THE DEPARTMENT OF HOMELAND SECURITY: AN ASSESSMENT OF THE DEPARTMENT AND A ROADMAP FOR ITS FUTURE

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

SEPTEMBER 20, 2012

Serial No. 112–119

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

81–128 PDF WASHINGTON : 2013

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

CONTENTS

THE DEPARTMENT OF HOMELAND SECURITY: AN ASSESSMENT OF THE DEPARTMENT AND A ROADMAP FOR ITS FUTURE

Thursday, September 20, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:07 a.m., in Room 311, Cannon House Office Building, Hon. Peter T. King [Chairman of the committee] presiding.

Present: Representatives King, Lungren, Rogers, McCaul, Bilirakis, Miller, Walberg, Marino, Turner, Thompson, Jackson Lee, Cuellar, Richardson, Richmond, Clarke of Michigan, and Hahn.

Chairman KING. Okay. Good morning. The Committee on Homeland Security will come to order. The Ranking Member has been delayed, but he will be here. His staff has suggested that we start the hearing, since our witnesses are here.

The committee is meeting today to examine the current state of the Department of Homeland Security—oh, the Ranking Member is here, thank you—and the solution to the future. I will now recognize myself for an opening statement.

I want to thank each of the witnesses for being here today. I believe all of you have testified here before. Mr. Baker has done double duty, also, by being in the Department testifying and now coming back