terrorist organization with that kind of capability certainly can develop and use cyber attacks or can send people to the United States to carry out attacks.

So we would have to go on a pretty substantial alert basis. They would be biting off a lot. They are already on alert against Israel and fighting in Syria themselves, so they may decide that it is not prudent to attack, but hope is not a strategy for us. We need to be worried about our defensive capabilities. For the first time, we would face the risk that we will have a cyber attack aimed at getting us to quit engaging in military action.

Iran is widely blamed for a series of attacks on our financial institutions that have been visibly punch-pulling exercises in which the attackers announce how long the attack will last and what day it will happen. Obviously they could do more and cause more damage. And, again, Iran, having blamed us for Stuxnet, is going to be less constrained about using that kind of weapon against the United States on behalf of an ally like Syria. So we will have to up our game both physically and virtually.

Chairman CARPER. OK. Thank you. Admiral Allen.

Admiral ALLEN. Let me start with a caveat. It has been several years since I sat in a tank. I am not up to speed on operational briefings, so I am just going to talk in generalities. I would not want to speak for anybody or make any comments that would not be appropriate in this situation.

In regard to cyber threats related to any untoward act—and it could be generated by this—one of the problems we are dealing with right now is we are trying to evolve these structures, and we have talked about them extensively here today. It is tough to talk about how you would deal with one of these things when the answer is what you talk about you need to do and you have not done yet.

But let me focus on something called advanced persistent threat, which is something that is discussed both domestically and internationally, and it relates a little bit to what Stewart was talking about. There are footprints that are left regarding behaviors that go on out there that are indications of something that is going to occur. And one of the reasons the changes that need to be made in the cybersecurity posture in this country have been made and continue to be looked at in the Executive Order, the NIST standards, and everything else is that we need to move to continuous monitoring, and then after that we need to move to continually be able to look at the precursor or the context that is being set for an attack, and we do know what those are, and a lot of it has to do with basically analyzing social media, because people talk about this.

So in regards to any threat situation, and this one specifically, I think there ought to be a fine-tuning of our sensors out there related to what is being talked about in social media and what types of activities are taking place. After 9/11, we used to talk about chatter. Well, we have a much better capability now with—we have a mismatch in computation, spectrum, and bandwidth management in this country. We do not utilize enough against these problems. I think in this case we will be looking at advanced persistent threat because if they are going to do anything immediately, they already have had to put the mechanism in place to do it.

Chairman CARPER. Thank you. Governor Ridge.

Mr. RIDGE. Senator, I appreciate the question, and I must tell you, based on a personal relationship, because you and I have had many long conversations over the years about topics of national interest, I am going to resist the opportunity to tell you how I think we got into this mess and how I think we ought to get out of it and answer your question exactly.

It reminds me of the National Security Council coming over to what was then a small core staff between the time I was sworn in as Secretary and the intervening 6 weeks before we opened the door on March 1, 2003, the first day of the Department of Homeland Security. A couple members of the National Security staff came over and said, very confidential at the time, “We are probably going into Iraq. We know you do not have a Department, but maybe you should think about potential blowback in this country and what we can do about it to minimize the effect.”

So, one, I think your question is very appropriate and play the “what if” and then figure out how we respond if the “if” occurs.

I think we have learned a lot since Liberty Shield. I think, frankly, the State and locals are far better prepared. We know defense readiness condition (DEFCON)—even the much maligned and occasionally referred to color-coded threat warning system, which I will carry with me for the rest of my life, at least we know now there are certain levels of security that are embedded in the Federal Government and even within some of the State and locals and the private sector, No. 1.

No. 2, I think the most likely pushback would be in the cyber realm, and to that end, again, it is a great place for me to suggest that this is precisely where the Federal Government should be sharing the precursors that it may know or the addresses that it has seen as it relates to the digital incursions that we have been hit with from the Syrian Army, perhaps the Hezbollah and the like. This is a classic example where we probably, in this instance, are more familiar with the electronic incursions directed at us from Russia, from Syria, et cetera, and at precisely the time that that information should be shared with not just State and locals but with the private sector.

So, long term, I think we are far better prepared to respond to an attack because—I do think the word has been used—we are far more resilient today than we were 12 years ago. But this is an excellent opportunity for the Federal Government to share some of the information that I am sure they have that the private sector would like to check that information against what they see occurring on the grid, with the data systems, the financial institutions, and transportation, et cetera, to see perhaps if they are missing something and can be better prepared if there is an electronic attack or digital attack if we go into Syria.

Chairman CARPER. All right. Thank you all for those very thoughtful responses. Governor Ridge mentioned how he will take with him to his grave the leadership that he provided with respect to the color-coding alert. I am not so sure if there is some way to work that into your tombstone and the narrative of your life.

I was kidding my wife recently. She said, “Why do you spend so much time on postal reform?” Dr. Coburn and I, along with our staffs, spent an inordinate amount of time this year trying to reach an agreement on bipartisan legislation. But she was kidding me about something about postal, and postal reform on my tombstone. And I thought out loud and said, “Well, maybe what would be appropriate would be just these words: ‘Return to Sender.’”

Mr. RIDGE. Again, it is a classic example of something that the Congress is going to have to deal with. I believe—look, we know that Russia and China have cyber attacks as part of their public warfighting strategy. We know this is a condition of not only military and diplomatic but business activity, international activity for the rest of the world. But, again, it is a place where you need the private sector and the public sector to sit down and really cooperate and determine if there is an attack, what are the consequences and who is responsible for returning it to sender? I mean, all this has to be worked out, and, again, I think that just calls for collaboration, cooperation, communication, and it does not require for a regulatory scheme where you check the compliance box and everybody feels that they are safe after that.

Chairman CARPER. All right. Thanks so much. Dr. Coburn.

Senator COBURN. I think Governor Ridge agrees with this. I would love to have the other panelists' thoughts. We spend billions on grants every year. Is it your opinion that those grants ought to be risk based rather than parochial based?

Mr. RIDGE. Absolutely.

Senator COBURN. Admiral.

Admiral ALLEN. Senator Coburn, following the attacks of 9/11—I was the Atlantic Area Commander, as I said earlier—I was concerned about the posture of our ports on the east coast, and I put a team together that developed a port security risk assessment model that now is called the Maritime Security Risk Assessment Model by which we look at impacts, trading off what you are protecting in a port based on risk and consequence.

I remember having a conversation with Secretary Chertoff about implementing that at the secretarial level across the Department to inform the grant programs, and early on we had a pretty significant impact in doing that because there was a lot of logic attached to what we did, until Secretary Chertoff ran into the buzz saw which is called New York City. And we are all still stinging from that adventure a couple years ago.

I unequivocally agree with you it ought to be risk based. It ought to be conditions based, based on the adherence of local communities to standards like the National Incident Management System (NIMS). It ought to be, in my view, linked to how they are making decisions on land use and reducing risk. I think there is every argument in the world to do that in a constrained budget environment.

Senator COBURN. Thank you.

Mr. RIDGE. Senator, may I make just one quick comment if I may?

Senator COBURN. Sure.

Mr. RIDGE. Because, again, I do not want to go back to the reorganization of Congress, but it just conjures up a couple conversations I had when we were trying to move it to risk based. And I could not agree with you more than my colleagues. Every dime going out the door ought to be risk based. But I think the Department of Homeland Security, of all the agencies in the Federal Government, is probably more susceptible to political meddling and interference and impact than any others.

I will give you a perfect example. Once we got into the second year of the Urban Security Initiatives, action initiatives, we had the FBI talk about and the intel community really assess based on the prior year's intelligence gathering and try to come up with a risk assessment model vis-a-vis the cities that were potentially impacted, just given the volume and the credibility of the traffic.

Long story short, from 1 year to the next, we took several cities off because on a risk-based analysis of the preceding year, they were no longer on the priority list. And the hue and cry from Congress, those who represented those communities, was not deafening, but it was fairly loud—not that we listened to it, but the fact of the matter is that it ought to be risk based, and I think you are on to something very important. But the whole system should be risk based.

Senator COBURN. One of the things the President proposed that I agreed with—I was kind of a loner on this Committee—is combining all these grants together to where you really have an efficient, effective grant program where you set metrics, there is transparency to it, you are following up, and if they are not following what the grant was for, you jerk the money. So that we actually saved money by consolidating the grant programs, and then we had more money to actually go where the greatest risk is. And then we followed up to make sure there is compliance with what the grant was for.

They got a pretty good cold shoulder here in Congress on that, and I got a cold shoulder when our Committee marked up while we were still doing things on the basis of parochial rather than risk based. As a matter of fact, that is in the law. Rather than risk based, we are doing it on a parochial basis.

Any recommendations on how we can accomplish that? I do not know whether you agree with the President's recommendation of consolidating these grants and then using them on a risk-based process. Any recommendations, one, on how we would do that; and, two, whether or not we should do it?

Mr. RIDGE. Again, without knowing specifically the recommendation, it is just very consistent with my thinking as to—after 10 years of maturity and 10 years of growth, sometimes I think growth has not meant we have become more efficient or effective. It just seems to me that homeland security is all about risk management and resiliency, and the dollars out the door to be based on some kind of assessment, and it would be well to bring that philosophy to everything they do as well as the approach in terms of appropriating dollars for these grant programs.

You might want to allow for—and I am going to speak and be very interested in my friend and colleague Thad Allen. I am not sure we have done quite enough with regard to maritime risks, port risks. So you may want to divide that aggregate, some might be into two or three verticals whereby you identify the greatest risks, one of which could be the maritime industry, and move on from there. But I know there is a duplication of programs and oversight, and I do not think it is needed and everything out the door to be risk-managed at this point.

Senator COBURN. Admiral Allen.

Admiral ALLEN. Yes, Senator, early on there was a port security grant program as well, and just one vignette associated with that. Then I would like to attack the larger issue that you raised.

I was prone to support requests for grants in areas where I saw that there was not only a recognition of risk but a commonality of purpose and regional approaches. And we saw some areas—one of them is Houston—where they came together and they created a regional entity by which they consolidated all their requirements that came in for a grant program. I think whenever you can do that, that kind of behavior ought to be encouraged.

Whatever you put in place—and this is going to be a lousy metaphor, but it is the only one I can come up with on the seat of my pants here—it is almost going to have to have an ironclad wall around it that allows it to be executed like the Base Realignment

and Closure (BRAC) program, an up-or-down vote, this is what we decided; it is executed or it is not executed.

Mr. RIDGE. Yes, I like that.

Admiral ALLEN. And I do not know how you structure that in law, but you are almost going to have to have a way where, once we decide how it is going to be done, the criteria are established and the decisions are made that it is irrevocable, it is either up or down, and it cannot be picked apart.

The issues, I saw Secretary Chertoff just get wire-brushed up here, ran into the political buzz saw in New York after even trying to diminish the funding, and it is not to say that New York does not have problems, but that was a very difficult time for us at the Department.

Mr. BAKER. I think Admiral Allen raises a point that is worth thinking about in terms of how much of your personal credibility and time you would invest in that, because even after you have built a pretty good risk system for grants, politics will not disappear, and that risk system, whatever it is, could get distorted by the kinds of politics that Secretary Chertoff encountered, and others have.

And so you may at the end of the day end up with a less mechanical system, but not one in which the politics have been eliminated. And at that point, it is possible you will ask yourself, "How much did I really achieve by introducing this risk concept?" I believe in it, but in practice, I am not sure that it works out as well as one imagines.

Senator COBURN. Well, thank you. My comment on that is you need a backbone, the person that is running the agency, and take the heat, but do what is right for the country. When we have a Bearcat garden, a pumpkin festival in Keene, New Hampshire, and you say what could those dollars have done to either protect us on cybersecurity, advance our intelligence, what else could we have done? So we are not using any cost/benefit analysis. What we are doing is parochial—dividing up the pie, and we are at a point where, first of all, this country cannot afford to do that anymore. We do not have the pleasure of doing that.

And so I think the next Homeland Security Secretary, that is going to be one of the qualifications I am looking for: Are you ready to take on the fight to do what is best for the country, not what is best for the politicians?

Thank you.

Mr. RIDGE. I think it would make the next Secretary and future Secretaries—you are right, a backbone will be essential. But it would be nice to have the institution that applies so much pressure, changing their jurisdiction, so, you know, the fact that you can apply pressure institution-wide is because they are answerable institution-wide. You start reducing that to a reasonable, necessary oversight and collaborative process, it will be a heck of a lot of pressure if the decisions—the legislative decisions that the Secretary is obliged to follow is reduced rather substantially and, therefore, held accountable to Senators Carper and Coburn.

Admiral ALLEN. Mr. Chairman, could I make one quick comment?

Chairman CARPER. Sure.

Admiral ALLEN. There are a lot of different grants out there. I am specifically going to refer—because I saw Senator Coburn on television making very strong statements after the tornadoes in Moore, Oklahoma. And this gets back to an earlier statement by Jane Harman. In the passage of the emergency supplemental following Hurricane Sandy, there were some very deft and artful amendments to the Stafford Act that got inserted into that bill that created more leeway and flexibility for local governments to deal with things like debris removal, where there was an economic incentive for them to do what was best for them, but also preserved those funds and allowed them for another use.

So I think there may be some utility in looking at what we were able to do, and I realize that was a really unusual way to amend the Stafford Act, but I think there may be some insight there to be gained on how you can empower local communities with flexibility so there is an economic incentive for them to do what is right and build off a concept like that, sir. And I congratulate everybody on that piece of legislation, by the way.

Chairman CARPER. All right. Thanks.

I believe it was back in March, Dr. Coburn and I held a hearing in this room to examine the progress that has been made and some of the challenges that still remain within the management of the Department of Homeland Security. I am sure that all of you are aware of the latest high-risk report from the Government Accountability Office (GAO) that found the Department had made considerable progress in integrating its components, moving toward actually having auditable financials and, we hope, an unqualified audit soon. But the overall management of the Department remains on GAO's high-risk list, and I have been really impressed by the efforts of the Department's leadership to address these management issues.

With the changing of the guard, the impending changing of the guard at the top of the Department, there are still a bunch of questions about how the Department can sustain and build upon the work of Secretary Napolitano and also, I should hasten to add, Deputy Secretary Jane Holl Lute.

What do you view as the most urgent steps that the Department should take to develop strong management institutions and practices? That is the question. What do you view as the most urgent steps that the Department should take to develop strong management institutions and practices, to further develop those practices? And are there any legislative steps that come to mind that those of us who serve on this Committee and our colleagues ought to take to strengthen the tools and institutions that the Secretary needs to manage the Department?

And a last quick question. Admiral Allen, you were there, I think, when we cut the ribbon on the new Coast Guard headquarters at St. Elizabeths. Were you there?

Admiral ALLEN. I was not, sir. I was on travel that day.

Chairman CARPER. That was a special day. I wish you could have joined us. But how does the consolidation of DHS' headquarters at St. Elizabeths play into management improvements? Those three questions, if you all could take a swing at those, three strikes, three pitches. Just make sure your—

Mr. RIDGE [continuing]. Those fast balls, Senator. I am familiar with the report, not the contents of the report, with regard to management. I have often said that the Department of Homeland Security from the get-go had two responsibilities that it had to deal with simultaneously: one, build a safety and security platform to deal with risk and resiliency; the other was the business line integration. It is a business. It is a budget that has doubled. You have a couple hundred thousand employees, and one of the ways—one of the regrets—and it is something that you could not do anything about—is if you were going to merge 20-plus agencies with multiple missions, with multiple procurement requirements and budget requirements, et cetera, in the private sector, you would at least have had a year or so by the time you got all the Federal and State regulatory approvals, because Homeland Security was and still is about mergers, acquisitions, divestitures, and startups. And the management around those things for the past 10 years apparently, according to the GAO, has not dramatically improved.

I frankly do not have an answer. I think that we have had some really good people there trying to get those things done. But absent buy-in from some of the management changes and the restructuring that they might recommend, and that is, buy-in by the Congress of the United States, it is pretty difficult to make reforms.

I think that it is not just endemic to Homeland Security. I just truly believe that there are still silos within that agency that will require—that have to be merged, and it can only be done with legislative oversight and direction.

I like the notion of consolidating. I hope you find money to build out St. Elizabeths, because as Secretary, when we would have periodic meetings with the leaders of the basically five or six really muscular agencies—they talk about 20 departments and bureaus, but basically there were five or six that provided most of the employees, and the rest were just bits and pieces from the other units of government. And to try to pull your leadership together a couple of times a week, taking them from their offices and bringing them over to the Nebraska Avenue Complex (NAC) and sitting down for 2 or 3 hours a couple times a week was not a good use of their time or ours. We had the opportunity to develop the kind of day-to-day working relationship that I think Congress wanted when it put these agencies together. It was a tremendous opportunity for disparate pieces of Homeland Security, and it has been demonstrated tactically with Customs and Border Protection working with the Coast Guard, working with ICE. The collaboration is important. But I think you get better management if you have the chief leaders of the entity interacting on a day-to-day basis rather than piecemeal.

I also think you get better management and efficiency if the restructuring that has been recommended by some of us from the outside and the Department of Homeland Security is put into law.

Chairman CARPER. OK. Thank you. Admiral Allen.

Admiral ALLEN. Mr. Chairman, this is an area I have a great passion about, so do not feel bad about cutting me off here. Let me hit a couple of these issues.

One of the things that happened when the Department was created was we aggregated the authorities and the jurisdictions from

the legacy departments. But one of the things that has been insidious for over 10 years now—and I know this from talking with staff on the Appropriations Committees—is that we took the appropriations structures from the legacy departments—Treasury, Justice, and so forth—and just moved them to a single committee. There is no comparability in the Department right now between components on what is a personnel cost, an operating cost, and a capital cost. And because of that, you cannot compare and tradeoff between components on where you want to make investments.

I have said in several hearings, both here and before the House, that in my view you have to get down to blocking and tackling if you are going to take on the management issues in the Department, and the first area should be to standardize the appropriations structure and how the budget is presented to the Congress in terms of the justifications so there is comparability. The Congress cannot make good decisions unless there is more transparency and comparability across the Department. That leads to financial management and the ability to have better insight on how you are spending your money.

They got a qualified opinion on their audit this last year. That was a major breakthrough. The Coast Guard got a qualified opinion, the first military service to ever do that. That should be taken as the floor, the minimum expectation. It needs to move forward. But you are starting to talk about the integration of IT systems, financial systems. There are three major financial platforms that are used in the Department right now. There is going to be a look this next year at shared services and maybe a better way to do this.

I think all that has to come on the table, and we have to look at really trying to integrate this enterprise and make it run efficiently like you would if you were running a corporation.

Now, regarding St. Elizabeths, I have to kind of sit on my hands here. I was the Commandant when we made the decision to move, and all I said was: “I can support this; I am behind it. I just don’t want to go there without the Secretary.” And I will leave it at that.

There are issues with the Federal buildings funds. There are issues with how this whole project has been funded, issues with the District of Columbia planning entities. But the overriding imperative to have a central operations center from which the Secretary can operate and make decisions, as Secretary Ridge said, is a primary need in this Department. It is my written testimony. I will not belabor the fact here. A National Operations Center at a unified Department, operations and situational awareness, absolute imperative moving forward.

Chairman CARPER. All right. Thank you. I think you can control those passions pretty well. Thank you. Mr. Baker.

Mr. BAKER. I would certainly agree with Admiral Allen on St. Elizabeths. They say in Washington that where you stand depends on where you sit, and I do think that if DHS components sit together, they are likely to stand together much better than they do today. And so to the extent that we can get everybody in one place, we are much better off.

I, too, am a little reluctant to make suggestions for changing the details of management in a Department that I left a few years ago.

I think that there are probably some opportunities with respect to the Quadrennial Homeland Security Review (QHSR) to turn that from an exercise in which we look at some very interesting and difficult issues into something that turns our budget into a multi-year, thoughtful priority-driven exercise rather than something in which we ask how much money do we have and what can we cut. And to the extent that authorizing legislation can move the Quadrennial Homeland Security Review in the direction of actually influencing budget decisions, I think that would be an enormously effective way of dealing with the looming crisis we have with respect to appropriations for everybody, and making sure that the cuts are much smarter than they otherwise would be.

Chairman CARPER. Thank you.

Before we wrap it up, let me just telegraph my final pitch, and that is, sometimes when we have a hearing like this, I like to invite our witnesses just to give a brief closing statement, just a couple of thoughts that you want to kind of pull together, just underline a few things and leave those for us. I would welcome, I think we would welcome that.

Let me just yield to Dr. Coburn for any last comments? OK.

Mr. Baker, do you want to give us a closing thought or two before we wrap it up?

Mr. BAKER. Yes. Nothing has made me prouder or caused me more frustration than my service at the Department of Homeland Security. I am deeply fond of the institution, and I believe that it is making a major contribution to the security of all Americans. It has changed our approach to the border in ways that nothing else could have, and that has paid dividends in almost every terrorist incident that has been planned or launched against us since 9/11.

We need the Department, but we need it to be better, and we need it to be more organized, more consolidated, more coordinated. That is the biggest challenge that the Department faces. We have gotten by with three great leaders, but we cannot count on personality-driven unification forever. We need to institutionalize it.

It is a big challenge, especially with the oversight authority that exists, but it is a challenge that you have the support, I am sure, of everyone on this panel in your effort to accomplish.

Chairman CARPER. All right. Thank you, sir. Admiral Allen.

Admiral ALLEN. Mr. Chairman, in regard to some of the mission areas that we have talked about today—cybersecurity, immigration reform, and so forth—a lot of that is going to necessarily involve the Congress to do that. I sit on the Advisory Board of the Comptroller General, so I am aware of the risk areas. Gene Dodaro and I have talked about this before.

I believe when it comes to the internal management of the Department of Homeland Security, there are adequate authorities in the Secretary, administrative space to operate. I think there needs to be a serious discussion about conditions of employment and a management agenda related to mission support activities and functional integration in the Department for the next leadership team moving in. And those ought to be clear and distinct, and they ought to be enforceable in the budget. And they ought to be laid out with metrics attached, as Senator Coburn would probably want.

I do not believe any legislation is needed to take care of the management improvements that the Department could implement immediately.

Chairman CARPER. All right. Thank you. Governor Ridge.

Mr. RIDGE. When you look back on those days when there was considerable debate in this town as to whether or not we actually needed a Department of Homeland Security, I remember my friends on my side of the aisle said we are creating a brand-new bureaucracy of 180,000 people. And I hopefully reminded them and they believed me that they were not new jobs; we were just going to consolidate units of government that historically had missions related to protecting our borders and gaining knowledge about the people and the goods that come across our borders.

Long needed in the 21st century world when the interdependency of the marketplace, the interdependency of information sharing for law enforcement purposes, and the interdependency of countries with regard to security is a part of our daily lives and how we are going to live. We are interdependent.

But I think the Congress did the wise thing. I do think they brought together the right agencies. I think the Department has evolved and matured, but I am reminded of Sean O'Keefe's phone call to me after I was announced as being the President's nominee to be the Secretary of the Department of Homeland Security. He said, "Tom, a couple of decades ago, we saw"—there was a smaller aggregation of responsibilities that created National Aeronautics and Space Administration (NASA), and he said, "Decades later I still see the vestiges of culture in silos in this entity and in this organization."

So, one, I do not think we should be surprised that we have not made as much progress as we all think we need. We are not as efficient as we need to be. We are not as risk-managed and risk-based as we need to be. I do not think anything is wrong with the management structure. I do think there needs to be efforts to oversee the oversight of that structure to hold both the Congress and the Department far more accountable for the outcomes we want.

At the end of the day, I think you have touched on some very important issues, and I am proud to have spent some time with these panelists. It is about information sharing. It is about resiliency. It is about risk-managed approach.

I would hope you can resolve these issues. I realize that, again, ironically enough, the issues that I just raised are not necessarily all within the exclusive purview of this Committee, which speaks to one of the challenges I think the Congress has. But at the end of the day, I am proud to have been the first Secretary. I think they have made marvelous progress. I would like to see some of it accelerated. I am just not convinced because it got bigger it has gotten better. I do not think it has. And that has nothing to do with the well-meaning intentions of the people who go to work there every single day to make you and me safer and more secure. It just does not have the kind of collaboration and oversight with the Congress that I think is absolutely essential.

At the end of the day, the mission is the same at the Department of Homeland Security. Make our country safe and secure. Do it in a way that is consistent with the Constitution and the rule of law.

And the big challenge associated with that has been with us since 2003. But with the Snowden revelations and the vast impact of the digital world and the cyber world, that challenge to maintain that privacy of individuals and the protection of these rights under the Constitution becomes more complicated for this Committee and for the Congress of the United States. And I look forward to future invitations to share my point of view with all of you who are committed to making a stronger and better Department. And I thank you very much.

Chairman CARPER. It is we who thank you. We thank you for this day. We thank you for your preparation for this day and for this conversation, and for your continued service to our country. I have a closing statement I am going to submit for the record.¹

And I will just say this: I think some remarkable progress has been made in the 10 years that has passed. Thank you for that initial leadership, Tom, as this Department was launched, and to Admiral Allen and Mr. Baker for your great leadership as well. This is as much progress as may have been made. There is clearly more to do. It is not a time to rest on our laurels.

I like to say that everything I do, I know I can do better, and clearly the same is true in terms of protecting our homeland.

So we leave here knowing that on this very special day we have learned a lot of lessons, and I think we have taken a lot of the appropriate steps to better secure our Nation. But obviously there is a whole lot more that we can do.

Dr. Coburn gave me a really good idea earlier this year, and that is that we should do a top-to-bottom review of the Department and try to figure out how we go about reauthorizing the Department. He said this is an appropriate time to start that process. And what you have done today in laying out for us really a banquet of knowledge, just a font of great ideas, this is enormously helpful to us in this process. So we thank you for all that. It is great to see you.

I want to thank our staffs for pulling this hearing together. You have all done a great job, and we are grateful to each of you.

With that having been said, the hearing record will remain open for 15 days until, I think, September 26th at 5 p.m. for the submission of statements and any questions for the record.

With that, again, our thanks and our thoughts and prayers for those whose lives we remember today. God bless. Thanks.

We are adjourned.

[Whereupon, at 12 noon, the Committee was adjourned.]

¹ The closing statement of Senator Carper appears in the Appendix on page 485.

A P P E N D I X

**Opening Statement of Chairman Thomas R. Carper
The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and
Addressing Emerging Threats
September 11, 2013**

Today marks the twelfth anniversary of 9/11. It is a day for reflection – not only on all that we lost that day – but on the sense of unity that brought us closer together as a nation in the wake of a terrible tragedy. This anniversary also provides us with an important opportunity to think about all the efforts we have taken to secure our country since that fateful day, as well as the challenges that lie ahead.

With us today, we have a remarkable group of witnesses that will share their thoughts on what we have accomplished since 9/11 and the future of homeland security. I would like to thank each of them for being here today and for their valuable service to our country.

This year, the Department of Homeland Security turned ten years old. While I'm sure we can all agree that the Department can do a better job in certain areas, we should not forget about the remarkable progress that has been made in keeping Americans safer. There is no doubt, in my view, that we are safer today than we were ten years ago.

I'd like to take a few minutes to highlight some of the more significant accomplishments:

We've enhanced aviation security through a more risk-based, intelligence driven system that begins screening passengers against national security databases four days before they board an airplane;

We've improved our preparedness for and ability to respond to disasters, while cutting red tape at the federal level.

We saw the fruit of these efforts in the response following the Boston Marathon bombings and also the natural disasters that have struck us recently, including Hurricane Sandy;

We've increased the security of our nation's borders with historic levels of manpower and resources; and

We've built up cyber security capabilities to work with the private sector and federal government agencies in preparing for, responding to, and mitigating against, the ever growing number of cyber attacks.

"But is there still room for more improvement? You bet there is. As I like to say, "the road to improvement is always under construction." One way the Department can improve is by doing a better job of preparing for tomorrow's threats -- today.

We do a good job at fighting the last war and preparing for the last type of attack, but to secure our homeland we must be better at anticipating the next type of attack. Ten years ago, for example, very few people were even talking about cybersecurity. Today, we can hardly go a day without reading about a cyber attack in the news.

To respond to the challenge of ever-changing threats, we need a Department of Homeland Security that is flexible and ready to adapt when necessary. And sometimes, we just need to use some common-sense. If a program is not working, we shouldn't just keep throwing good money after bad. Rather, we must work smarter with our limited resources and find ways to get even better results for less money.

That is why Dr. Coburn and I are holding this hearing and a series of others.

We are conducting a top to bottom review of the Department so that we can learn from instances where the Department succeeded and where it came up short. This information will help us focus our scarce resources on what works.

As the Committee conducts this review process, we will be looking to ensure that the Department is making smarter acquisition decisions, developing a stronger workforce, and improving its financial management systems. This review will also look at how we can strengthen the defenses of our homeland against very sophisticated and highly agile threats.

One of the most important things we can do to improve homeland security is to come together to pass cybersecurity legislation. The threat is too great, and the consequences of inaction are too severe, to do nothing. Passing a cybersecurity bill will not be easy. But, we have a shared responsibility -- Democrat and Republican, House and Senate, government and industry -- to get this legislation into the end zone.

We already saw many of these different parties come together to pass comprehensive immigration reform in the Senate a few months ago.

I do not agree with everything that is in the bill, and I know that Dr. Coburn does not either. But I believe that it is vastly preferable to our current immigration system, the failings of which undermine both our national and economic security. It is my hope that the House will pass its own version of immigration reform so we can go to conference and pass this historic piece of legislation.

So as we remember 9/11 and discuss the challenges that lie ahead, we must seek to recapture that spirit of unity that prevailed twelve years ago if we are to succeed in making the Department of Homeland Security stronger over the next ten years. I look forward to working with our members, our witnesses, and the Administration to achieve this goal.

Closing Statement of Chairman Thomas R. Carper
“The Department of Homeland Security at 10 Years: Examining Challenges and
Achievements and Addressing Emerging Threats”
September 11, 2013

My thanks to each of our witnesses for their contribution to this hearing and to my colleagues for joining us today.

As we all know, we live in complicated and challenging times.

Every day, we are faced with targeted cyber attacks against our federal networks and critical infrastructure.

Even after the elimination of Osama Bin Laden, Al-Qaeda and its affiliates are plotting to carry out damaging attacks against U.S. interests at home and abroad.

Over the past year, natural disasters such as Super-storm Sandy and the tornadoes that ravaged parts of Oklahoma reminded us of the devastation and disruption that nature can bring to bear.

And our nation’s growing deficit problems and fiscal challenges have made it even harder for the federal government to address these issues.

The Department of Homeland Security was born out of a need to have one government agency in charge of preventing terrorists from coming to our shores and threatening the American people.

Over these first ten years, the Department has seen many successes, as well as some challenges.

Our witnesses today shared with us some of the areas where the Department has thrived and fulfilled its mission to protect the homeland. I am encouraged by these successes.

However, our panelists also pointed out the areas where Department needs to do a better job and made their recommendations for how to do so. Today’s discussion will help this Committee build a roadmap for strengthening the Department of Homeland Security.

I look forward to partnering with Dr. Coburn and the rest of my colleagues on this Committee to work toward this objective.

The hearing record will be open for fifteen days for the submission of additional statements and questions.

This hearing is adjourned.

Opening Statement by
Sen. Tom Coburn, MD
Ranking Member

September 11, 2013 HSGAC Hearing:

"The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats"

This 12th anniversary of the September 11th terrorist attacks is a sobering reminder of the threats that we face and our responsibility to keep America safe. The Department's original mission was focused on counter-terrorism: sharing intelligence and coordinating between agencies.

Today, DHS's mission looks very different, and it's unclear that the original mission is being fulfilled. The Department's original counter-terrorism mission has transformed into an "all-hazards preparedness" mission, including subsidizing state and local public safety spending.

Given the \$17 trillion national debt and the federal government's growing obligations, we do not have the luxury of continuing to increase DHS's mission, programs, and budget. Instead, this Committee and the next DHS Secretary have a responsibility to focus the agency on a clear mission for the next decade.

There are several big lessons we have learned and challenges that must be addressed. Ten years after DHS's creation, we still can't measure how much safer we are due to spending on homeland security.

As our December report on DHS Grants – "Safety at Any Price" – found, more than \$35 billion has been spent on DHS grant programs since 2003.

These were intended to make Americans safer from terrorist attacks. However, 10 years and \$35 billion later, DHS still does not know how to measure whether these funds were used to make Americans safer.

Another example is federal support for state and local fusion centers. Our bipartisan PSI investigation into DHS's fusion center program found that it was unclear exactly

how much DHS was spending on fusion centers¹ or even how many were actually in operation. Our investigation found that despite spending as much as \$1.4 billion, the fusion center program was yielding little value for the federal government's counter-terrorism mission and the work of the intelligence community.

And earlier this year, we learned during the aftermath of the tragic Boston bombing incident that the fusion center wasn't providing much value either before or after that attack.²

Perhaps the most disappointing return on investment is at our borders. Despite spending \$90 billion³ on border security over the past decade, our borders are not secure and our immigration laws are not been effectively enforced.

When we asked DHS to explain their border security strategy, they have been unable to provide us a document which demonstrates they have a comprehensive approach to securing the border.

That lack of planning has consequences, and results are more illegal crossings. The Council on Foreign Relations surveyed the illegal immigrant population and recidivism rates and found that an illegal immigrant would be stopped is closer to 40 to 55 percent, not the 80 or 90 percent figure that we have heard from DHS.

And we have heard very basic concerns about DHS's commitment to enforcing the rule of law and our nation's immigration laws, including from the Department's own ICE agents and US Citizenship and Immigration Services (USCIS) officers.

Another serious challenge is finding competent and willing leadership. DHS continues to struggle in the area of management. A lack of strong management can cripple efforts to implement the changes needed to improve the department.

As Governor Ridge can surely tell us, standing up, coordinating, and integrating 22 separate agencies into what has become an organization that employs more than 200,000 people is no easy task. While DHS deserves recognition for the progress it has

¹ The PSI report estimated that between \$289 million and \$1.4 billion in federal appropriations were spent on the fusion centers between 2003 and 2011.

² For example, at the Boston hearing, you asked the Boston Police Commissioner whether the fusion center was providing any intelligence after the bombing that was not being provided through other channels, such as the JTTF. He answered that it was not.

³ "\$90b spent on border security, with mixed results," *Associated Press*, June 26, 2011.

made in this area, continued management challenges are undermining the Department's ability to confront emerging threats.

DHS relies heavily on contracts to field new IT systems and capabilities that directly support its most critical missions, but we know these programs are still often over budget, behind, and deliver less than the men and women on DHS' front lines need.

DHS also faces a leadership vacuum. As of August, 15 senior positions remain vacant, and we do not have a nominee to serve as the next Secretary. Combined with morale levels that are among the lowest in the federal government, this poses a significant threat to DHS' ability to meet any of its missions.

Before further expanding DHS's mission—and giving DHS broad new responsibilities, like cyber security—we need to make sure the Department is well-equipped to manage these responsibilities.

The Obama administration and others would like to significantly expand DHS's role in cyber security, including overseeing federal and private sector cyber security. While cyber security is one of the real and emerging national security threats that we will face moving forward, we should be cautious and thoughtful about whether DHS can provide value, and if so, where that might be.

In other areas, such as the CFATS program to protect chemical security facilities, DHS has struggled when it has been tasked to be a regulator. I am concerned that we would be setting the Department up for more failure if we gave it broad responsibilities over private sector cyber security, which is a far more challenging and dynamic technological problem to address.

This is particularly the case since we know that, according to GAO and the DHS Office of the Inspector General, the Department has struggled to manage its own cyber security responsibilities—and even the agency's own cyber security!—effectively. For example, the DHS OIG tells me that 45 of its recommendations for cyber security remain open as of August 2013.

Before trusting DHS with significant new responsibilities for cyber security, our Committee and the next Secretary should carefully review DHS's existing cyber programs—including its management of the executive order—to determine where DHS can provide a valuable contribution to address that real and emerging threat.

This anniversary also provides a good opportunity to look at the work of this very committee, which was instrumental in creating the Department. Have we provided the necessary oversight to help the department succeed?
Are we asking the right questions – the hard questions – and insisting on transparency?

It is not enough for us to create a new Department and call it a day. If we expect success from DHS, we must hold it accountable for its shortcomings, or we are as much to blame as the department's leadership, regardless of party.

**Opening Statement of Senator Jeffrey S. Chiesa
at the
U.S. Senate Committee on Homeland Security and Governmental Affairs
Hearing on
The Department of Homeland Security at 10 Years:
Examining Challenges and Achievements and Addressing Emerging Threats
September 11, 2013**

Thank you, Mr. Chairman and Senator Coburn for convening this important hearing today. Your leadership of this committee is helping to keep our country safe and I know I speak for all Americans in expressing my appreciation for the outstanding job you are doing.

Twelve years ago, the United States confronted, really for the first time, the enormous challenge of protecting our country, our people, and our way of life from terrorists and others who would inflict on our country the sort of previously unimaginable destruction we suffered that day.

For the first time in decades, the United States was attacked on its own soil. No one in this room – indeed, no one who experienced the events of 9-11 – needs to be reminded of the shock, the pain, the fear, and the uncertainty that every American experienced.

The memories are indelibly etched on our minds and on our souls.

One common refrain during the days following 9-11 was that nothing would ever be the same again.

And there is no denying that in many ways, both large and small, our lives have changed.

Because of the very real threats we face, we have become vigilant in new ways. And that vigilance has come with a cost – both in terms of the money spent and in terms of the impact on our daily lives.

But it is also important to remember that this vigilance is, in no small measure, also the price of our liberty.

The overarching success of the policies, procedures, and institutions established in the weeks and months following the attacks on America are self-evident.

As Governor Ridge often noted, in fighting terrorism we have to succeed 100 percent of the time in our mission; the terrorists only have to succeed once.

And while they have not succeeded, we have.

That record, however impressive – and it is impressive – should not preclude us, from time to time, from evaluating the ongoing efforts our government is making to secure our country. We must be looking for ways in which we can improve the defense our country so that we can continue to be successful 100 percent of the time.

After all, every policy, every procedure, and every institution changes over time.

Sometimes the change comes about through careful study and consideration.

Other changes, however, can occur organically, in the form of "mission creep," and those changes do not always contribute to the overall success of the goals we all share.

And just as we must evaluate the changes that have occurred over the past dozen years, we must also recognize the existence of bureaucratic inertia. The often-heard phrase "But we've always done it this way," is an enemy of the vigilance we must continue to practice.

There's no doubt that terrorists are continually adapting to the measures we put in place.

They are constantly probing to find the weak spots in our security. They look for the most vulnerable places to strike, bypassing the least vulnerable targets. That is why this hearing is so important.

Our witnesses have the experience and the knowledge to inform this committee about what has worked and what needs improvement. They can also help us evaluate the shifting nature of the threats we face.

I am looking forward to the testimony of our witnesses, each of whom has earned the respect and gratitude of this country for giving so much of themselves to ensure that we remain vigilant in the defense of our country and our liberty.

Thank you, Mr. Chairman.

As Prepared for Delivery

**The Honorable Tom Ridge
President and CEO of Ridge Global
First Secretary, U.S. Department of Homeland Security**

**Senate Homeland Security and Governmental Affairs Committee
September 11, 2013**

***The Department of Homeland Security At 10 Years:
Examining Challenges and Achievements and Addressing Emerging Threats***

Good morning, to my former House colleague, Chairman Carper. To Ranking Member Coburn, thank you for the invitation. To distinguished members of the Homeland Security and Governmental Affairs Committee, thank you for the opportunity to be with you today.

I am Tom Ridge, President and CEO of Ridge Global. Prior to heading Ridge Global, and following the tragic events of September 11th, I became the first Assistant to the President for Homeland Security. In 2003, I was honored to become the first Secretary of the U.S. Department of Homeland Security (DHS), where I had the privilege to work with more than 180,000-plus dedicated employees of the department.

I am testifying today in my personal capacity. However, I also chair the U.S. Chamber of Commerce's National Security Task Force. The task force is responsible for the development and implementation of the Chamber's homeland and national security policies and is a voice for businesses across America—both large and small. This position certainly informs my perspective on many issues.

I welcome the opportunity to appear here to examine ways in which we can secure America's future. I recognize that we have limited time here, so I request the opportunity to revise and extend my remarks for the record.

Before I begin I want to, on this anniversary, acknowledge the families that lost loved ones on September 11, 2001. We all love our country. The reason we are here is to work together to do our best to ensure that such events do not happen again and that other families do not have to suffer like those of our 9/11 heroes.

I was invited here today to provide my views on *The Department of Homeland Security At 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats*.

With your indulgence, I would like to make two general observations first, and then focus on what I believe is a cross-cutting issue that both DHS and the broader federal government have faced in the past-- and it has the potential to complicate our future.

It is becoming clear that members of this body intend to pass some form of immigration reform. DHS components can be expected to play a significant role in implementing these reforms. My position is that the time has come to grant status to those who wish to enter to our

country legally, to work lawfully, and to pay taxes. But unless the Congress balances this approach by providing for effective enforcement mechanisms and providing adequate resources to the men and women of Customs and Border Protection, ICE and Border Patrol, and Citizenship and Immigration Services (CIS), DHS will be unable to meet its mission, regardless of the political plan you put in place. We can talk about reaching consensus in Washington, but unless reforms are resourced, DHS components will be saddled with an impossible mission in the critical area of border security.

On a related note, I have been concerned about the number of critical senior-level vacancies at DHS. In particular, as Congress debates immigration reform and with tensions high in the Middle East, DHS has had no permanent Secretary, no confirmed Deputy Secretary or General Counsel. And vacancies remain for Director of Immigration and Customs Enforcement and Under Secretary for Intelligence and Analysis. While several key nominations were recently made, several of these positions were open for months. Earlier this summer, as many as 15 senior positions were unfilled. This comment is not directed at Acting Secretary Beers or other dedicated public servants who, in their acting capacities, are doing their best under the circumstances. Such a high number of DHS vacancies should be disconcerting at any time. I urge the Administration to fill remaining vacancies quickly and the Senate to, in a judicious but timely manner, exercise its advice and consent responsibilities.

Mr. Chairman and members of the Committee, considering your topic today: *The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats*, I would like to spend the rest of my time discussing the challenges of information sharing. This issue has been with us since 9/11 and cuts across a range of challenges that have and will continue to confront the dedicated men and women of the Department of Homeland Security and their partners.

The nature of the terrorist threat has changed. As we have seen in Iraq, Afghanistan and today in Syria, our enemy is no longer just Al Qaeda, but like-minded organizations and nation-states that are willing to ally themselves in order to harm their common enemy—the United States. In my opinion, this will require the intelligence community to renew its commitment to work more closely with one another than ever before. Congress, in its oversight role, should ensure that DHS specifically remains plugged into the federal intelligence community horizontal. For if intelligence indicates a physical or cyber threat against the homeland, DHS will be required to work with our partners along the vertical—with state and local governments and critical private sector owner-operators—to address the concern. Further, we should ensure that the great progress that has been made for information sharing with state and local partners—such as the establishment of fusion centers—continues to be nurtured.

No discussion of the DHS threat environment or about information sharing can be complete without discussing cyber security in more detail. There is no part of our national economy, infrastructure, or social fabric that is not in some way connected to the internet backbone. Our critical power and communications, transportation and product supply chains, and financial systems. And DHS owns many of these sector-specific relationships.

This cyber threat is not new or emerging. In fact, when I was Secretary, in 2003, a full decade ago, the first US *National Strategy to Secure Cyberspace* was released. Greater awareness of this threat may be emerging, but the threat itself has been with us and will be with us for the rest of our lives.

As the first Secretary of Homeland Security, I believe I have perspective on this issue. We learned after 9/11 that information sharing and coordination at all levels of government—and with the private sector—would be critical to preventing future attacks and being resilient if attacks did occur. This was acknowledged in the development of the initial *National Strategy for Homeland Security*, the *National Infrastructure Protection Plan* as well as numerous other strategic documents and subsequent revisions overseen by Secretaries Chertoff and Napolitano.

After Hurricane Katrina, in post-disaster report after post-disaster report, we learned that the private sector brought great capabilities to the response and that improving collaboration between the public and private sectors would be critical in future emergencies and necessary to make our country more resilient.

Now, today, threats in the cyber world are getting quite a bit of attention. I have heard many of my friends and colleagues from the intelligence and security communities say that we will soon be visited by a “Cyber Pearl Harbor.” I share this concern. The issue, however, is not whether government and private sector leaders recognize the threat. The threat is clear. The question is what do we do about it?

In the cyber realm, the US Government—from the White House and Department of Defense to the US Congress itself—has been unable to prevent many attacks on its systems. Meanwhile, US companies that employ millions of Americans are not only attacked by criminal organizations and lone wolf hackers, but also by Nation-States. Disruptions occur, business is being halted, data and proprietary information is being stolen, and our economy is being impacted. And many of our public and private networks are greatly interdependent.

At the end of the day, if we are not prepared to enable government and critical industries to share information and coordinate to prevent major cyber attacks and incursions, we will also be unprepared to respond together and to be resilient if and when attacks occur. In this sense, we are just as vulnerable to experience a “Cyber Katrina”—that is, experience a disaster on top of a disaster—as we are to realize a “Cyber Pearl Harbor.”

Information sharing and public-private partnerships must be foundational to our national cyber security and resilience efforts. I applaud the President for issuing his Executive Order on Cybersecurity and for pursuing, through NIST, a public-private framework. This is a positive and important step. But I would caution against leveraging this process as merely a path toward prescriptive mandates.

In a world that sees data move at the blink of an eye, you will not be able to legislate or regulate fast enough to stop the evolving dangers we see—or do not see—in the cyber domain.

I know that some members favor a prescriptive approach to cyber security because of the legitimate concern that critical infrastructure will be impacted. But if we know that Nation-States and terrorist groups are probing and attacking the systems of our critical infrastructure operators, doesn't government have a responsibility to work with the private sector owners? And if government and private sector owner-operators are not collaborating, how will we determine the source of an attack or determine the proper course of action to take in a timely manner?

The game has changed. A 20th Century regulatory model simply will not work to combat this 21st Century threat. It requires both government and industry leaders to think anew. We need to support agile paradigms based on information sharing and public-private partnership.

The development of the cybersecurity framework is off to a good start. It has the potential to build balanced and sustained relationships between business and government so that individuals can experiment freely and quickly counter fast-paced threats to U.S. national security.

I highly recommend that Congress pass cyber bills that have earned widespread industry support, such as information-sharing measures, and refrain from codifying the cyber executive order before it has had the opportunity to demonstrate its efficacy. Lawmakers should conduct oversight of the presidential order to ensure that the private sector is an equal partner in its design and implementation.

As cyber threats grow, we can choose to repeat history. After a major incident, we can point fingers or issue voluminous post-mortem reports only to learn, as we did after 9/11 and after Katrina, that we needed more information sharing and collaboration are necessary between the public and private sectors.

Or, we can learn from history and do what needs to be done now. Enact Federal Information Security Act (FISMA) reform to get the government's own house in order. As the House has done on a wide bipartisan basis, pass information sharing legislation. Provide liability protections for private sector entities working with the government. Let's focus on areas of agreement and get legislation passed.

The adage, "We have faced the enemy and it is us," need not be the case.

Today we are facing numerous enemies in both the physical and cyber worlds. We need to face them together.

To be more specific, Mr. Chairman, I would like to expound upon some of the issues I have just summarized and make additional points to validate how successful public private partnerships have benefited our overall homeland security and why their application to our cyber challenges are relevant:

-The future of homeland security is tied to successful public-private partnerships, which has a lengthy history.

My experiences over the past decade and more tell me that the future of homeland security is closely tied to the success of partnerships between government and the private sector.

As you know, the protection of U.S. critical infrastructure has a lengthy history involving the business community. Issued in 1998, Presidential Decision Directive No. 63 (PDD-63) helped spur the protection of critical infrastructure and launch the formation of information sharing and analysis centers (ISACs) across the private sector. In 2003, Homeland Security Presidential Directive No. 7 (HSPD-7) updated the policy of the United States and the roles and responsibilities of various agencies related to critical infrastructure identification, prioritization, and protection.

Jumping forward a few years, 2006 witnessed the creation of the National Infrastructure Protection Plan (NIPP) and the Critical Infrastructure Protection Advisory (CIPAC). The NIPP resulted in the establishment of sector-coordinating councils (SCCs) and government-coordinating councils (GCCs) to work together on furthering the protection and resilience of the critical infrastructure community under the authorities of CIPAC. The NIPP was revised in 2009 to reflect an evolution of the process, including expanded integration of all-hazard and similarly important risk-management principles.

Businesses focus on guarding their operations from interruption, preventing the loss of intellectual property and sensitive customer data, and protecting public safety. Companies devote considerable resources toward maintaining their operations in the wake of a natural hazard or man-made threat, such as a terrorist attack. Business owners and operators understand it is imperative that critical infrastructure assets be well protected and resilient.

Issued on February 12, 2013, PPD-21, *Critical Infrastructure Security and Resilience*, calls on DHS to update the NIPP and deliver it to the president next month. At the same time, the administration is undertaking several homeland security-related initiatives simultaneously—including creating the cybersecurity framework, framework performance goals, and framework incentives. Each initiative, including reworking the NIPP, features one or multiple working groups in combination with tight deadlines, contributing to a flurry of activity.

Important elements of the business community—e.g., individual companies, SCCs, the Partnership for Critical Infrastructure Security (PCIS), and industry associations—dedicate vast resources toward engaging the government because it's in their best interests to do so. But they are also committed to advancing the common good of their communities and the nation.

-Policymakers should highlight public-private successes against America's adversaries in order to reinforce and replicate collaborative and innovative performances in the future.

a. Global supply chain security.

Businesses are linked together through a global web of interconnected, predictable, and efficient supply chains. American firms rely on these complex supply chains to access international consumers and compete in the global marketplace. Making improvements to

address cross-border friction would smooth the flow of trade and would ensure timely delivery of inputs and final products. Implementing such improvements would increase the competitiveness of U.S. businesses and unleash the potential for small- and medium-sized businesses to access foreign markets. DHS needs to review how these supply chains enhance U.S. businesses competitive advantage, and see how the department can reform and modernize their processes.

In the aftermath of September 11th, government officials and their private-sector counterparts came together to strengthen supply chain security, including developing the Customs-Trade Partnership Against Terrorism (C-TPAT). Together, both sides stepped up, invested in the program, and solved many of the mutual problems faced by government and the private sector.

Similarly, in the wake of the printer cartridge bomb plot on October 29, 2010, the private and public sector worked together to develop the Air Cargo Advance Screening (ACAS) pilot. The pilot program was up and running within two months of the terrorist attempt, and it closed gaps in security to ensure it could never happen again. Just as important, the ACAS program was flexible and fit existing business processes to ensure that businesses were not overburdened with mandates.

The public and private sector have interests that align much of the time. The challenges are finding those areas of commonality, and working together to develop a plan or program that promotes U.S. economic and physical security. Finding common ground should not always take a crisis to facilitate. We should be working with the private sector to facilitate trade, travel, ports, and supply chains to enhance to competitiveness of industry, so that when a crisis does come, we have the appropriate people working together to respond.

In the next 10 years, I hope to see the public and private sector relationships in homeland security go to the next level, where they work together to modernize our borders, our emergency response capabilities and other areas of the DHS mission, to a place where the private sector is viewed as a partner in homeland security, rather than just the “regulated” party.

I recommend that the United States reach out to its trading partners to develop a comprehensive, multilateral supply chain security program that promotes trade and security on both sides of the transaction. The United States can accomplish these goals by furthering discussions via the World Customs Organizations SAFE Framework and moving forward on Mutual Recognition Arrangements (MRAs) with key trade partners. Businesses harmonize processes around the globe and governments should as well.

Also, the U.S. should set the global example for border management, and present a “one-government” approach to border management. This would happen when all government border agencies work together to facilitate the legitimate flow of trade. Multiple agencies unsurprisingly have duplicative mandates, data requirements, and approaches to clearing goods. This is inefficient and ineffective for both the private and public sector. U.S. Customs and Border Protection (CBP) have taken steps to promote their “Trade Transformation Agenda” that includes this and other major trade and security priorities. These efforts and encourages the agency to deliver commercially meaningful results.

Congress would do well to support funding CBP for 3,500 additional customs officers at the ports of entry to improve security, trade, and travel facilitation. The dual role of CBP is to secure our homeland and facilitate trade and travel. Over the past five years, a disproportionate amount of funding has been designated for increasing staffing of border patrol officers between the ports of entry. These efforts seem reasonable, but more funding needs to be devoted towards customs officers at ports of entry.

Related, commercial and pedestrian border crossings suffer from understaffing which increases wait times, costs industry billions, and discourages travelers and trade from approaching the border. Investing in staffing at the ports of entry would enhance security, facilitate trade, and improve travel for the millions of business and leisure travelers entering the United States every year.

b. Chemical security.

Under the Chemical Facility Anti-Terrorism Standards (CFATS) program, U.S. businesses will commit billions of dollars toward measures approved by the Department of Homeland Security (DHS) to make chemical facilities more secure and resilient in an all-hazards context. CFATS is a relatively new example of public-private partnership in the context of homeland security, which is why it is important for policymakers to take industry views into consideration as the program takes shape. Although revelations about mismanagement of the CFATS program have been a concern, the concepts underpinning the program remain sound.

The tragedy at the West Fertilizer Company facility shows that we need to redouble our public-private efforts to bring so-called outlier sites into CFATS. DHS needs appropriate resources to administer the program in a timely fashion. Ultimately, to enhance security at chemical facilities, Congress should pass legislation authorizing a clean, long-term extension of CFATS, and avoid proposals that would add layers of complexity and costs on businesses.

Genuine Public-Private Partnerships are necessary to meet our cybersecurity challenges

a. The Cyber Framework

As mentioned previously, the cybersecurity framework under development has the potential to build balanced and sustained relationships between business and government so that individuals can experiment freely and quickly counter fast-paced threats to U.S. national security. It is constructive that the National Institute for Standards and Technology (NIST) has been given the responsibility to coordinate an environment where technical and security professionals come together to identify the most applicable and effective guidance throughout industry sectors and promote its implementation.

I agree with comments made by Patrick Gallagher, Under Secretary of Commerce for Standards and Technology at the Department of Commerce, who testified in March before the Homeland Security and Commerce committees that a NIST-coordinated and industry-led framework would “draw on standards and best practices that industry is already involved in

developing and adopting,” and would “ensure a robust technical underpinning to the framework.” He emphasized that a multi-stakeholder approach would take advantage of the strengths of the public and private sectors to develop solutions that both sides would find beneficial to security. Under Secretary Gallagher said that the “approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace.”

Critical infrastructure entities identified under cybersecurity executive order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, should be the primary voices behind the development of the cybersecurity framework. In turn, the administration has a unique opportunity to collaborate with the private sector as components of the EO are being developed and put into practice.

It is significant that S. 1353, the “Cybersecurity Act of 2013,” stopped short of codifying elements of the EO, because it is constructive to let framework efforts play out fully before they are written into law.

b. Information Sharing Bill

Developing the framework is only one piece of the cybersecurity puzzle. I urge Congress to focus on improving information sharing and liability protections, encouraging international cooperation against cybercrime, enhancing national cybersecurity R&D, reforming the Federal Information Security Management Act of 2002 (FISMA), and heightening public awareness and education.

Of particular importance, Congress should pass a cybersecurity bill to improve the exchange of cyber threat information between business and government to elevate overall situational awareness in a manner that’s sustainable. Legislation needs to help put timely, reliable, and actionable information into the hands of business owners and operators so that they can better protect their systems and assets against the increasing threat of cyberattacks.

Legislation should support existing information-sharing and analysis organizations and incorporate lessons learned from pilot programs and exercises undertaken by critical infrastructure sectors. They offer complementary, demonstrated models for enabling the government to share actionable cyber threat information with the private sector—thereby affording security professionals the opportunity to implement measures intended to reduce a business’ cyber risk profile—without creating burdensome regulatory mandates or new bureaucracies.

In addition, businesses need certainty that threat and vulnerability information voluntarily shared with the government would be provided safe harbor and not lead to frivolous lawsuits, would be exempt from public disclosure, and could not be used by officials to regulate other activities. Legislation also needs to include an exemption from antitrust laws, which limit exchanges of information between private entities, in order to help prevent, investigate, and mitigate threats to cybersecurity.

Further, executive action, like legislation, must focus not only on strengthening U.S. critical infrastructure but on encouraging innovative cybersecurity practices. Policymakers need to help the law enforcement community increasingly shift the cost of cyber intrusions to nefarious actors, which the business community and government both confront daily.

Conclusion

In a post 9/11 environment, the government has to be mindful that they are not the only interests with skin in the homeland security mission. The private sector owns and manages the majority of critical infrastructure, and its facilities are vital to the economic security of this country. The United States cannot solve myriad global threats by regulating the business community.

DHS needs to work collaboratively with the private sector to nurture business solutions to the security challenges that face this country. When a natural hazard or bad actor threatens our nation, the private sector has vested interest in ensuring that the incident is mitigated successfully or prevented and that the business community is resilient. Thus, policymakers should focus on public-private successes—including in the areas of global supply chain security, chemical security, and cybersecurity—against America's adversaries in order to reinforce and replicate special and innovative performances in the future.

Once again, I greatly appreciate the opportunity to testify today and look forward to working with the committee on these and other issues. Thank you very much.

###

**THE HONORABLE JANE HARMAN
TESTIMONY
SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE
SEPTEMBER 11, 2013**

Twelve years ago today, as the towers were falling and the Pentagon fire was burning, I was walking toward the US Capitol. My destination was the intelligence committee rooms in the Capitol dome—the place most believe was the intended target of the fourth plane which, thanks to the heroism of its passengers, went down in Shanksville, Pennsylvania. My staff called to alert me that the Capitol had just been closed, as were the House office buildings. So most of Congress and I milled around on the lawn in front of the Capitol. There was no evacuation plan. We had no roadmap for a response.

Part of the solution which some of us in the intelligence and counterterror field recommended was to create a dedicated homeland security function. The White House proposed a much more ambitious concept, and in order to pass legislation to create this new capability, Congress agreed to combine 22 agencies into the Department of Homeland Security (DHS).

Now in its tenth year, I'm proud of my role as one of the Department's "founding mothers" and want to thank the thousands of DHS employees serving us daily around the country and the world. As I speak, Customs and Border Patrol (CBP) agents in mega-ports like the port of Dubai are screening US-bound cargo for dangerous weapons and materials, specially trained Homeland Security Investigation agents in diplomatic posts around the world are reviewing suspicious visas, and TSA screeners are daily depriving al Qaeda and other terror groups the ability to turn more aircraft into weapons – a tactic we know they continue to attempt.

Today, DHS remains a work in progress but the efforts of its people are its backbone. And ours.

I testified before this Committee last year, and said that there are homeland functions that work well, including:

- CBP and TSA efforts to prevent suspicious individuals from departing foreign and domestic airports while allowing the rest of the flying public to travel,
- Expansion of the See Something Say Something campaign,
- Coordination with state and local law enforcement, including fusion centers, to identify terror suspects, and
- A massive vulnerability assessment of US critical infrastructure.

But I noted challenges:

- The failure of the intelligence function to fully develop at DHS,
- The need for DHS to focus more on its relationships with critical infrastructure owners and operators (which is now happening), and
- The failure of Congress to reorganize its committee structure.

Since I testified, much has happened. There is good news and bad news.

The bad news first:

- we failed to thwart the Boston Marathon bombing,
- there has been an exponential increase in cyber attacks,
- another devastating Hurricane,
- Edward Snowden, and
- bombmaker Ibrahim al Asiri of al Qaeda in the Arabian Peninsula is still on the loose.

The significant good news is that we are doing better on four major fronts:

- information sharing,
- resilience,
- collaboration with the private sector on cyber, and
- we're getting ahead of privacy concerns.

Information Sharing

Information sharing since 9/11 has improved dramatically, but there is more to be done. In the past year, while we were not able to stop the Boston bombing, our sharing of information after the attack was better and faster than it has ever been. Boston PD worked seamlessly with local, state and federal intelligence and law enforcement agencies to identify the suspects and detain them, using extensive camera footage and cell phone data. This was the first full-scale effort to use the American people as a significant investigative resource.

DHS homeland security grant money was critical – according to the Boston PD – in making sure that the city was trained to share information rapidly during an emergency. DHS also participated in the Multi-Agency Coordination Center (MACC) that was operational before and during the marathon. Representatives from Boston's police, fire, and emergency medical services, as well as public safety personnel from seven other cities and towns along the marathon course participated. The MACC was a critical in coordinating communications once the bombs exploded.

Resilience

At the time of the bombings, Boston was one of the best-prepared cities in the country to handle an emergency event, in large part because of DHS's preparedness and resiliency programs and collaboration with state and local officials. Last fiscal year, DHS distributed almost \$11 million to Boston through its Urban Areas Security Initiative (UASI).

That money had been used, in part to upgrade over 5,000 portable radios for first responders, install a communication system inside the tunnels of the Boston T, and to conduct two citywide disaster simulations in collaboration with DHS. Using the preparation and after-action reports from the first trial (in May 2011), local and state authorities worked to improve the city's preparedness in a second city-wide drill, in November 2012, less than a year before the bombings. Boston Police Commissioner Edward Davis has said that the "interoperability" learned during those drills "made a difference in our ability to respond to the Marathon."

DHS also responded successfully to Hurricane Sandy. On October 27th, FEMA activated its National Response Coordination Center, a multi-agency center based at headquarters in Washington. By October 28th, just before Sandy made landfall in New York and New Jersey, more than 1,032 FEMA personnel were positioned deployed along the East Coast working to support disaster preparedness and response operations, including search and rescue, situational awareness, communications and logistical support.

Collaboration with the Private Sector on Cyber

DHS will never “own” the cyber mission, but it is responsible for a central piece: critical infrastructure protection. In the past year, DHS has tracked and responded to nearly 200,000 cyber incidents – a 68% increase from the year before.

I have seen firsthand how the Department is working hard to build strong and lasting relationships with the private sector – owners and operators of critical infrastructure – and the IT companies that help those facilities function. In June, the Wilson Center hosted Secretary Napolitano for an off-the-record discussion between industry and the Department about what’s going right and what’s going wrong.

We heard that real-time data sharing about threats will be hard, but if industry knows their counterparts at DHS who can then coordinate with other government agencies, the process is a lot easier: they can just pick up the phone. The National Cybersecurity and Communications Integration Center (NCCIC), now open now about four years, has responded to almost half-a-million incident reports and released tens of thousands of actionable alerts to the public and private sector partners. In the same room, DHS has different government representatives from different government agencies all talking together – with the private sector. This is unheard of.

The Secretary spoke publicly about how important this mission is for DHS, calling it a “grand experiment,” – the first time that our government has approached a major national security problem hand-in-hand with the private sector.

Getting ahead of privacy concerns

Recent disclosures by Edward Snowden have shown that in most cases, our self-policing system works. But privacy and civil liberties concerns will only grow as our government becomes more intertwined in the cyber experiment.

At DHS, there is a privacy and a civil liberties office mandated to review – on the front end – DHS policies to make sure there are appropriate protections for personal private information built in from the start. Regular “Privacy Impact Assessments” are issued for any new or substantially revised information technology system within the Department, and the DHS Civil Rights and Civil Liberties Office has delivered training to Privacy Officials at 68 of the 78 fusion centers.

In-house efforts at DHS should finally be augmented by the Privacy and Civil Liberties Oversight Board, which became operational in May of this year – 9 years after it was established by the 2004 intelligence reform law.

DHS will continue to face difficult challenges going forward, including al Qaeda's enormous ability to evolve, the rise of lone wolf terrorists, the constant increase in type and sophistication of cyber attacks – especially the risk of exploits in software, and privacy issues related to information technology.

To return to my introductory remarks, thousands of selfless DHS people deserve our thanks. So does former Secretary Janet Napolitano for her service over the last five rugged years.

Testimony of

**Thad W. Allen
Admiral, U.S. Coast Guard (retired)**

**U.S. Senate
Committee on Homeland Security and Government Affairs**

**The Department of Homeland Security at 10 Years:
Examining Challenges and Achievements and Addressing Emerging Threats**

**Wednesday September 11, 2013
342 Dirksen Senate Office Building**

Mr. Chairman, Ranking Member Senator Coburn, and members of the committee, I am pleased to have been invited to testify on this important topic and I thank you for the opportunity.

For the record I am testifying in my personal capacity today and am not representing any other entity.

I am also pleased to be here with my distinguished colleagues Secretary Tom Ridge and former Congresswoman Jane Harmon, both of whom have served their country with distinction. I consider them friends and role models.

Mr. Chairman, in the last year we have witness three key anniversary dates in the history of the Department of Homeland Security. The Homeland Security Act was signed into law by President Bush on 25 November 2002. The Department came into existence on 24 January 2003. Finally, the agencies and functions from legacy departments were transferred to the Department on 1 March 2003, completing the statutorily mandated actions to create the Department.

The Past and Present

In prior testimony before this committee I have provided my personal view of the creation of the department and the implications of the compressed timeframe between the signing of the legislation and the first day of full operations, barely more than three months. While this could be considered government at light speed, little time was available for deliberate planning and thoughtful consideration of available alternatives. The situation was complicated by the fact that the law was passed between legislative sessions and in the middle of a fiscal year. Other than Secretary Ridge, early leadership positions were filled by existing senior officials serving in government and did not require confirmation. Funding was provided through the reprogramming of current funds from across government for departmental elements that did not have existing appropriations from their legacy departments.

Operating funds for components that were transferred were identified quickly and shifted to new accounts in the Department to meet the deadline. Because of the wide range of transparency and accuracy of the appropriation structure and funds management systems of the legacy departments some of the new operational components faced a number of immediate challenges. Estimating the cost of salaries for Customs and Border Protection (CBP) or Immigration and Customs Enforcement (ICE) required the combination of different work forces, with different grade structures, different career ladders, and different work rules.

Basic mission support functions of the department such as financial accounting, human resource management, real property management, information resource management, procurement, and logistics were retained largely at the component level in legacy systems that varied widely. Funding for those functions was retained

at the component level as well. In those cases where new entities were created (i.e. Departmental level management and operations, the Under Secretary for Science and Technology, the Under Secretary for Intelligence and Analysis, the Domestic Nuclear Detection Office) support systems had to be created rapidly to meet immediate demands of mission execution. Finally, components and departmental offices that did not preexist the legislation were located in available space around the Washington DC area and the Secretary and number of new functions were located at the Nebraska Avenue Complex in Northwest Washington.

At the time of this transition I was serving as the Coast Guard Chief of Staff and was assigned as the Coast Guard executive to oversee the Service's relocation from the Department of Transportation to the new Department. We began planning for eventual relocation as soon as the administration submitted legislation to the Congress. I also assigned personnel to the Transition Planning Office (TPO) that was created in the Office of Management and Budget by Executive Order to prepare for the transition. A considerable challenge during this period was the fact that the TPO was part of the Executive Office of the President and there were legal limitations on how much of their work could be shared externally. As a result much of that effort was redone or duplicated when the Department was created.

My intent is not to dwell on the past but to frame the degree of difficulty facing the leaders attempting to stand up the Department from the outset. Many of these issues persist today, ten years later. Despite several attempts to centralize and consolidate functions such as financial accounting and human resource management, most support functions remain located in departmental components and the funding to support those functions remains in their appropriations. Because of dissimilarities between appropriations structures of components transferred from legacy departments there is a lack of uniformity, comparability, and transparency in budget presentations across the department. As a result it is difficult to clearly differentiate, for example, between personnel costs, operations and maintenance costs, information technology costs, and capital investment. Finally, the five-year Future Years Homeland Security Plan (FYHSP) required by the Homeland Security Act has never been effectively implemented as a long range planning, programming, and budgeting framework inhibiting effective planning and execution of multi-year acquisitions and investments.

In the Washington Area the Department remains a disjointed collection of facilities and the future of the relocation to the St. Elizabeth's campus remains in serious doubt. One of the great opportunity costs that will occur if this does not happen will be the failure to create a fully functioning National Operations Center for the Department that could serve as the integrating node for departmental wide operations and establish the competency and credibility of the Department to coordinate homeland security related events and responses across government as envisioned by the Homeland Security Act. As with the mission support functions discussed earlier, the Department has struggled to evolve an operational planning and mission execution coordination capability. As a result, the most robust

command and control functions and capabilities in the Department reside at the component level with the current NOC serving as a collator of information and reporting conduit for the Secretary.

The combination of these factors, in my view, has severely constrained the ability to the Department of mature as an enterprise. And while there is significant potential for increased efficiencies and effectiveness, the real cause for action remains the creation of unity of effort that enables better mission performance. In this regard there is no higher priority than removing barriers to information sharing within the department and improved operational planning and execution. Effective internal management and effective mission execution require the same commitment to shared services, information systems consolidation, the reduction in proprietary technologies and software, and the employment of emerging cloud technologies.

Looking to the future the discussion should begin with the Department's missions and whether they adequately reflect the needs of the Nation ten years later ... and the need to create unity of effort internally and across the homeland security enterprise.

The Quadrennial Homeland Security Review

The Quadrennial Homeland Security Review was envisioned as a vehicle to consider the Department's future. The first review completed in 2010 described the following DHS missions

- Preventing Terrorism and Enhancing Security
- Securing and Managing Our Borders
- Enforcing and Administering our Immigration Laws
- Safeguarding and Security Cyberspace
- Insuring Resiliency to Disasters

An additional area of specific focus was the maturation of the homeland security "enterprise" which extends beyond the department itself to all elements of society that participate in and contribute to the security of the homeland.

The QHSR outcomes were consistent with the fiscal year 2010 budget that was submitted in early 2009 following the change of administrations. That request laid out the following mission priorities for the Department

- Guarding Against Terrorism
- Securing Our Borders
- Smart and Tough Enforcement of Immigration Laws and Improving Immigration Services
- Preparing For, Responding To, and Recovering From Natural Disasters
- Unifying and Maturing DHS

The FY 2010 budget priorities and the follow-on QHSR mission priorities have served as the basis for annual appropriations requests for four consecutive fiscal years.

I participated in the first review prior to my retirement and we are approaching the second review mandated by the Homeland Security Act. This review presents an opportunity to assess the past ten years and rethink assumptions related to how the broad spectrum of DHS authorities, jurisdictions, capabilities, and competencies should be applied most effectively and efficiently against the risks we are likely to encounter ... and how to adapt to those that cannot be predicted, including complex, hybrid events that cross organizational and functional boundaries. This will require a rethinking of what have become traditional concepts associated with homeland security over the last ten years.

Confronting Complexity and Unity of Effort

In 2012 I wrote an editorial for journal *Public Administration Review* entitled "Confronting Complexity and Leading Unity of Effort." I proposed that the major emerging challenge of public administration and governing is the increased level of complexity we confront in mission operations, execution of government programs, and managing non-routine and crisis events. Driving this complexity are rapid changes in technology, the emergence of global community, and the ever-expanding human-built environment that intersects with the natural environment in new more extreme ways. That environment remains today as we continue to witness extreme weather events, climate change, evolving threats, and the ascendancy of security issues associated with the internet.

The results are more vexing issues or wicked problems we must contend with and a greater frequency of high consequence events. On the other hand advances in computation make it possible to know more and understand more. At the same time structural changes in our economy associated with the transition from a rural agrarian society to a post industrial service/information economy has changed how public programs and services are delivered. No single department, agency, or bureau has the authorizing legislation, appropriation, capability, competency or capacity to address complexity alone. The result is that most government programs or services are "co-produced" by multiple agencies. Many involve the private/non-governmental sector, and, in some cases, international partners. Collaboration, cooperation, the ability to build networks, and partner are emerging as critical organizational and leadership skills. Homeland Security is a complex "system of systems" that interrelates and interacts with virtually every department of government at all levels and the private sector as well. It is integral to the larger national security system. We need the capabilities, capacities and competency to create unity of effort within the Department and across the homeland security enterprise.

Mission Execution ... Doing the Right Things Right

As a precursor to the next QHSR there should be a baseline assessment of the current legal authorities, regulatory responsibilities, treaty obligations, and current policy direction (i.e. HSPD/NSPD). I do not believe there has been sufficient visibility provided on the broad spectrum of authorities and responsibilities that moved to the department with the components in 2003, many of which are non discretionary. Given the rush to enact the legislation in 2002 it makes sense to conduct a comprehensive review to validate the current mission sets as established in law.

The next step, in my view, would be to examine the aggregated mission set in the context of the threat environment without regard to current stove piped component activities ... to see the department's mission space as a system of systems. In the case of border security/management, for example, a system of systems approach would allow a more expansive description of the activities required to meet our sovereign responsibilities. For the purpose of today's hearing I would like to address four areas: The Border, National Resiliency, Counter Terrorism and Law Enforcement, and Cyber Security.

The Border

Instead of narrowly focusing on specific activities or regions such as the physical security of the Southwest Border we need to shift our thinking to the broader concept of the management of border functions in a global commons. The border has a physical and geographical dimension related to the air, land and sea domains. It also has a virtual domain where many governmental activities occur such as the processing of advance notice of arrivals, analysis data related to cargoes, passengers, and conveyances, and the facilitation of trade. These latter functions do not occur at a physical border but are a requirement of managing the border in the current global economic system.

The air and maritime domains are different as well. We prescreen passengers at foreign airports and the maritime domain is a collection of jurisdictional bands that extend from the territorial sea to the limits of the exclusive economic zone and beyond. These domains are interconnected and must be seen as a system.

The key concept here is to envision the border as an aggregation of functions across physical and virtual domains instead of the isolated and separate authorities, jurisdictions, capabilities, and competencies of individual components. Further, there are other governmental stakeholders whose interests are represented at the border by DHS components (i.e. DOT/Federal Motor Carriers regarding trucking

regulations, NOAA/National Marine Fisheries Service regarding the regulation of commercial fishing).

A natural outcome of a functional or systems view of the border is a cause for action to remove organizational barriers to unity of effort, the consolidation of information systems to improve situational awareness and queuing of resources, and integrated/unified operational planning and coordination among components. The additional benefits accrued in increased efficiency and effectiveness become essential in the constrained budget environment. The overarching goal should always be to act with strategic intent through unity of effort. Here the Department continues to be challenged with the internal integration of functions within Customs and Border Protection and the creation of an integrated, fused view of the border across all domains working other components and agencies of government.

Specific areas that would create greater unity of effort and more effective performance include:

- Aggregation of data related to border functions into a single cloud reference architecture (license plate reader data, passenger information, private aircraft and vessel arrivals)
- Sharing and fusing of sensor information across all domains (air, land, sea and cyber)
- Visualization of knowledge through geospatial display tools that allow leaders to see and understand threats
- Addressing issues of border security or control of the border through a functional approach that recognizes the physical diversity border and level of risk by corridors or regions.

National Resiliency

The concept of national resiliency transcends a narrow focus on natural disasters. We need to promote a risk-based whole of community approach that is informed by the collective threat/risks presented by both the natural and human built environments. The latter is a more expansive concept than “infrastructure” and the overall concept subsumes the term “disaster” into larger problem set that we will face. This strategic approach would allow integration of activities and synergies between activities that are currently stove piped within FEMA, NPPD, and other DHS components and other departments of government (i.e. HHS and a pandemic). It also allows cyber security to be addressed as an issue that touches virtually every citizen and player in the homeland security enterprise.

Key components include:

- Regionally based risk assessments that focus on the most likely and consequential threats from the natural and built environments. The latter includes a better understanding of population densities and infrastructure that are exposed to higher risk.
- A better understanding of mitigation and collective action to reduce risks through individual preparedness, local community actions regarding land use and building codes, inclusion of mitigation measures in infrastructure development, better use of scientific data in the understanding and prediction of events, and policies that allocate the cost of risks to those who incur it. The overarching goal is to fundamentally change how risk is viewed by individuals and governments ... and to change behavior.
- Development of an improved incident management doctrine that more clearly defines roles and responsibilities and removes ambiguity before, during and after responses. We are seeing more complex events that defy existing response protocols regarding which agency should lead and what roles should other agencies play.
- We need to anticipate hybrid events that cross functional and organizational boundaries. One example of a hybrid event would be a man made disaster precipitated by a cyber attack on an industrial control system. Such an event would involve DHS (NPPD, FEMA), the FBI (criminal activity), and potential the defense industrial base. Responding to an event of this nature under current circumstances would be extremely difficult and challenging.
- A national operations center for the Department of Homeland Security that centralizes and visualizes risks and facilitates the monitoring and management of operations. Unity of effort within DHS is the first goal, including greater internal integration in CBP and NPPD.

Counter Terrorism and Law Enforcement Activities

In regard to terrorism and law enforcement operations we should understand that terrorism is, in effect, political criminality and as a continuing criminal enterprise it requires financial resources generated largely through illicit means. All terrorists have to communicate, travel, and spend money, as do all individuals and groups engaged in criminal activities. To be effective in a rapidly changing threat environment where our adversaries can quickly adapt, we must look at cross cutting capabilities that allow enterprise wide success against transnational organized criminal organizations, illicit trafficking, and the movement of funds gained through these activities. As with the "border" we must challenge our existing paradigm regarding "case-based" investigative activities. In my view, the concept of a law enforcement case has been overtaken by the need to understand criminal and terrorist networks as the target. It takes a network to defeat a network. That in turn demands even greater information sharing and exploitation of advances in computation and cloud-based analytics. The traditional concerns of the law enforcement community regarding confidentiality of sources, attribution, and

prosecution can and must be addressed, but these are not technology issues ... they are cultural, leadership, and policy issues.

Key components include:

- Development and deployment of a classified and unclassified cloud reference architecture that allows the aggregation and analysis of all relevant information held across DHS components including sensor data.
- Development a network discovery doctrine that transitions traditional law enforcement and intelligence “case management” processes to an outcome focused strategy that attacks terrorist and organized crime networks at nodes where they are exposed. This needs to include a more realistic recognition that non-events or the prevention of an attack is preferable, in some cases, to arrest and conviction.
- Aggregation and analysis of biometric information that anticipates advances in technology such as DNA testing and facial recognition that can be readily accessed by field personnel and mobile devices.

Cyber Security

We need to understand that cyber space touches everything and everyone. It is an ubiquitous feature of our lives. Development of better knowledge of this domain in terms of national governance, legal issues and international governance remain works in progress. But the fact is that the internet has produced the sociological, cultural, economic, and legal equivalent of climate change. We must adapt and manage this change. Related to the Department’s mission, this includes the protection of the Department’s networks, effectively leading the government’s protection activities of it’s own networks, and, finally, the effective interface with the private sector, state and local governments, and other affected stakeholders to reduce risks and improve national resiliency. These activities must be carried out in cooperation with the Department of Defense, the Intelligence Community, and the Department of Justice to create unity of effort at a national level. There has been recent progress in role definition between these major players. Also, significant activity is currently underway through continuous monitoring initiatives and the presidentially mandated Interagency Task Force to develop a framework to address cyber threats to our critical infrastructure.

Key components include:

- Transition from the current federal information security structure to continuous measurement and mitigation at our internet connections.
- The sharing of information on threats across government and the maturation of information systems and security measures that converge to common architecture

- Development of an effective means to share threat information with the private sector where most of our critical infrastructure resides.
- More effective identification of threats in advance through improved diagnostics
- Cyber legislation to address those areas where administrative action is inadequate to deal with legal issues.

Mission Support

As we address the operational challenges of the Department we must also address the need for improved more integrated mission support. In the rush to establish the Department and in the inelegant way the legacy funding and support structures were thrown together in 2003, it was difficult to link mission execution and mission support across the Department. To this day, most resources and program management of support functions rest in the components. As a result normal mission support functions such as shared services, working capital funds, core financial accounting, human resources, property management, and integrated life cycle based capital investment have been vexing challenges. While this testimony has been focused on operational issues, it is critical that progress be made toward the integration and more effective support of mission execution across the Department.

Conclusion

Mr. Chairman, I have attempted to keep this testimony at a strategic level and focus on thinking about the challenges in terms that transcend individual components, programs, or even the Department itself. I have recently spoken to the Department of Homeland Security Fellows and the first DHS Capstone course for new executives. I have shared many of the thoughts provided today over the last ten years to many similar groups. Lately I have changed my message. After going over the conditions under which the Department was formed and the many challenges that still remain after ten years, I was very frank with both groups. Regardless of the conditions under which the Department was created and notwithstanding the barriers that have existed for ten years, at some point the public has a right to expect that the Department will act on its own to address these issues. Something has to give. In my view, it is the responsibility of the career employees and leaders in the Department to collectively recognize and act to meet the promise the Homeland Security Act. That is done through a shared vision translated into strategic intent that is implemented in daily activities from the NAC to the border through the trust and shared values that undergird unity of effort. It is that simple, it is that complex.

Testimony of Stewart A. Baker

Before the Committee on Homeland Security and Governmental Affairs
United States Senate

**“The Department of Homeland Security At 10 Years:
Examining Challenges and Achievements and Addressing Emerging Threats”**

September 11, 2013

Thank you, Chairman Carper, Ranking Member Coburn, and distinguished members of the Committee, for this opportunity to testify on the state of the Department of Homeland Security (“DHS”).

This is a timely hearing. DHS has now been in existence for 10 years. We should not expect big shifts in the structure or mission of the Department unless those shifts are driven by the Department’s successes or failures. So it is fair to ask what DHS has done well, where it has stumbled, and, especially, how it can do better in the future.

DHS’s Failing

I begin with DHS’s biggest failing. Despite considerable effort, and even some progress, DHS has not developed the tools and institutions it needs to unify the work of its many components. By saying that, I do not mean to suggest, as some would have it, that DHS is a sprawling and inherently uncontrollable amalgam of agencies. That is wrong. The Department has had many management successes, some of them critical to stopping terrorist attacks. But in many cases, the key to success has been the personal, daily involvement of the Secretary or Deputy Secretary. We have been lucky to have only three secretaries in the last ten years, all of whom have understood how to lead large agencies. They have achieved a lot through force of personality. But personality is not enough. What we need is the equivalent of the Office of the Secretary of Defense – a strong, institutionalized set of offices devoted to carrying out the Secretary’s policies and decisions on issues when the Secretary cannot spend time every day on the problem. This should be done by the offices that focus on policy, planning, international affairs, procurement, and personnel, but these have limited authority and staff. They have been hampered by resistance from component agencies, and in many cases from legacy authorizing committees who see any strengthening of the Department’s center as undermining their authority and prerogatives.

This issue is especially pressing now, given the leadership changes underway and the difficult budget outlook ahead. After seven fat years in budget terms, DHS is now deep into a cycle of lean years that may stretch far into the future. As we try to do more with less, it’s even more important to set policy and budget priorities across component lines. Budget decisions simply must be based on how each component’s expenditures fit the Department’s highest priorities. For the first time, DHS has to identify redundancies and may have to eliminate or scale back programs that have powerful constituencies. If that is not done on the basis of a careful, institutionalized review of the Department’s overall strategy, we will not use the scarce dollars that remain in a way that best protects the country. That would be a tragedy.

Apart from centralizing oversight, there are other steps that can be taken to ensure that the center holds. The assistant secretary for policy should be elevated to undersecretary status, as was intended when it was created. When I held that office, the Secretary and Deputy Secretary treated me as an undersecretary and *de facto* third in command for the Department. But the failure to institutionalize the office’s status has made it difficult to sustain that role. That, in turn, has left the Department with a thinner bench and fewer officials who are fully prepared to step in and lead when – as now – the Secretary and Deputy Secretary are gone. Restoring the intended and historic status of the office of policy would help to avoid future leadership crises.

Another way of addressing the looming budget crisis is to make lemonade from it. The same forces cutting DHS’s budget are affecting the Department of Defense and the intelligence community. These agencies and

their contractors badly need to find new buyers for equipment and technology originally developed for conflicts in Afghanistan and Iraq. DOD and the Intelligence Community have invested billions of dollars in the development and deployment of new capabilities, from sophisticated sensor and surveillance networks to data integration and analysis capabilities, to cybersecurity tools. Many of these technologies are directly relevant to supporting homeland security missions. Customs and Border Protection (“CBP”) and the Science and Technology Directorate (“S&T”) in particular have taken positive steps in this direction, working with DOD to identify potential solutions. More fully leveraging that which we’ve already paid for would bolster homeland security capabilities while reducing the need to spend additional taxpayer dollars on new research and development. To facilitate this kind of concerted effort, multiple organizations and actors – from DOD, the intelligence community, and DHS to the private sector and others – will need to work together to identify what equipment and technologies are most relevant and create efficient processes for their transfer and ongoing operation.

DHS’s Success: Intelligence-Driven Security Screening

Let me now turn to one of the Department’s unquestionable successes – the way it has unified the government’s screening and enforcement on the border, something that was once a side business for three or four departments with many other priorities.

It’s not easy to find a handful of terrorists and criminals in a flood of millions of travelers, especially if you have less than 30 seconds to make the call. DHS quickly realized that taking more time to inspect everyone would not solve the problem. Indeed, DHS could quadruple the wait (and the hassle), and it’d still be trying to find bad guys based on two minutes of scrutiny. As a result, border officials began gathering more background data earlier on all travelers, and they used that data to decide which travelers needed more than 30 seconds of attention.

And DHS’s use of advance information at the border – particularly Passenger Name Record (“PNR”) data – has produced a number of tangible successes. Faisal Shahzad, the would-be Times Square bomber was pulled off a plane at JFK as it was preparing to leave the country because of PNR data. Similarly, the PNR data of Najibullah Zazi – the guy who rented a truck and drove cross country to set off explosives in the New York City subway – was used to identify the scope of the conspiracy. These are just the public successes. In fact, PNR data has aided nearly every recent high profile terrorist investigation. And, it’s not just national security cases that benefit from the use of PNR. PNR also enables more traditional law enforcement operations, identifying, for example, previously unknown individuals involved in narcotics and currency smuggling operations.

The Department has also gone on the offensive to get other important data about travelers. Before the Department was created, remarkably, our border inspectors had no way to know whether travelers from other countries had been convicted even of the most serious crimes. Now, thanks to the leverage of the Visa Waiver Program, DHS has information-sharing agreements with dozens of countries. The Department has also implemented ESTA, a “reservation” system that allows the Department to screen risky VWP travelers before they begin their trips. DHS should continue to expand the VWP to partners who are willing to take steps and share information that improve both countries’ security.

DHS has further expanded available information by launching Global Entry, which speeds clearance at the border for travelers who have been vetted in advance. There are now nearly 900,000 participants in the program, and just last month the Department announced that vetted citizens from the United Kingdom, Germany, the Republic of Korea, and Qatar are eligible for Global Entry benefits. DHS should be applauded for its efforts to continue to expand Global Entry to include citizens from Brazil, India, and elsewhere. Adding these travelers to Global Entry will not reduce our ability to screen them for terrorism purposes, but it will give us more information to use in the screening process while also speeding most travelers through the checkpoints much faster. Finally, having overcome some State Department resistance, DHS’s international operations are increasingly robust. The Department has begun gathering more data in foreign airports, posting U.S.

government officers there to interview and in some cases pre-clear travelers, a convenience that is avidly sought by local governments. It is also working with a growing number of partners – especially in our hemisphere – to enhance coordination and build capacity.

These programs have improved the efficiency and effectiveness of border screening immensely while also speeding most travelers across the border more quickly. But they did not happen without immense effort. Privacy campaigners did their best to kill them. The European Union, which is far more enthusiastic about regulating American security programs than its own security agencies, spent a decade negotiating and then breaking agreements with DHS in the hope of killing travel data programs.

Despite this resistance, the programs have proved themselves. There have been no known abuses of the data. This is a success that could only have been achieved by a unified Department. It is a success that DHS can be proud of.

But that does not mean that it is perfect, as the recent controversy over the proposed pre-clearance in Abu Dhabi illustrates. In my view, our international engagement strategy needs a more coherent plan, with priorities, to make sure we get the most important information about the riskiest travelers at least cost to the United States. The criteria also need to be more transparent to our potential foreign partners, many of which are actively seeking engagement. But these are tactical criticisms of a program that is a great strategic victory.

Indeed, it is a victory that is paying dividends in airports around the country as well. Transportation Security Administration (“TSA”) personnel face the same problem securing passenger flights against terrorists, such as Richard Reid, the shoe bomber and Umar Farouk Abdulmutallab, the underwear bomber. Screening technology, such as a standard metal detector, was unable to detect the explosives used in these plots. Unlike border officials, though, TSA ended up taking more time to inspect everyone, treating all travelers as potential terrorists, and subjecting many to whole-body imaging and enhanced pat-downs. We can’t blame TSA for this wrong turn, though. Privacy lobbies persuaded Congress that TSA couldn’t be trusted with data about the travelers it was screening. With no information about travelers, TSA had no choice but to treat them all alike, sending us down a long blind alley that has inconvenienced billions.

At long last, however, TSA has begun successfully to implement risk-based screening that takes data and passenger risk into account. Under the Secure Flight program, TSA now receives each traveler’s name, gender, and date of birth from the airlines for pre-screening. This data is hardly sensitive, but it has begun to transform passenger screening. Even more encouraging is TSA’s TSA Pre✓™ program, which is currently at 40 airports and will be operational at 100 airports nationwide by the end of this year. Participation in TSA Pre✓™ enables the “known” traveler to use a “fast” lane where the most aggravating and time-consuming security procedures have been largely eliminated. Because TSA Pre✓™ is voluntary and has been rolled out cautiously, privacy campaigners have been quiet. To date, more than 15 million passengers have experienced TSA Pre✓™.

DHS should seize this moment to further integrate air and border security approaches so that TSA and CBP both know that a traveler is coming their way in time to plan for screening. While the Department has made great strides towards integration of its various databases, this process is not yet complete. All elements of the Department should have as much information as possible regarding those they are screening, whether that information was originally collected by CBP, TSA, Immigration and Customs Enforcement (“ICE”), or any of DHS’s other component agencies.

Such a strategy would not be free of controversy or complication. Because of past privacy limitations, it is likely that DHS will need Congressional assistance to achieve this goal. But the gains in reduced delays, in increased security, and in personal dignity would be significant. No one wants to be against privacy, but we’ve tried the privacy campaigners’ preferred solution, denying even the smallest scrap of data to the government, and they saddled us with ten years of stupid screening at our airports, where a lack of data forced TSA to treat everyone

like a suspected terrorist. No one liked that solution, with good reason. It's time to recognize that failure and encourage experiments in smarter, faster, more informed screening based on data-sharing.

During its second decade DHS will face threats and risks beyond terrorism. One area where the risks are certainly growing, and which will require investment of new resources, as well as the assistance of Congress, is cybersecurity and operations. As former Secretary Napolitano rightly noted just before her departure: "More must be done, and quickly."

Work in Progress: Cybersecurity

Sometimes it's easier to persuade the team to give you the ball than to actually run with it after you get it. That is DHS's problem right now.

DHS seems to have successfully fended off the many agencies and committees that wanted to seize parts of its cybersecurity mission. Recent presidential orders have given DHS a large role in civilian cybersecurity. This is consistent with the Homeland Security Act, which clearly gave DHS authority over those issues, but that Act does not provide specific or explicit authorization for many of the cybersecurity activities that the Department is now carrying out, especially with respect to protecting critical infrastructure. It is reasonable, then, to codify authority for DHS's existing activities, thereby cementing the Department's role for the future. This basic step may seem obvious, but this is Washington, and doing the obvious is not easy.

That's particularly true when the technology is changing as fast as our attackers change tactics. When I left the Department, it was just getting started on Einstein – an effort to detect malware and other intrusion signatures aimed at the federal civilian agencies. Deployment of Einstein is now widespread, covering perhaps 60% of the federal workforce. Of course, detecting intrusions is not the same as stopping them. Einstein 3A is meant to automate intrusion prevention, and it is just rolling out now. What's more, as security researchers have realized how hard it is to stop attacks at the edge of the network, watching inside networks has become a higher priority, and DHS has taken responsibility for deploying Continuous Diagnostics and Mitigation ("CDM") technology to scan civilian networks for flaws and signs of compromise. These are all necessary and very large programs that pose implementation and turf challenges. Not surprisingly, some agencies have questioned whether DHS has the authority to do what is necessary, and providing a statutory basis for DHS's programs would be a valuable contribution that this committee could make to cybersecurity.

One problem that should be of particular interest to the committee is the risk of conflict between the Federal Information Security Management Act ("FISMA") and CDM. In essence, CDM performs many of the functions that FISMA requires. However, FISMA envisions a paper-centered audit process that is far too slow for the current threat, while CDM performs its audits electronically, on a 72-hour cycle. Everyone recognizes that CDM is better than a paper process, and FISMA should be modified to reflect changes in both the threat and the solution, as well as to make clear that DHS has responsibility for implementing the operationally demanding solution.

These are all complex systems that DHS is essentially running for most of the civilian government. That would be a challenge for an established agency with a veteran workforce, but DHS does not have nearly the number of trained personnel it needs. Finding talented cyberwarriors is a challenge even for private sector firms. Attracting them to the Department has been doubly difficult, especially with a hiring process that in my experience was largely dysfunctional. The Department's biggest challenge is hiring and maintaining a cybersecurity staff that can earn the respect of private cybersecurity experts. There are bright spots. Doug Maughan, in the S&T Directorate, has the respect of his counterparts at NSA and Goldman Sachs. Phyllis Schneck, recently named as the Department's deputy undersecretary for cybersecurity, has great technical and private sector credibility in the field. DHS is on the right track, but the way is steep. It must keep expanding its technically competent cybersecurity staff, because that is the foundation of all the other things it must do. That likely means that it must have authority to hire workers in ways that do not fit the standard federal process.

The other challenges for DHS in cybersecurity are many. They include:

Building a clear relationship with NSA.

I am one of the few officials who has worked at a policy level for both the National Security Agency ("NSA") and DHS. There are certainly days and even weeks when I feel like the child of a troubled marriage. But the fact remains that the outlines of a working relationship between DHS and NSA are obvious. As a concerted campaign of leaks has left NSA reeling and mistrusted by the public, it must be clear that on cybersecurity matters affecting the civilian sector, DHS is calling the policy shots. At the same time, DHS must rely heavily on NSA's technical and operational expertise to succeed. This fundamental truth has been obscured by personalities, mistrust, and impatience on both sides. It's got to end, especially in the face of adversaries who must find the squabbling email messages especially amusing because they are reading them in real time.

Gaining authority to insist on serious private sector security measures.

DHS has plenty of authority to cajole and convene in the name of cybersecurity. It's been doing that for ten years. The private sector has paid only limited attention. In part that's because DHS had only modest technical expertise to offer, but it's largely because few industries felt a need to demonstrate to DHS that they were taking its concerns seriously. I fully recognize that cybersecurity measures do not lend themselves to traditional command-and-control regulation, and that information technology is a major driver for economic growth. But the same could have been said about the financial derivatives trade in 2007. We cannot allow the private sector to cut costs by vastly increasing risk, whether in cybersecurity or in financial markets.

Sometimes the businessmen arguing against regulation are wrong – so wrong that they end up hurting their own industries. I believe that this is true of those who oppose even the lightest form of cybersecurity standards. Even on their own terms, the businesses lobbying against a substantive cybersecurity bill are likely to fail. Most of the soft quasi-regulatory provisions business groups rejected last year in talks with the Senate were incorporated into an executive order that they had little ability to influence. Those provisions will in turn become the basis for future, harder regulations, particularly if Congress delays action until we have a cybersecurity meltdown.

For now, however, it will be up to DHS to use the soft authorities and the mandate conferred by an executive order with energy and wisdom. And, to be candid, that is a big enough job for the near future.

Action beyond the legislative and executive order.

The legislative stalemate does not mean that DHS can only improve cybersecurity by pushing the private sector to do things it doesn't want to do. There are many other steps that DHS could take to improve cybersecurity without touching the regulatory third rail. Here are some:

Information-sharing. Everyone understands why the targets of cyberattacks need to share information. We can greatly reduce the effectiveness of attacks if we use the experience of others to bolster our own defenses. As soon as one victim discovers a new command-and-control server, or a new piece of malware, or a new email address sending poisoned files, that information can be used by other companies and agencies to block similar attacks on their networks. This is not information-sharing of the "let's sit around a table and talk" variety. In a world of zero-day attacks and polymorphic malware, it must be automated and must occur at the speed of light, not at the speed of lawyers or bureaucrats.

I supported the Cyber Intelligence Sharing and Protection Act ("CISPA"), which would have set aside two poorly-conceived and aging privacy laws that made it hard to implement such sharing. I still do. But if CISPA is blocked by privacy groups, as seems likely, we need to ask whether the automated system we need can be built without falling foul of those aging privacy laws. A more creative and determined approach to the law is needed.

To take one example, many of the privacy rules that restrict sharing can be waived if a service's customers consent to the sharing. Since the purpose of the sharing is to protect the cybersecurity of those same customers, they are highly likely to consent in large numbers. Working with government, service providers could find ways to obtain consent to a data-sharing regime designed to protect both privacy and cybersecurity – all without amending existing law.

This committee can move information-sharing forward by calling on DHS to lead an interagency effort that would work within existing law to improve information sharing by considering the adoption of statutory interpretations, standard customer terms, and other techniques that serve everyone's interest in better cybersecurity.

Emphasize attribution. We will never defend our way out of the cybersecurity crisis. I know of no other crime where the risk of apprehension is so low, and where we simply try to build more and thicker defenses to protect ourselves. We started on this Maginot Line exercise because attribution of cyberattacks seemed too difficult; attackers could hop from country to country and server to server to protect their identities.

But that view is out of date. Intelligence agencies have stopped trying to trace each hop the hackers take. Instead, they've found other ways to compromise the attackers, penetrating their networks directly, observing their behavior on compromised systems and finding behavioral patterns that disclose much. In short, we *can* know who are our attackers are. We can know where they live and what their girlfriends look like. That's because it's harder and harder for hackers to function in cyberspace without dropping bits of identifying data here and there. The massive amount of data available online makes the job of attackers easier, but it can also help the defenders if we use it to find and punish our attackers.

Sometimes the best defense really is a good offense; we need to put more emphasis on breaking into hacker networks and gathering information about what they're stealing and who they're giving it to. That kind of information will help us prosecute criminals and embarrass state-sponsored attackers. It will also allow us to tell the victim of an intrusion with some precision who is in his network, what they want, and how to stop them.

Again, this committee can put DHS at the center of a new emphasis on attribution. Its Computer Emergency Readiness Team and intelligence analysis arms should be issuing more detailed information about the tactics and tools being used by individual attack units and fewer bland generalities for local law enforcement agencies.

Move from attribution to deterrence. The committee could also perform a service by calling on DHS to take the lead in identifying ways to use attribution more effectively to deter cyberattacks. There are many ways to improve deterrence. While the administration has become more open about identifying Chinese cyberattacks as a particular problem, the Snowden affair has made "naming and shaming" less effective in this context. Instead, we should be looking for other ways to identify individual attackers and their enablers and then bring U.S. legal pressure to bear on them. This is a target-rich environment:

- The Magnitsky Act, passed in 2012, imposes trade sanctions on Russian officials for human rights violations they committed in Russia. Yet government-sponsored hackers have been violating the human rights of Americans in the United States, spying on and sabotaging Tibetan rights groups, for example. How can it be that we are doing more to punish human rights violations in Russia than right here at home? Sanctions of this sort can be imposed on the basis of intelligence that remains classified, and it does not require legislation. It requires only that the Administration consider cyberattacks to constitute an economic emergency.
- Some of the hackers identified publicly by private security researchers do business in the West. Others may have jobs with Chinese multinationals. Some got their start as hackers at Chinese universities.

This creates an opportunity. Foreign multinationals and universities need visas to come to the United States. Before we issue visas to entities that have hired or enabled the hacking of American companies, we should require them to cooperate in our efforts to identify and penalize hackers.

Use DHS law enforcement authorities more effectively. The law enforcement agency most associated in the public mind with cybercrimes is the Federal Bureau of Investigation ("FBI"). This is a little odd because two DHS law enforcement agencies, the Secret Service and ICE, both have strong cybercrime units and may between them handle as many cases as the FBI.

My concern is not who gets the credit for these investigations. But we cannot let law enforcement determine our cybersecurity posture. Agencies like the FBI and Secret Service only occasionally solve hacking cases, and even more rarely are they able to actually arrest the hackers. If they are allowed to hoard evidence of cyberintrusions, we may lose valuable intelligence about the intruders' tactics and targets. This committee should consider legislation calling for a coordinated approach to all computer intrusions to ensure that detailed information sharing occurs across agency lines. At the same time, it is often law enforcement that tells businesses they have been compromised. This is a "teachable moment," when all of DHS's cyberdefense and industry-outreach capabilities should be engaged, talking to the compromised company about the nature of the intruder, his likely goals and tactics, and how to defeat them. But that happens less than it should, judging by the experience of my clients. A deeper, Congressionally mandated coordination would make these encounters far more useful to the private sector.

Finally, I fear that letting law enforcement take the lead on a case-by-case basis means that investigations are not being prioritized in ways that would maximize their intelligence value. (Since these investigations rarely lead to prosecutions, using criminal authorities to gather information about attackers should be a particularly high priority – even when there is no prospect of criminally prosecuting the attackers.) While interagency coordination with the FBI can be a challenge, coordination between DHS's cybersecurity offices and the ICE and Secret Service investigators also seems to be equally *ad hoc* at best. This committee should consider requiring DHS's law enforcement agencies to work computer crime cases under the coordinating and deconflicting authority of the National Protection and Programs Directorate ("NPPD") to ensure strategic use of law enforcement authorities and proper sharing of information.

Recruit private sector resources to the fight. In my private practice, I advise a fair number of companies who are fighting ongoing intrusions at a cost of \$50,000 or \$100,000 a week. The money they are spending is almost entirely defensive. At the end of the process, they may succeed in getting the intruder out of their system. But the next week, the same intruder may get another employee to click on a poisoned link and the whole process will begin again. It is a treadmill. Like me, these companies see only one way off the treadmill: to track the attackers, to figure out who they are and where they're selling the information, and then sanction both the attackers and their customers. But under federal law, there are grave doubts about how far a company can go in tracking their attackers. I think some of those doubts are exaggerated, but only a very brave company would ignore them.

Now, there's no doubt that U.S. intelligence and law enforcement agencies have the authority to conduct such an operation, but by and large they don't. Complaining to them about even a state-sponsored intrusion is like complaining to the DC police that someone stole your bicycle. You might get a visit from the police; you might get their sympathy; you might even get advice on how to protect your next bicycle. What you won't get is a serious investigation. There are just too many higher priority attacks.

In my view, that's a mistake. The United States should do some full-bore criminal and intelligence investigations of private sector intrusions, especially those that appear to be state-sponsored.

But if we want a solution that will scale, we have to let the victims participate in, and pay for, the investigation. Too many government officials have viewed private countermeasures as a kind of vigilante lynch mob justice.

That just shows a lack of imagination. In the real world, if someone stops making payments on a car loan but keeps the car, the lender doesn't call the police; he hires a repo man. In the real world, if your child is kidnapped, and the police aren't making it a priority, you hire a private investigator. And, if I remember correctly the westerns I watched growing up, if a gang robs the town bank and the sheriff is outnumbered, he deputizes a posse of citizens to help him track the robbers down. Not one of those solutions is the equivalent of a lynch mob. Every one allows the victim to supplement law enforcement while preserving social control and oversight.

DHS very likely has sufficient authority to try that solution tomorrow, as does the FBI. DHS's law enforcement agencies often have probable cause for a search warrant or even a wiretap order aimed at cyberintruders. But they rarely have the resources to use that authority fully and strategically against the intruders. I know of no legal barrier to relying on private resources to conduct a deeper investigation under government supervision. (The Antideficiency Act, which prohibits acceptance of free services, has more holes than my last pair of hiking socks, including exceptions for protection of property in emergencies and for gifts that also benefit the donor.) If systematic looting of America's commercial secrets truly is a crisis, and I believe that it is, why have we not already done this?

I understand the concern expressed by some that we cannot turn cyberspace into a free-fire zone, with vigilantes wreaking vengeance at will. No one wants that. Government should set limits and provide oversight for a true public-private partnership, in which the private sector provides many of the resources and the public sector provides guidance and authorities. The best way to determine how much oversight is appropriate is to move cautiously but quickly to find alternatives to the current failed cybersecurity strategy. Again, this committee can move the ball forward by authorizing DHS and its law enforcement agencies to develop a pilot project – working with hacking victims and their security firms to use government authorities in a cooperative fashion.

Use existing funds to improve state and local cybersecurity preparedness. There may still be low-hanging fruit in the Department's budget to improve cybersecurity. For example, we can make it easier for state and local governments to use existing grant funding to beef up their cybersecurity. Over the last decade DHS has provided billions of dollars to state and local governments to fund the purchase of a wide range of security capabilities. Cybersecurity tools – from installing basic firewalls to deploying advanced defenses that rely on virtual “detonation chambers” – are allowable purchases, along with hazmat suits and interoperable communications tools. However, DHS can do more to encourage state and local governments to spend grant funds on cybersecurity, and Congress should support those efforts.

Mr. Chairman, that concludes my prepared testimony. I will be pleased to answer any questions the committee may have.



**Task Force Report on
Streamlining and Consolidating
Congressional Oversight of the
U.S. Department of Homeland Security**

September 2013





THE ANNENBERG RETREAT AT SUNNYLANDS

About the Annenberg Foundation Trust at Sunnylands

The Annenberg Foundation Trust at Sunnylands, which operates The Annenberg Retreat at Sunnylands and Sunnylands Center & Gardens at Rancho Mirage, Calif., is an independent 501(c)(3) nonprofit operating entity established by the Annenberg Foundation to hold high-level retreats that address serious issues facing the nation and the world community and to educate the public on the historical significance of Sunnylands. More information may be found online at www.sunnylands.org.



THE ASPEN INSTITUTE JUSTICE & SOCIETY PROGRAM

About the Aspen Institute Justice & Society Program

The Justice & Society Program convenes individuals from diverse backgrounds to discuss justice and how a just society ought to balance fundamental rights with the exigencies of public policy in meeting contemporary social challenges and developing the rule of law. The annual Justice & Society Seminar in Aspen, co-founded by Supreme Court Justice Harry A. Blackmun, continues to be led each summer by preeminent judges and law professors. JSP's Washington, D.C.-based public programming component brings together public officials, established and emerging opinion leaders, and grass-roots organizers to share their perspectives in a neutral and balanced forum. For more information, see www.aspeninstitute.org/jsp.

The Aspen Institute is an educational and policy studies organization based in Washington, D.C. Its mission is to foster leadership based on enduring values and to provide a nonpartisan venue for dealing with critical issues. It has campuses in Aspen, Colo., and on the Wye River on Maryland's Eastern Shore.

Task Force Executive Summary

Congressional leaders are best able to judge what committee should have jurisdiction over this department and its duties. But we believe that Congress does have the obligation to choose one in the House and one in the Senate, and that this committee should be a permanent standing committee with a nonpartisan staff.

—9/11 Commission Report

Nearly a decade after the 9/11 Commission issued its report on the greatest act of terrorism on U.S. soil, one of its most significant recommendations has not been acted upon. The call for consolidated Congressional oversight of the U.S. Department of Homeland Security (DHS) is, in the words of Commission co-chair Thomas H. Kean, “maybe the toughest recommendation” because Congress does not usually reform itself.

To underscore the importance of this reform, The Annenberg Foundation Trust at Sunnylands and the Aspen Institute’s Justice and Society Program convened a task force in April 2013, including 9/11 Commission co-chairs Kean and Lee H. Hamilton, former DHS officials under Presidents Barack Obama and George W. Bush, and members of Congress (Appendix). While the failure to reform DHS oversight may be invisible to the public, it is not without consequence or risk. **Fragmented jurisdiction impedes DHS’ ability to deal with three major vulnerabilities: the**

threats posed by small aircraft and boats; cyberattacks; and biological weapons.

“I think we’ve been distinctly less secure from a biological or chemical attack than we would have been had we had a more rational and targeted program of identifying the most serious threats,” said former Sen. Bob Graham (D., Fla.). As the 9/11 Commission Report noted: **‘So long as oversight is governed by current Congressional rules and resolutions, we believe that the American people will not get the security they want and need.’**

Earlier work by policy groups such as the Heritage Foundation and Brookings Institution attests to the consensus that consolidated oversight of DHS is needed. Among the concerns: More than 100 Congressional committees and subcommittees claim jurisdiction over it. In 2009, the department spent the equivalent of 66 work-years responding to Congressional inquiries. Moreover, the messages regarding homeland security that come out of Congress sometimes appear to conflict or are drowned out

altogether. As former DHS Secretary Michael Chertoff noted, “When many voices speak, it’s like no voice speaks.”

The task force recommends that:

- DHS should have an oversight structure that resembles the one governing other critical departments, such as Defense and Justice.
- Committees claiming jurisdiction over DHS should have overlapping membership.

Since a new committee structure cannot be implemented until the 114th Congress is seated in 2015, the task force also recommends these interim steps toward more focused oversight:

- Time-limiting subcommittee referrals to expedite matters of national security.
- Passing, for the first time since formation of the department in 2002, an authorization bill for DHS, giving the department clear direction from Congress.

Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security

So long as oversight is governed by current Congressional rules and resolutions, we believe that the American people will not get the security they want and need.

—9/11 Commission Report

In 2002, the federal government's third-largest department, the Department of Homeland Security, was created by putting under one umbrella 22 departments and agencies, from the Coast Guard in the Department of Transportation to the Border Patrol in the Department of Justice to the U.S. Secret Service in the Treasury Department. In July 2004, the 9/11 Commission issued 41 recommendations, including one that the Commission itself noted was among "the most important" but also "the most difficult to realize" — reform of Congressional oversight of the U.S. Department of Homeland Security (DHS). In the words of Commission co-chair Thomas H. Kean, "We had a number of members of the commission like [co-chair and former Rep. Lee H.] Hamilton who had served in the body, and they all said the same thing: This may be the toughest recommendation" because Congress doesn't usually reform itself.¹

The recommendation of the 9/11 Commission addressed problems that had contributed to the United States' vulnerability to attack on 9/11. Former Sen. Bob Graham (D., Fla.), co-chairman of the Senate Intelligence Committee on 9/11, recalls:

We found among other things that there had been inadequate communication among the agencies with a responsibility to alert us to a security threat. The FBI and the CIA had information which, had it been brought together, might well have allowed us to have avoided 9/11.²

The 9/11 Commission reached the same conclusion. In the words of former Gov. Kean:

Before 9/11, Congress was not doing its job of oversight of the intelligence agencies that were not doing the job themselves. That was one of the lessons of 9/11. This recommendation [resulted from asking the question], "How can we make sure that ... Congress is in fact ... doing the most that [it] can to protect [us]?"³

In the nine years since the 9/11 Commission issued its findings, the vast majority of its recommendations have been implemented in whole or in part. Not so the one urging the streamlining of Congressional oversight of DHS. Since the 9/11 report was promulgated, independent reports by a

variety of groups – including the Bipartisan Policy Center, the Heritage Foundation, the Brookings Institution, George Washington University's Homeland Security Policy Institute, and the Center for Strategic and International Studies-Business Executives for National Security – have underscored the need for oversight reform. They have characterized the current system as “balkanized and dysfunctional” (CSIS-BENS, 2004)⁴, “jurisdiction ... carved up to accommodate antiquated committee structures” (BPC, 2011),⁵ “duplicative and wasteful” (HSPI, 2004),⁶ a “crushing ... failure” (Brookings, 2006),⁷ and “byzantine” (Heritage, 2012).⁸

To raise awareness of the need for Congress to respond to this 9/11 Commission recommendation, The Annenberg Foundation Trust at Sunnyslands and the Justice and Society Program of the Aspen Institute, in partnership with the Annenberg Public Policy Center of the University of Pennsylvania, convened a high-level bipartisan Task Force on Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security, in April 2013, at The Annenberg Retreat at Sunnyslands in Rancho Mirage, Calif. Among its members are 9/11 Commission co-chairs Hamilton and Kean, former DHS officials under Presidents Barack Obama and George W. Bush, and past and present members of Congress (see Appendix, p. 24).

The task force members examined five questions:

- Why does Congressional oversight matter?
- What are the characteristics of an effective oversight structure?
- How does fragmented oversight affect

the nation's well-being and security?

- What are the structural and political barriers to reform?

- What should be done now and when the new Congress convenes in January 2015?

Drawing on the experience of its members as evidence, this report offers the Sunnyslands-Aspen Task Force's answers.

Why Congressional Oversight Matters

Congress' job is to look into every nook and cranny of the executive branch to see that the laws are being properly executed, to make suggestions [about] where improvements can be made. To understand what the policy of the executive branch is. To try to be constructive and to be a critic as well if they don't like what the executive is doing. If it is properly done, if the right questions are asked, it can greatly strengthen the operation of a department. ... Proper, tough, robust oversight can put the bureaucracy on its toes, can make sure that the law is being implemented, can see that there's not a lot of hanky-panky going on, corruption. And to make sure that the people are being well served.⁹

—9/11 Commission co-chair and former Rep. Lee H. Hamilton (D., Ind.)

“Properly executed” oversight, as former DHS Secretary Michael Chertoff notes, enables members of Congress to better “understand the department that they're looking at, understand the issues well, ask sharp and informed questions and get answers that are helpful in determining whether the

department or agency is performing most efficiently.”¹⁰ Former Homeland Security Adviser Kenneth L. Wainstein agrees: Effective Congressional oversight “enhances our national security” by helping “to inform the legislative process. The more Congress conducts oversight, the more [its members] understand the workings of the executive branch, and the better the legislation that they produce, which assists the executive branch in its efforts to protect the country.”¹¹

“We oversee to make sure that they’re doing what we ask them to do — that’s the law,” observes Rep. Loretta Sanchez (D., Calif.), a member of the House Committee on Homeland Security. “We oversee them to know that they’re not spending too much or too little money in an arena, that there’s no corruption.”¹²

“Congressional oversight,” says former Rep. John Tanner (D., Tenn.), “is probably as important a function of Congress as any other. ... It has to do with the wise utilization of whatever resources come to the government. And it has to do at the end of the day with the confidence level people have ... the confidence that the government is actually functioning in a way that makes sense to people.”¹³

The Characteristics of an Effective Congressional Oversight Structure

Effective oversight occurs when corresponding committees in each House hold a department accountable and use their power to ensure that it has the authorizations and resources it requires to accomplish its mission well and in a way that makes efficient use of tax dollars.

Congressional oversight is most constructive when a Congressional committee builds expertise and is in a position to see the

Congressional oversight is most constructive when a Congressional committee builds expertise and is in a position to see the big picture, ensuring that existing legislation is implemented properly and new legislation responds to evolving threats.

big picture, ensuring that existing legislation is implemented properly and new legislation responds to evolving threats. For example, as Chertoff notes, “Over time the committees in the defense area in Congress have had quite a lot of influence on the direction of defense policy because there’s been a single focal point in each House for authorizing what the Department of Defense does.”¹⁴

The Constitution, in Article I, Section 9, provides, in part: “No Money shall be drawn from the Treasury, but in Consequence of Appropriations made by Law.” This gives the Congress the power over federal spending. This legislative provision is broadly enforced by laws, such as the Antideficiency Act, that limit what executive branch officials can do with the funds given them.

As the size and role of government has grown, Congress has realized that it needs to divide policy deliberations from spending. Both Houses have established separate authorizing and appropriations committees to achieve this. Programs and their administration are to be funded through an annual

appropriation process, while overseen and authorized by a separate authorizing committee. The Congress exercises its "power of the purse" through this authorization and appropriation of funds.

Most executive agencies are chiefly associated with and scrutinized by a single legislative committee in each chamber of Congress. For instance, the operations of the Department of Labor are principally overseen in the Senate by the Committee on Health, Education, Labor & Pensions and in the House of Representatives by the Committee

on Education & the Workforce. Likewise, these two committees have the main responsibility for developing and drafting legislation relating to the Department of Labor.

The same is true of most of the other departments and agencies of the Executive Branch. The State Department is closely aligned with the House Committee on Foreign Affairs and the Senate Committee on Foreign Relations. As the following table shows, major Cabinet departments correspond with one or two substantive committees in each chamber of Congress.

Department or Agency	House Committee	Senate Committee
Agriculture	Agriculture	Agriculture, Nutrition & Forestry
Defense	Armed Services/ Intelligence	Armed Services/ Intelligence
Education	Education & the Workforce	Health, Education, Labor & Pensions
Energy	Energy & Commerce	Energy & Natural Resources
Justice	Judiciary	Judiciary
Labor	Education & the Workforce	Health, Education, Labor & Pensions
Director of National Intelligence/CIA	Intelligence	Intelligence
State	Foreign Affairs	Foreign Relations
Treasury	Financial Services/ Ways and Means	Finance/Banking, Housing and Urban Affairs
Veterans' Affairs	Veterans' Affairs	Veterans' Affairs

However, when jurisdiction is diffuse — asserted, in this case, by more than 100 committees and subcommittees, each with a different mandate — good oversight is difficult. As Chertoff, DHS Secretary from 2005 to 2009, said at Sunnylands:

A fragmented oversight structure means conflicting direction, maybe uncertainty about what Congress wants, and it certainly means a burden of appearing at hearings or producing paper for Congress that multiplies in a way that actually impedes the department's ability to focus on its operations.¹⁵

The lack of alignment between the House and Senate committees claiming jurisdiction is problematic as well. Currently, the Senate Homeland Security and Governmental Affairs Committee has less oversight of homeland security than its counterpart, the House Committee on Homeland Security. Caryn Wagner, who worked both on the House Permanent Select Committee for Intelligence and for DHS as Under Secretary for Intelligence and Analysis, explains the difficulty created when House and Senate committee jurisdiction does not match up:

The House passes a bill and the Senate passes a bill. Then they get together in conference and come up with one bill that ideally the president signs into law. If you don't have jurisdiction over the same elements, it's really impossible to conference a comprehensive bill.¹⁶

How Fragmented Oversight Affects the Nation's Well-Being and Security

The current state of DHS oversight hampers the department's functioning in three primary ways: redundant requests from committees drain valuable resources; the overlap of legislative roles complicates Congressional oversight and results in less Congressional control; and that same fragmentation prevents Congress from addressing pressing concerns in a timely fashion.

1. A Drain on Resources

Forcing people who should be doing their jobs securing our homeland to spend more of their time reporting to Congress than doing their job is wrong.¹⁷

—Former Rep. and House Rules Committee chair David Dreier (R., Calif.)

The complications created by fragmented oversight were on vivid display in November 2012 when a DHS official decided not to fulfill a request to testify before a Congressional committee. As Administrator of the Transportation Security Administration (TSA), a part of DHS, John S. Pistole oversees a 61,000-person workforce, the security of more than 450 U.S. airports, and the Federal Air Marshal Service, as well as highway, railroad, port, mass-transit and pipeline security throughout the nation. In late 2012, he drew attention to the issue of divided oversight when he declined a request by the House Subcommittee on Aviation to testify on passenger policies on the grounds that the panel lacked jurisdiction over the TSA.

At that time, Pistole said the TSA would continue to work with its committees of

jurisdiction to pursue effective security solutions. What appeared to the TSA to be a measured response to a redundant demand was taken by the subcommittee as a symbolic finger in the eye. While conceding that the subcommittee does not have “direct jurisdiction,” Rep. Bill Shuster (R., Pa.), the incoming chair, observed of the TSA, “When they impede the traveling public, they need to answer to the committee.”¹⁸ Although the TSA head challenged the subcommittee’s jurisdiction, the Homeland Security Department’s Inspector General’s office tacitly granted it by accepting an invitation to testify at the same hearing.¹⁹

In the 112th Congress (2011-2013), TSA personnel testified at 38 hearings and provided 425 briefings for members of Congress, numbers consistent with the worry expressed in 2010 by then-Homeland Security Secretary Janet Napolitano that:

Our principals and their staff [are] spending more time responding to Congressional requests and requirements than executing their mandated homeland security responsibilities.²⁰

Every request for a briefing or invitation to attend a hearing requires a commitment of resources. By one estimate, no other agency spends as much time on Capitol Hill as DHS. In 2007 and 2008, for example, officials at the Department of Veterans Affairs, a department of comparable budget and size to DHS, testified at half the number of hearings before just two committees, and gave less than one-tenth as many briefings as DHS.²¹ By contrast, Congress recently brought DHS officials before five committees for almost a dozen hearings on cybersecurity issues in less than a year, requesting answers to

Every request for a briefing or invitation to attend a DHS hearing requires a commitment of resources. By one estimate, no other agency spends as much time on Capitol Hill as DHS.

dozens of redundant questions on network protection.²² Nonetheless, Congress has been unable to pass a comprehensive cybersecurity bill.

“When you have different Congressional committees all asking questions or conducting oversight into the same areas of an agency’s operations,” Wainstein says, “that means that their officials ... who are responsible for, in the case of DHS, protecting the homeland [are] spending hours responding to redundant questions. ... That’s time that they’re not committing to protecting the nation.”²³

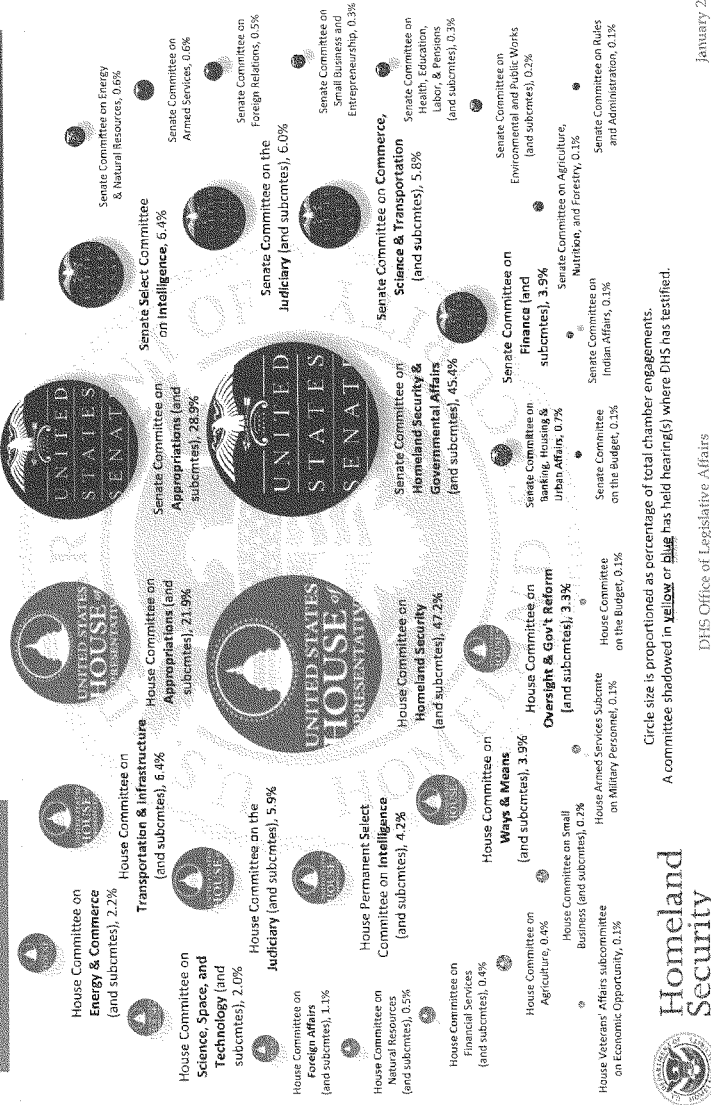
In the 112th Congress, more than 100 Congressional committees and subcommittees asserted jurisdiction over DHS (compared with the 36 committees and subcommittees that oversee the Department of Defense, which has a budget 10 times greater and millions more employees). DHS personnel participated in 289 formal House and Senate hearings, involving 28 committees, caucuses and commissions, which required testimony from more than 400 DHS witnesses. The department also participated in more than 4,300 briefings and other non-hearing engagements with Congress.²⁴

DHS Congressional Engagement ~ 112th Congress ~

1650 engagements with 17 of the
21 standing House Committees
204 were hearings

1346 engagements with 17 of the
25 standing Senate Committees
82 were hearings

119 Committees, Subcommittees,
caucuses and commissions



Think of having 100 bosses. Think of reporting to 100 people. It makes no sense. You could not do your job under those circumstances.²⁵

—9/11 Commission co-chair and former New Jersey Gov. Tom Kean

Three buzzwords used in Washington are “accountability,” “disclosure,” and “transparency.” Those three words are thrown out all the time. If you look at the notion of the people at the Department of Homeland Security being accountable, the difficult thing here is, to whom are they accountable?²⁶

—David Dreier

These numbers understate the time commitment required to respond effectively. Drafting testimony for each hearing typically requires the work of two or three subject matter experts. The Office of Legislative Affairs and the general counsel must review the prepared remarks. Depending on the issue, senior managers may need to approve the substantive content of the testimony. One or more preparation sessions are required. And after the hearing there typically will be a series of questions for the record, for which responses must be drafted. One estimate suggests that each hearing requires one month's worth of person-hours of preparation.²⁷ In 2009 alone, DHS spent roughly 66 work-years responding to questions from Congress, at a cost to taxpayers of \$10 million.²⁸

Rep. Lamar Smith (R., Texas), chair of the House Judiciary Committee, which oversees part of DHS, asserted in 2011 that Congress meant to create a “purposeful redundancy” with its oversight.²⁹ But as Kean

noted in a recent interview, “You can’t have oversight with over 90 committees ... [and] it’s gotten worse, not better. And so in that area, it continues to be dysfunctional. And everybody knows it.”³⁰

So, for example, in the House the Transportation Committee, which used to have the Coast Guard and FEMA under its supervision, will continue to try to insert itself into supervising those parts of the Department of Homeland Security, even though there actually is a Homeland Security Committee that’s supposed to look at the whole department. As a consequence it’s a little bit like childhood soccer games. Everybody runs after the ball, and they wind up colliding into each other.³¹

—Former Homeland Security Secretary Michael Chertoff

2. Diminished Congressional Influence

The fractured system of Congressional oversight makes it difficult for Congress to enact substantive legislation guiding DHS. Emblematic of this difficulty: In the 10 years since it was established, DHS has never had a comprehensive authorization bill. Such legislation, routine for comparable agencies such as the Department of Defense, is the forum in which Congress sets its priorities and offers comprehensive policy direction to a department, while providing it with the legislation necessary to effectively perform its daily operations. In the absence of such a bill, most DHS policy is made through the already overextended appropriations committees (a process that severely diminishes the Congressional “imprint” on DHS),

through piecemeal authorizations such as the SAFE Port Act, or through executive interpretation of statute.

"The authorizing legislation is the primary means by which the Congress tells the executive branch what it wants done," Hamilton notes.³² "They write it into law in the authorization law. Totally absent in the Department of Homeland Security. There's never been an authorization bill. Why not? Because responsibility is so fragmented within the House and the Senate that they can't get a bill out. ... What this means is that the power of the Congress is sharply diminished. And it shifts over to the executive branch because they don't have any guidance ... from Congress."

To get an authorization bill [for the Coast Guard] requires that bill to be sent to a lot of committees because they have jurisdiction over portions of the bill. ... In my four years as commandant of the Coast Guard, I did not get an authorization bill in any year. So every year I was appropriated money. But to the extent that there were changes in law needed for how we deal with oil spill response, the safety of vessels, these kinds of things, there was no vehicle by which to make those policy changes or seek changes in those laws for four years.³³

—Thad Allen, retired Admiral and
23rd Coast Guard Commandant

While DHS is not the only department hampered by the recent trend toward operating through appropriation and continuing resolutions, the negative effect of this lack of guidance on a relatively new department is

The fractured system of Congressional oversight makes it difficult for Congress to enact substantive legislation guiding the Department of Homeland Security.

more severe. In the words of Caryn Wagner, DHS Under Secretary for Intelligence and Analysis during President Obama's first term, "The lack of an effective authorization process for the Department headquarters compounds the difficulties of the Department in maturing its foundational business processes and in properly structuring and resourcing itself to achieve the type of synergy envisioned when the Department was created."

Moreover, the messages regarding homeland security that come out of Congress sometimes appear to conflict or are drowned out altogether. With so many Congressional voices dictating to DHS, there is little cost to the department in ignoring the messages that it dislikes or the policies it wishes not to implement. As Chertoff puts it: "When many voices speak, it's like no voice speaks."³⁴

The [DHS] winds up getting a mixed message. ... So either the department has no guidance or, more likely, the department ignores both because they're in conflict. And so the department does what it wants to do.³⁵

—Michael Chertoff

The erosion of interest in serving on the Committee has been accompanied by a decline in the age, homeland-security experience, and influence of its members, and thus in the influence of the Committee itself.

Among the problematic results is a reduced rather than enhanced Congressional role in protecting the homeland. So, for example, a 2012 study examining the degree of influence that Congress has over policy in various federal departments and agencies found an inverse correlation between the number of committees exercising oversight of an agency and Congressional influence on policy matters. Indeed, looking at DHS, the study said that the “108 committees and subcommittees overseeing the Department of Homeland Security may provide members with access to DHS resources but also affect the ability of Congress to compete with presidential influence over the general direction of agency policy. Members overly focused on securing district resources ... may be unwilling or unable to focus on the larger policy goals.”³⁶

Proceeding hand-in-hand with the proliferation of oversight committees has been a decline in interest in serving on the House Committee on Homeland Security. In the immediate aftermath of 9/11, the magnitude of that tragedy elicited a strong desire to serve on the Committee in order to enhance

the nation's security and resilience. As the memories of 9/11 have dimmed and no comparable attack has occurred, interest in serving has waned.

In the beginning, the committee actually was populated with some of the appropriators and some of the chairmen or more senior members of other committees that would have a vested interest in making homeland security a real being in the Congress. But after a while it became pretty apparent that those chairmen were not really interested in vesting the real meat of some of the problems in oversight issues in the committee, and so soon they fell off of the committee. They decided they didn't want to be on it any longer, and it became populated by people with less seniority, and today has many, many freshmen on it.³⁷

—Rep. Loretta Sanchez (D., Calif.),
Homeland Security Committee member

The erosion of interest in serving on the Committee has been accompanied by a decline in the age, homeland-security experience, and influence of its members, and thus in the influence of the Committee itself. In the process, overall Congressional participation in DHS oversight has — at least in part — degenerated into turf battles, as indicated by the cases of biological and cybersecurity threats and unregulated vehicles noted below. Moreover, where other departments and agencies enjoy the benefits of having a champion on their primary committee, DHS does not.

3. Delayed Response to Pressing Concerns

In a fragmented structure, no one committee is tasked with — and as a result accountable for — seeing the big picture. At the same time, getting legislation passed is complicated by competing demands from multiple committees and by a process that is filled with opportunities for intervention by those whose interests are not served by passage of the bill. Routine pieces of legislation that would enable the Department to function more effectively can take months to go through multiple committees with differing agendas, and may never be enacted.

I believe that the worst thing that happens by not concentrating oversight into a committee like the Homeland Security Committee is that everybody knows a little bit but nobody is really taking a look at the overall picture. And that's very dangerous because that's how things fall between the cracks.³⁸

—Rep. Loretta Sanchez

The Homeland Security Act was successful in creating a single subcommittee on appropriations for homeland security. But the act ... didn't resolve overlapping jurisdictions, gaps in jurisdictions [on the authorizing structure]. One of the things at the 10th anniversary of DHS that's sorely needed is a baseline evaluation of all those statutes that were merely aggregated against what we think Homeland Security ought to be 10 years later. And it's hard to do that with the current oversight structure with multiple committees.³⁹

—Thad Allen

During the retreat at Sunnylands, task force members identified vulnerabilities that highlight the need to consolidate oversight as soon as possible: unregulated small aircraft and boats, cybersecurity, and biological threats.

Unregulated Small Vehicles

Suppose I've got a small plane coming into Teterboro. I walk out to the airport and get into the plane. I don't go through any screening. The same problem occurs with boats. We have to get control of our air space and our waterways to make sure nothing that could harm us comes in by that method.⁴⁰

—Tom Kean

Task force members voiced concern that DHS and Congress have not done enough to protect against the prospect that small, general aviation aircraft and unregulated sea vessels will transport weapons of mass destruction into the United States, be used as weapons themselves (as were the planes on 9/11), or will transport individuals into the country intent on doing it harm. Admiral Thad Allen said that he spent years attempting to advance draft legislation on small-vessel security:

What size vessel should carry an identification device [of the sort] required on aircraft? Should there be licensing so you know who's operating a boat? Should there be areas where small boats shouldn't operate because of the vulnerable infrastructure that's in the area? ... If you try to come up with

a framework to deal with unregulated small boats and the vulnerabilities that exist there, and you look at the number of committees that would have to be involved, it becomes very, very hard. And frankly there hasn't been an appetite to take this on.⁴¹

Cybersecurity

"A lot of our national leaders — military leaders, leaders of our intelligence agencies — think that one of the great growing threats to American security are these cyberattacks," notes former Rep. Howard Berman (D., Calif.). Meanwhile, efforts to combat cyberthreats, including those originating from countries such as China and Iran, have been caught up in disputes over whether DHS or the National Security Agency has authority. Task force members fear that divided jurisdiction over this complex issue has made it more difficult for the nation to respond effectively to a major cyberattack, with one participant pressing for much greater attention to the difficulties of managing the nation's "virtual border in a global commons."⁴²

The Armed Services Committee has thoughts about the subject [of cybersecurity]. The Homeland Security Committee thinks this is about making the homeland more secure. ... So it is harder to get a consensus. It's harder to give the authority to the Executive Branch to create the defense than it might otherwise be. That's a problem.⁴³

—Former Rep. and Foreign Affairs Committee chair Howard Berman (D., Calif.)

The cyberthreat is a big threat to this country. Congress can't pass a bill on it. They've worked at it for years. They've not been able to agree between the House and Senate. ... What that means is that the House and Senate — the Congress, if you will — is deferring power to the president. The president writes an executive order. An executive order is not as good as a piece of legislation. It pertains to the executive branch. So there are limitations to that.⁴⁴

—Lee Hamilton

Cybersecurity is not an issue about partisanship because many of the proposed bills have had bipartisan support. It's really an issue of so many different committees that all have their particular interest and they can't get together with a coherent plan to pass a law to help protect the United States against very real cyberthreats.⁴⁵

—Arif Alikhan, deputy executive director for law enforcement and homeland security, *Los Angeles World Airports*

Attempts to clarify oversight have been frustrated. In 2005, for instance, a plan to give jurisdiction over cybersecurity to the House Homeland Security Committee was met by protests from the Energy & Commerce Committee, and the matter was dropped.⁴⁶ The seven Congressional committees that claim some jurisdiction over cybersecurity issues often clash, producing bills that conflict with one another by vesting jurisdiction in favored agencies within and outside DHS. The result: Bills are reported out of commit-

tee but fail to secure the needed votes on the House or Senate floor, or are so watered down that they fail to address the threat.

For example, in 2012 the House Homeland Security Committee's Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act sought to give cybersecurity regulatory authority to DHS. But it competed with the House Intelligence Committee's Cyber Intelligence Sharing and Protection Act, the House Oversight and Government Reform Committee's Federal Information Security Amendments, and the House Committee on Science, Space & Technology's Cybersecurity Enhancement Act—all of which put the authority elsewhere.⁴⁷ None got the traction to pass both houses of Congress.

In April 2013, for the second year in a row, the House passed the Cyber Intelligence Sharing and Protection Act. But the Senate has refused to vote on the measure. Senators now are reportedly drafting bills in at least three committees: Homeland Security, Commerce, and Intelligence.⁴⁸

Biological Threats

The need for a more systematic approach to bio-threats was voiced at the retreat by retired Sen. Bob Graham (D., Fla.), former co-chair of the Congressionally mandated Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, who said:

Unless the Congress is in a position to look at an issue like biological attacks in a strategic way and not just focus on the one piece of the problem that may be within the jurisdiction of a particular

committee, you're not likely to get it right, and the American people are therefore more vulnerable to what the WMD Commission found to be the most likely weapon of mass destruction to be used.⁴⁹

We haven't been able to get Congress to act because the responsibility for setting priorities for biological mechanisms is scattered in several committees and they have disagreed as to which federal agencies should have the ultimate responsibility for making these priority decisions and about how these decisions should be made. ... If the committee is responsible for, say, the Centers for Disease Control, it would like the responsibility to be in the Centers for Disease Control because then it would have oversight of it.⁵⁰

Though experts say that only a dozen or so deserve close scrutiny, the federal government maintains a list of 75 biological threats. Legislation recently introduced to prioritize those threats failed to pass. One of the primary reasons was disagreement over which agency will retain control. "We've been trying," Graham noted, "...to redo this list and have those 12 or so that are the major threats put in a category where they will get the highest level of attention and security. ... We haven't been able to do that because the Congress has the jurisdiction of the Department of Homeland Security in one committee and the jurisdiction of the Department of Health and Human Services in another, and they haven't been able to decide which executive agency should have the responsibility for managing this new list."⁵¹

Americans should not settle for incremental, ad hoc adjustments to a system designed generations ago for a world that no longer exists.

—9/11 Commission Report

Structural and Political Barriers to Reform

Despite the advantages that would accrue to the nation, task force members and other experts have noted roadblocks to consolidating and streamlining DHS oversight. Chief among them: strong resistance from the chairs of committees who would lose some of their power were oversight to be streamlined and the challenge of capturing the media's attention and the public's imagination with an issue that at first glance appears remote from most people's lives.

Those seeking to reform oversight must take into account the political realities that undergird the jurisdictional structure. Service as chair of the House Committee on Homeland Security or the Senate Homeland Security and Governmental Affairs Committee is unlikely to carry electoral payoffs, since enhancements to public safety are most often experienced at the national level rather than as specific benefits to a district or state. Moreover, if oversight reform is implemented, some existing committee chairs will lose some power and turf.

Members of Congress have tried to keep as much of the power that they had historically through this concept of legacy jurisdiction over the agencies even though the agencies have technically been moved under another committee.⁵²

—Bob Graham

One of the things I concluded 20 years ago was that members of Congress would just as soon give up their first-born [as] give up jurisdiction over the executive branch in particular areas.⁵³

—David Dreier

All of this suggests that the most promising strategy for reform lies in convincing Congressional leadership that it is the right thing to do. Only a leadership convinced of the benefits to the country is likely to make such oversight reform happen.

Finally, the issue of Congressional oversight has long been seen as an "inside-the-Beltway" problem, one hidden beneath layers of procedure and mundane logistics. As a result, even though Congress' failure to act may jeopardize the safety and security of the country, it has been difficult to mobilize public interest in remedying the problem. Former Rep. Dan Glickman (D., Kan.), executive director of the Aspen Institute's Congressional program, recently observed that the American people are most concerned with issues that affect their day-to-day lives, and that is why more people have an opinion about the TSA than about most other DHS component agencies.

Americans encounter DHS' FEMA in times of disaster, its Customs and Border Protection during international travel, and its Coast Guard employees in coastal communities and at sea. Yet a decade after DHS was formed, most Americans still don't understand the department's "all hazards" mission, or how all

its components fit together. As a result, the public is unlikely to tell members of Congress that they ought to reform the oversight structure of DHS. And an issue involving oversight is, admittedly, a distinctly unsexy topic, far less likely than others to capture media attention.

What Should Be Done Now and When the New Congress Convenes in January 2015

To meet the ongoing security challenges our country faces, the task force recommends specific actions by the executive and legislative branches, as well as a role for the media:

1. Congress

Fragmented oversight, the task force concluded, increases security risks for the United States by reducing the coherence of our national focus on prevention, protection and planning at a time when more needs to be done. Under the current arrangement, retired Coast Guard Admiral and task force member Thad Allen said, Congress all too often “engages in random acts of after-sight.”

Consistent with the 9/11 Commission’s recommendation, this report has argued:

To ensure that the oversight process works efficiently, Congress should significantly reduce the number of committees with jurisdiction over homeland security and consolidate primary oversight of the key DHS component agencies under one committee in the House and one in the Senate, with coordinated jurisdiction.

Task force members were united in the conviction that:

Consolidating Congressional oversight of DHS would enhance accountability.

If it is to function effectively, such oversight should be consistent with that of Cabinet departments that bear similar levels and kinds of responsibility for the safety and resilience of Americans in the face of both man-made and natural threats and disasters.

The task force believes that the oversight process in both houses should be significantly streamlined and the Senate and House oversight structures aligned with each other to the extent possible.

The task force noted that previous studies agree that streamlined Congressional oversight of DHS would benefit the nation. Their reform proposals include separating the supervision of DHS’ immigration and homeland security roles and retaining the main oversight committees while canceling the jurisdiction of other Congressional committees considered redundant.

This task force believes that Congress is best positioned to decide which structure best satisfies the 9/11 Commission's goal. But it recommends that any structure be consistent with the following principles:

- The oversight structure for DHS should resemble the one governing other critical departments, such as the departments of Defense and Justice.
- Congress should align the jurisdictional oversight of the House and Senate committees to the greatest extent possible.
- Committees claiming common jurisdiction should have some overlapping membership to encourage the sharing of information and curtail redundant requests.

The consolidation and simplification of oversight depends largely upon Congressional leadership. The best chance for major reform comes during reorganization at the beginning of a new Congress. In the meantime, there are ways that Congress can enhance the effectiveness of oversight without requiring committees to relinquish jurisdiction. For instance, it can pass authorizing legislation and ensure expedited action by imposing time limits on committee referrals.

Pass Authorizing Legislation The need to pass authorizing legislation extends beyond DHS. By some estimates the country is operating with approximately \$400 billion of spending unauthorized annually. As this report contends, passing authorizations improves Congressional oversight and prioritizes programs within DHS. When large

segments of the Department of Homeland Security operate with "unauthorized appropriations," the administration is able to set its priorities unguided by Congress and might not be spending money on programs that Congress considers important.

Limit the Time for Action When a bill comes under the jurisdiction of multiple committees that ask to review it in sequence after the primary committee acts, the process is all but stopped awaiting committee action unless there is a time limit on the referrals. Time may run out with nothing enacted. The task force believes that Congress should limit the time for action of sequential referrals to another committee, ensuring that if committees fail to act on what has been sent to them within a set period of time their jurisdiction would lapse, with the matter returning to the primary committee.

2. The Executive

The White House could increase the likelihood that pressing issues move onto the national and Congressional agenda by creating a more robust role for the Homeland Security Adviser, and by placing the Secretary of Homeland Security on the National Security Council.

3. Media and Public Information

If Kean is correct that Congress is unlikely to reform itself, then reform must be jump-started by external demand. As shown by the country's experience with the Boston

Marathon bombing, recent ricin threats against public officials, and natural disasters from Hurricane Sandy to the May 2013 Oklahoma tornado, the fourth estate has a vital role to play in informing the public about national security concerns, and the nation's editorial pages have the capacity to increase the likelihood that Congress will see the wisdom of implementing this important recommendation of the 9/11 Commission Report.

The Bottom Line

In sum, while reform of Congressional oversight can't make the nation 100 percent safe, it is a key component of any national effort to manage evolving threats. We close with the words of two task force members:

We have a really important issue. How do we keep America secure? And we have a structure in the Congress that makes it harder to maintain that focus on that very important issue. And that's not good.⁵⁴

—Howard Berman

If the [oversight] recommendation of the 9/11 Commission on Homeland Security is put into law and becomes effective, the American people in their pursuit of their daily lives will be safer.⁵⁵

—Lee Hamilton

NOTES

- ¹ Lee H. Hamilton and Thomas H. Kean interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ² Bob Graham interview, 1 August 2013, New York, N.Y.
- ³ Thomas Kean interview, 12 August 2013, Far Hills, N.J.
- ⁴ "Untangling the Web: Congressional Oversight and the Department of Homeland Security," 10 December 2004, Center for Strategic and International Studies-Business Executives for National Security.
- ⁵ "Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations," September 2011, Bipartisan Policy Center.
- ⁶ "Consolidating the House's Homeland Security Efforts: The Time to Act Is Now," 29 December 2004, George Washington University Homeland Security Policy Institute.
- ⁷ Norman J. Ornstein and Thomas E. Mann, "When Congress Checks Out," November/December 2006, Brookings Institution.
- ⁸ Jessica Zuckerman, "Politics Over Security: Homeland Security Congressional Oversight In Dire Need of Reform," 10 September 2012, the Heritage Foundation. See also "Stopping the Chaos: A Proposal for Reorganization of Congressional Oversight of the Department of Homeland Security," 4 November 2010, the Heritage Foundation.
- ⁹ Lee Hamilton interview, 8 August 2013, Bloomington, Ind.
- ¹⁰ Michael Chertoff interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ¹¹ Kenneth Wainstein interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ¹² Loretta Sanchez interview, 17 July 2013, Washington, D.C.
- ¹³ John Tanner interview, 16 July 2013, Washington, D.C.
- ¹⁴ Michael Chertoff interview, 25 July 2013, Washington, D.C.
- ¹⁵ Michael Chertoff interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ¹⁶ Caryn Wagner interview, 16 July 2013, Washington, D.C.
- ¹⁷ David Dreier interview, 19 July 2013, Los Angeles, Calif.
- ¹⁸ Jeff Plungis, "TSA to Mica: You Have No Jurisdiction," *Bloomberg*, 27 November 2012, <http://go.bloomberg.com/political-capital/2012-11-27/tsa-to-mica-you-have-no-jurisdiction/>.
- ¹⁹ Jim Barnett, "TSA Chief Will be a 'No Show' at Congressional Hearing," CNN, 29 November 2012, <http://www.cnn.com/2012/11/28/politics/tsa-friction>.
- ²⁰ "Inside Washington: DHS Most Overseen Department," Associated Press, 17 May 2011, <http://www.npr.org/templates/story/story.php?storyId=136382414>.
- ²¹ Sarah Laskow, "Is Congress Failing on Homeland Security Oversight?" Center for Public Integrity, 16 July 2009, <http://www.publicintegrity.org/2009/07/16/2822/congress-failing-homeland-security-oversight>.
- ²² Aliya Sternstein, "House Homeland Security Lawmakers Request Sole Oversight," *Nextgov*, 25 January 2012, <http://www.nextgov.com/cybersecurity/2012/01/house-homeland-security-lawmakers-request-sole-oversight-of-dhs/50515/>.
- ²³ Kenneth Wainstein interview, 16 July 2013, Washington, D.C.
- ²⁴ Data provided by the DHS Office of Legislative Affairs.
- ²⁵ Thomas Kean interview, 12 August 2013, Far Hills, N.J.
- ²⁶ David Dreier interview, 19 July 2013, Los Angeles, Calif.

- ²⁷ DHS, Office of Legislative Affairs Internal Analysis (2007).
- ²⁸ "Inside Washington: DHS Most Overseen Department," Associated Press, 17 May 2011, <http://www.npr.org/templates/story/story.php?storyId=136382414>.
- ²⁹ Jeff Plungis, "TSA to Mica: You Have No Jurisdiction," *Bloomberg*, 27 November 2012, <http://go.bloomberg.com/political-capital/2012-11-27/tsa-to-mica-you-have-no-jurisdiction/>.
- ³⁰ Thomas Kean interview, 12 August 2013, Far Hills, N.J.
- ³¹ Michael Chertoff interview, 25 July 2013, Washington, D.C.
- ³² Lee Hamilton interview, 8 August 2013, Bloomington, Ind.
- ³³ Thad Allen interview, 17 July 2013, Washington, D.C.
- ³⁴ Michael Chertoff interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ³⁵ Michael Chertoff interview, 25 July 2013, Washington, D.C.
- ³⁶ Joshua D. Clinton, David E. Lewis, and Jen Selin, "Influencing the Bureaucracy: The Irony of Congressional Oversight," Center for the Study of Democratic Institutions, 3 May 2013, http://www.vanderbilt.edu/csdi/research/cls_csdiwp_5_2012.pdf.
- ³⁷ Loretta Sanchez interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ³⁸ Loretta Sanchez interview, 17 July 2013, Washington, D.C.
- ³⁹ Thad Allen interview, 17 July 2013, Washington, D.C.
- ⁴⁰ Thomas Kean interview, 12 August 2013, Far Hills, N.J.
- ⁴¹ Thad Allen interview, 17 July 2013, Washington D.C.
- ⁴² Thad Allen interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ⁴³ Howard Berman interview, 19 July 2013, Los Angeles, Calif.
- ⁴⁴ Lee Hamilton interview, 8 August 2013, Bloomington, Ind.
- ⁴⁵ Arif Alikhan interview, 19 July 2013, Los Angeles, Calif.
- ⁴⁶ A draft report for the Sunnylands-Aspen Task Force, 17 March 2013, prepared by William Pitts, who was chief policy adviser to former Rep. Robert Michel (R., Ill.) and chief of staff to former House Rules Committee Chair Rep. David Dreier (R., Calif.).
- ⁴⁷ Mickey McCarter, "House to Vote on 4 Cybersecurity Bills But Not Homeland Security Committee Measure," *Homeland Security Today*, 23 April 2012, <http://www.hstoday.us/industry-news/general/single-article/house-to-vote-on-4-cybersecurity-bills-but-not-homeland-security-committee-measure/1be33a8fe12129b1bf5e87c40da1c40a.html>.
- ⁴⁸ Jason Koebler, "ACLU: CISA Is Dead (For Now)," *U.S. News & World Report*, 25 April 2013, <http://www.usnews.com/news/articles/2013/04/25/aclu-cispa-is-dead-for-now>. Chloe Albaneisus, "Senate Will Not Consider CISA, Citing Privacy," *PC Magazine*, 26 April 2013, <http://www.pcmag.com/article2/0,2817,2418228,00.asp>.
- ⁴⁹ Bob Graham interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ⁵⁰ Bob Graham interview, 1 August 2013, New York, N.Y.
- ⁵¹ Bob Graham interview, 6 April 2013, The Annenberg Retreat at Sunnylands.
- ⁵² Bob Graham interview, 1 August 2013, New York, N.Y.
- ⁵³ David Dreier interview, 19 July 2013, Los Angeles, Calif.
- ⁵⁴ Howard Berman interview, 19 July 2013, Los Angeles, Calif.
- ⁵⁵ Lee Hamilton interview, 8 August 2013, Bloomington, Ind.

Appendix

Task Force on Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security

Task Force Members

Arif Alikhan	Juliette Kayyem
Thad Allen	Thomas H. Kean Sr.
Howard Berman	Loretta Sanchez
Michael Chertoff	John Tanner
David Dreier	Caryn A. Wagner
Bob Graham	Kenneth L. Wainstein
Lee H. Hamilton	

Retreat Organizers

Meryl Justin Chertoff	Kathleen Hall Jamieson

Biographical Information on Retreat Participants and Organizers

Arif Alikhan

Counterterrorism and homeland security expert Arif Alikhan joined Los Angeles World Airports as the new deputy executive director for law enforcement and homeland security on Nov. 7, 2011. Prior to that, Alikhan was a Distinguished Professor of Homeland Security and Counterterrorism at National Defense University in Washington, D.C. Alikhan previously served as assistant secretary for policy development at the U.S. Department of Homeland Security. His federal service also includes 10 years with the U.S. Department of Justice as a federal prosecutor and senior adviser to two U.S. attorneys general on cybercrime and intellectual property.

Thad Allen

Thad Allen is senior vice president of the Virginia-based consulting firm Booz Allen

Hamilton. Allen supports the firm's work with the departments of Justice and Homeland Security. Allen completed his distinguished career in the U.S. Coast Guard as its 23rd commandant. Prior to that assignment, Allen served as Coast Guard chief of staff. During his tenure in that post, in 2005, he was designated principal federal official for the U.S. government's response and recovery operations in the aftermath of hurricanes Katrina and Rita in the Gulf Coast region.

Howard Berman

Howard Berman is a former representative from California who served 15 consecutive terms in the U.S. House of Representatives from 1982 to 2012. In 2008, he was appointed chairman of the Foreign Affairs Committee. In addition, Berman served on the Judiciary Committee and the Subcommittee on Immigration, Citizenship, Refugees, Border Security & International Law.

Meryl Justin Chertoff

Meryl Justin Chertoff is director of the Aspen Institute's Justice and Society Program and an adjunct professor of law at Georgetown Law. From 2006 to 2009, Chertoff was director of the Sandra Day O'Connor Project on the State of the Judiciary at Georgetown Law. She served in the Office of Legislative Affairs at the Federal Emergency Management Agency, participating in the agency's transition into the Department of Homeland Security. Chertoff has been director of New Jersey's Washington, D.C., office under two governors, and legislative counsel to the chair of the New Jersey State Assembly Appropriations Committee.

Michael Chertoff

Michael Chertoff served as secretary of the U.S. Department of Homeland Security from 2005 to 2009. He is chairman and co-founder of the Chertoff Group. At the Chertoff Group, Chertoff provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response, and recovery. Before heading the Department of Homeland Security, Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit.

David Dreier

David Dreier was elected to Congress from California in 1980 and became a member of the House leadership when he took the helm of the House Committee on Rules in 1999. As the youngest Rules chairman, he played a pivotal role in fashioning legislation for debate in the House. He authored the 1995 Congressional reform package. He is a member of the Council on Foreign Relations

and serves on the board of the International Republican Institute. Dreier is the founding chairman of the House Democracy Partnership and the founding chair of the Congressional Trade Working Group.

Bob Graham

Bob Graham is the former two-term governor of Florida and served for 18 years in the U.S. Senate. Graham retired from public service in January 2005, following his presidential campaign in 2004. After retiring from public life, Graham spent a year as a senior fellow at the Harvard Kennedy School of Government. In recent years, he was appointed by President Obama and served as co-chair of the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. This followed his service as a commissioner on the Financial Crisis Inquiry Commission, as chairman of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, and on the CIA External Advisory Board.

Lee H. Hamilton

Lee H. Hamilton is director of the Center on Congress at Indiana University. He served in the U.S. House of Representatives from 1965 to 1999, representing Indiana's 9th District. Since retiring from Congress, Hamilton remains at the center of efforts to address some of the nation's major homeland security and foreign policy challenges. He served as vice chair of the 9/11 Commission, co-chair of the Iraq Study Group, and co-chair of the U.S. Department of Energy's Blue Ribbon Commission on America's Nuclear Future. He is a member of the President's Intelligence Advisory Board, the President's Homeland Security Advisory Council, the CIA External

Advisory Board, and the U.S. Department of Homeland Security Task Force on Preventing the Entry of Weapons of Mass Effect on American Soil.

Kathleen Hall Jamieson

Kathleen Hall Jamieson is the Elizabeth Ware Packard Professor of Communication at the Annenberg School for Communication and Walter and Leonore Annenberg Director of the Annenberg Public Policy Center at the University of Pennsylvania. She is a fellow of the American Academy of Arts and Sciences, the American Philosophical Society, the American Academy of Political and Social Science, and the International Communication Association. Jamieson is the author or co-author of 16 books. She is co-founder of FactCheck.org, founder of the new political literacy site FlackCheck.org, and program director of The Annenberg Retreat at Sunnylands.

Juliette Kayyem

Juliette Kayyem is a lecturer in public policy at the Harvard Kennedy School of Government, a former national security and foreign policy columnist for *The Boston Globe*, and a former contributor to CNN. She served President Obama as Assistant Secretary for Intergovernmental Affairs at the Department of Homeland Security. She served as co-chair of the Congressionally mandated Preparedness Task Force, and as a member of President Obama's Task Force on Puerto Rico and the Defense Department's Council of Governors. Before joining the Obama Administration, Kayyem served as Massachusetts Gov. Deval Patrick's homeland security adviser.

Thomas H. Kean Sr.

Tom Kean served as president of Drew University from 1990 to 2005 and as governor of New Jersey from 1982 to 1990. In 1986, he was re-elected governor by the largest margin in state history. Prior to serving as governor, Kean was a member of the New Jersey Assembly from 1968 to 1977. In 2002, President George W. Bush named Kean as chairman of the 9/11 Commission. He headed the American delegation to the U.N. Conference on Youth in Thailand, was vice chairman of the American delegation to the World Conference on Women in Beijing, and served as a member of the President's Initiative on Race.

Loretta Sanchez

Congresswoman Loretta Sanchez was first elected to the House of Representatives in 1996, and is currently serving her ninth term as the representative for California's 46th District. Sanchez is the second highest-ranking Democrat on the House Armed Services Committee. She is the ranking member of the Tactical Air and Land Forces Subcommittee. Rep. Sanchez is also a senior member of the Subcommittee on Strategic Forces. She is founder and co-chair of the Women in the Military Caucus and is the highest-ranked female on the Armed Services Committee. She also serves on the House Committee on Homeland Security, where she is the second-ranked Democrat and most senior female member.

John Tanner

John Tanner is vice chairman of Prime Policy Group. He joined the firm after serving in the U.S. House of Representatives for 22 years, representing Tennessee's 8th District. In

Congress, Tanner served on the House Foreign Affairs Committee and the Ways & Means Committee. He also served on the House Armed Services and House Science Committees and served as Chief Deputy Whip for the Democratic Congress in the 109th, 110th, and 111th Congresses. In November 2008, Tanner was elected to a two-year term as president of the NATO Parliamentary Assembly.

Caryn A. Wagner

Caryn Wagner served as Under Secretary for Intelligence and Analysis in the Department of Homeland Security from 2010 to 2012. She served on the intelligence agency review team of the Obama-Biden Transition Project. She retired from federal service from the House Permanent Select Committee on Intelligence on Oct. 1, 2008, for which she served as budget director and cybersecurity coordinator. Prior to that, Wagner served in the Office of the Director of National Intelligence as an assistant deputy director of

National Intelligence for Management and was the first chief financial officer for the National Intelligence Program. Her final position was that of the senior Defense Intelligence Agency Representative to Europe.

Kenneth L. Wainstein

Kenneth L. Wainstein is co-chair of the business fraud group at the law firm of Cadwalader, Wickersham & Taft. In 2008, after 19 years at the Justice Department, Wainstein was named homeland security adviser by President George W. Bush. Prior to his White House service, he was twice nominated and confirmed for leadership positions in the Justice Department. In 2006, the U.S. Senate confirmed him as the first Assistant Attorney General for National Security. In 2004, he was appointed, and later confirmed, as the U.S. attorney in Washington, D.C. In 2001, he was appointed director of the Executive Office for U.S. Attorneys, where he provided oversight and support to the 94 U.S. Attorneys' Offices.

The New York Times

September 10, 2013

Homeland Confusion

By THOMAS H. KEAN and LEE H. HAMILTON

NO single event in the last half-century has had a greater effect on American national security policy than the terrorist attacks that occurred 12 years ago today. When we co-chaired the 9/11 Commission, which was set up in 2002 and issued its report on the attacks in 2004, we investigated the failures that left our country vulnerable and recommended 41 actions to correct them and strengthen our national security.

Nine years after the 9/11 Commission made its case, our country is still not as safe as it could and should be. Though the vast majority of our recommendations have been followed, at least in part, Congress has not acted on one of our major proposals: to streamline the way it oversees homeland security.

In a cumbersome legacy of the pre-9/11 era, Congress oversees the Department of Homeland Security with a welter of overlapping committees and competing legislative proposals. The department was created in 2002 out of 22 agencies and departments. More than 100 congressional committees and subcommittees currently claim jurisdiction over it. This patchwork system of supervision results in near-paralysis and a lack of real accountability.

This needs to change. In a bipartisan report that we are releasing today, as members of a task force of national security experts, former Homeland Security officials and former and current members of Congress (convened by the Annenberg Retreat at Sunnylands and a program of the Aspen Institute), we argue that the American people will be safer if Congress takes a clearer, less complicated approach to its supervision of national security. Congress needs to treat the Department of Homeland Security as it does the Departments of Justice and Defense and give primary oversight responsibility to fewer committees.

The complexity of the current system leads to gridlock. In August, Robert S. Mueller III, then the director of the Federal Bureau of Investigation, warned that a cyberthreat will “equal or even eclipse the terrorist threat” — yet the seven

congressional committees that claim jurisdiction over the issue haven't been able to agree on whether the Department of Homeland Security or another agency should take primary responsibility for addressing the threat.

Last year, when a bill on cybersecurity from the House Homeland Security Committee competed with proposals from three other House committees, none gained enough traction to pass both the House and the Senate. In April, a bill on cybersecurity intelligence sharing was passed by the House, but it has not been brought to a vote in the Senate, which is reportedly drafting its own bills on the issue in at least three different committees.

The system also results in gaps in oversight. When you fly on a major airline from a major airport, you are screened by the Transportation Security Administration, a part of the Department of Homeland Security — but because of insufficient federal supervision, that's not necessarily so when you board a private jet at any number of small airports across the United States. Likewise, a federal list of 75 biological threats hasn't been properly prioritized, preventing us from focusing on the deadliest ones, in part because Congress oversees the Department of Homeland Security in one committee and Health and Human Services in another.

Finally, the system is wasteful. In the 112th Congress, which ended in January, Homeland Security personnel took part in 289 formal House and Senate hearings, involving 28 committees, caucuses and commissions. In 2009 alone, Homeland Security personnel spent the equivalent of 66 work-years responding to questions from Congress, at an estimated cost to taxpayers of \$10 million.

This isn't a partisan issue. The first homeland security secretary, Tom Ridge, a Republican appointee, raised concerns during his tenure about the fragmented system of oversight, and the former homeland security secretary Janet Napolitano, a Democratic appointee, complained that members of her staff were often "spending more time responding to Congressional requests and requirements than executing their mandated homeland security responsibilities."

Congress, typically reluctant to give up its powers midterm, is unlikely to enact serious reform until the 114th Congress in 2015. In the meantime, though, members should take steps to accelerate homeland security legislation by

placing time limits on committees' consideration of Homeland Security bills. They also should set clear priorities for the department by passing an authorization bill, which Congress has never done.

Congress needs to reform the way it oversees homeland security and examine the department with tough and direct scrutiny. As we said in the 9/11 Commission report, unless Congress does its job, "the American people will not get the security they want and need."

Thomas H. Kean and Lee H. Hamilton, members of a task force on oversight of the Department of Homeland Security, were co-chairmen of the 9/11 Commission.

Tom Ridge

November 8, 2013

(Sent Via Email to Laura W. Kilbride at Laura_Kilbride@hsgac.senate.gov)

Senator Thomas J. Carper
U.S. Senate Committee on Homeland Security & Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC, 20510

Attn: Laura W. Kilbride

Dear Senator Carper:

Thank you for the opportunity to testify on September 11, 2013 on "The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats." I am grateful for the work the men and women of DHS do each and every day but realize there is still much more to do to ensure our security and prosperity in a rapidly evolving environment. The committee's interest in information sharing, cybersecurity, and the management of DHS are of utmost importance. As we discussed at the hearing, I am very concerned about the number of senior level vacancies at DHS and I urge the Senate to take up the outstanding nominations for DHS leadership positions in a timely and judicious manner upon nomination by the President.

I have attached my answers to the Questions for the Record submitted by Senators Ayotte and McCaskill. I ask they be included as part of the hearing record. Thank you.

Sincerely,

A handwritten signature in black ink that reads "Tom Ridge" followed by a horizontal line.

Tom Ridge
First Secretary, U.S. Department of Homeland Security
43rd Governor of the Commonwealth of Pennsylvania
CEO, Ridge Global

Attachment

**Post-Hearing Questions for the Record
Submitted to Hon. Tom Ridge
By Senator Claire McCaskill**

“The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats”

Wednesday, September 11, 2013

- 1) During the hearing, the witnesses all agreed that the unification of DHS from numerous individual agencies has been slow to occur. As a result, the federal government views threats to the homeland in silos and the relative risks of events in different silos are not weighed against each other. DHS directs the spending of billions dollars without understanding, for example, an unexpectedly powerful hurricane impacting the northeast is more or less likely than a crop duster releasing anthrax over St. Louis.

Do you believe it is wise, particularly given the current fiscal environment, for DHS to continue issuing material threat assessments that look only at the likelihood of different types of terrorist attacks weighed against each other, or should these threat assessments be broadened to assess the relative likelihoods of all threats to the homeland (from terrorism to natural disasters to pandemics) so that spending more accurately reflects the likelihood of all threats?

Washington is often a reactionary in terms of how it provides resources. Constantly “fighting the last war” leaves the nation vulnerable to new, evolving or emerging threats. For example, in the aftermath of 9/11 the public focus was on fighting terrorism. In the wake of Hurricane Katrina, there was a concentration on preparedness and response to natural disasters. But we must be careful to avoid pendulum-like swings. At the end of the day, DHS is an all-hazards agency. It must be prepared to assess threats to the nation from any number sources--manmade or natural. If the fiscal environment or any one particular concern becomes the predominant driver of what and how we assess threats, we will limit our visibility into the full range of threats thereby resulting in an incomplete threat picture. While we cannot know or prevent everything, having a robust understanding of the range of threats is critical to identifying key interdependencies and is a foundation for maintaining a risk-based approach and funding for homeland security.

- 2) All of the witnesses touched on risk-based approach to homeland security. However, none of the witnesses discussed what DHS has told my staff is the greatest threat to homeland security: the so-called lone wolf operator. While detecting and protecting against lone wolf operators is inherently more difficult than actions taken by foreign terrorist networks, they must nonetheless be included in any risk-based calculations and threat assessments. These assessments are used to procure hundreds of millions of dollars in technological defenses and biological countermeasures. In your experience,

how, if at all, is the lone wolf actor accounted for when DHS assesses threats to the homeland?

I would defer to DHS on how it currently and specifically assesses lone wolf threats. But I can say that lone wolves were of concern during my tenure at DHS. They are the most difficult actors to combat because—by their nature—they limit their connectivity to others. Interestingly, it requires our intelligence, law enforcement, and technical stakeholders to be very connected in order to share information that can be used to identify and neutralize lone wolf actors. To the extent possible, we should ensure that technological and detection procurements are tied to relevant information sharing programs and protocols.

Information sharing will continue to be a challenge for multi-jurisdictional stakeholders. And it will never be perfect. But we can focus on constant improvement. In its oversight role, Congress should regularly assess both horizontal (across the Federal family, particularly members of the IC) and vertical (Federal to state and local). It should also regularly engage state and local law enforcement and other first responder organizations, and private sector security experts in order to receive updates on information sharing gaps/challenges as well as to illuminate successful models that may duplicated.

**Post-Hearing Questions for the Record
Submitted to the Honorable Thomas J. Ridge
From Senator Kelly Ayotte**

**“The Department of Homeland Security at 10 Years: Examining Challenges and
Achievements and Addressing Emerging Threats”
September 11, 2013**

- (1) In your written testimony, you noted the importance of information sharing. You further noted that the intelligence community must renew its commitment to bridge gaps and work together—and I wholeheartedly agree. To that end, what is the importance of having DHS intelligence officers in fusion centers? In my state, the New Hampshire Information and Analysis Center benefits immensely from that DHS presence and expertise.

Yes, fusion centers play a critical role in the sharing of information amongst Federal, State, and Local law enforcement officials. However there needs to be a proper level of oversight to make sure that fusion centers remain effective. Threats change and evolve. As such, we must regularly assess that our fusion centers are not just processing reams of data, but are producing a return on investment—both in terms of resources committed and the quality and relevance of products that they produce. As mentioned in my remarks, Congress must ensure that DHS remains a key component of the intelligence community at large to ensure that its stakeholders at the state, local, and private sector level are appropriately informed of risks and threats. Further, Congress should always have an oversight role in balancing our security needs with the protection of privacy and civil liberties.

Having a DHS presence at fusion centers can help ensure the proper flow of information both from the federal intelligence arm down to the local level and vice versa. It is critical for players from both sides of the equation to have actual working knowledge of one another's operational environment and to see the benefit of bi-directional collaboration on a regular basis.

- (2) While we have made progress in the fight against Al Qaeda, affiliate groups are showing a resurgence in Al Qaeda's ideological extremism and the threat is growing in the region. Factions and affiliates now cover an even wider geographic area—Al Qaeda in the Islamic Maghreb, Al Qaeda in the Arabian Peninsula, Al Qaeda in Iraq, al-Nusra, and Al Shabaab, to name a few. From your perspective as a former Secretary of DHS, how do we stop these groups from gaining greater influence within their geographic areas, and among sympathizers who may be in the United States? What must we do to prevent them from conducting, encouraging, or inciting violence against American interests?

The groups you mention share a common enemy in the United States and our way of life. In some cases, these groups are willing to ally themselves if

necessary to expand their operational capabilities. Likewise, we must not only leverage full US intelligence assets, but those of our allies as well. Unfortunately, the Snowden affair and resulting scrutiny of the National Security Agency have complicated this effort by straining many allied relationships.

However, our intelligence community and the US military cannot be left alone to act. If we are to protect American interests and avoid the loss of blood and treasure whenever possible, the United States must express its leadership on the world stage utilizing a diverse portfolio of assets. The current global threat environment demands a multi-prong US approach to include consistent policy and diplomatic engagement, the strategic support of stability operations and the effective deployment of economic development resources—so-called “soft power.” Rather than cut our international affairs budget (which is just 1% of the total federal budget), I believe Congress should enhance it. Promoting stability in regions that are susceptible to influence from the groups you reference can help combat poverty and the rise of actors which use despair to recruit desperate followers and build extremist or despotic regimes that threaten the United States and our interests.

- (3) As we are all well-aware, the Boston Marathon bombings in April were a tragic reminder that terrorist threats don't only emanate from abroad. In your opinion, how real is the threat of homegrown violent extremists? What must we do to prevent such attacks in the future?

Threats can emanate from anywhere. From home (as we have seen in Oklahoma City and Boston) or abroad (e.g. 9/11). While we cannot stop every attack, prevention, whenever possible, is critical. However, it is dependent on the development of intelligence and both horizontal and vertical information sharing.

Based on reports that I have read, local law enforcement leaders in Boston expressed frustration with a lack of information sharing by the FBI and federal agencies regarding the Tsarnaev brothers. This reinforces the previously mentioned need for congressional oversight to ensure consistent and effective horizontal (across the IC and relevant federal agencies) and vertical (state, local, and private sector) information sharing. Oversight should not come solely in reaction to an information sharing failure. Congress should regularly and proactively invite state and local law enforcement, fusion center directors as well as key private sector security representatives to testify about both shortcomings and successes related to vertical information sharing programs and protocols.

- (4) With regard to cybersecurity, from what I understand, NIST is doing a good job of organizing the framework laid out in the President's Executive Order. However, I believe we should refrain from codifying the Executive Order until it has shown to be

a smart and effective policy. Do you believe we should rush to codify the EO or should we let the framework process play out?

Digital threats can change and evolve instantaneously. We cannot legislate or regulate fast enough to keep up. I am concerned that prescriptive, regulatory approach will put both government and corporate compliance lawyers, rather than technical experts, in charge of cybersecurity. And we know that compliance does not equal security. If the majority of America's critical infrastructure is privately owned and operated, then the private sector must be viewed as security partners.

I agree with your assessment that it is best to let the framework play out before codifying it or any standards into as law. Last week NIST released the draft framework and it will be important to properly assess the feedback that is received from private industry. The draft framework has many worthy components to include its recognition of the role of the private sector in owning, operating and securing Critical Infrastructure, its call for a voluntary, risk-management approach that is prioritized and flexible. And it attempts to focus public and private sector organization leaders on areas of greatest concern. But it can be improved to better define objectives and desired outcomes. And more clarity is needed in terms of its discussion of privacy and civil liberty protection. No cyber framework will ever be perfect, but a collaborative public-private dialogue toward continuous improvement offers the best opportunity to make the nation more cyber secure.

- (5) With the current situation on-going in Syria, Bashar al Assad recently said that the U.S. should expect a response if the U.S. conducts a strike and all responses may not come from government. Given Assad's relationship with Hezbollah, I am interested in your assessment of the threat that Hezbollah could present to the homeland? What kind of reach do you assess that Hezbollah has in the United States? Do you believe that Hezbollah has sleeper cells in the U.S.? What is the likelihood that terrorists associated with Hezbollah could cross our borders in order to conduct attacks? Which border (northern or southern) is the more likely path of infiltration into our country?

Hezbollah's stretch, and as such Iran's growing influence, is very concerning. Hezbollah has shown that they are willing to carry their battle outside of their traditional strongholds. Technology (e.g. internet) provides the organization with the capability of propagating its philosophy and potentially its operations, regardless of political boundaries or borders. As for the presence of cells and path of potential attack, I must defer to the intelligence community.

That said, securing our borders in an intelligent manner is critical to ensure that the threat posed by those who seek to cause harm to us is averted. At the same time, our borders must remain open to commerce and help expedite

those who wish to lawfully enter our nation. I have always, and continue to, push for a smart and balanced approach to immigration reform. Border security and immigration reform are not mutually exclusive, both can be accomplished through a realistic risk management approach.

- (6) In a recent interview, Assad mentioned the attacks of September 11, 2001, and how no one expected such an attack. He clearly hinted that the U.S. should expect the unexpected. What homeland defense vulnerabilities remain that require the most attention from the federal government?

One of the greatest threats that we are still in great need of addressing is the cyber threat. While this threat has been clearly identified, there is still a great deal of political debate about what to do about cybersecurity concerns. Meanwhile, our companies are experiencing business disruptions, loss of data and the theft of intellectual property, and all impacting our nation's economy. We must ensure collaborative—rather than adversarial—relationships between government security and private sector critical infrastructure owner-operators if we are to effectively reduce related cyber risk. Information sharing is key to not only preventing attacks when possible, but to enabling recovery should attacks occur. This is vital to national resilience.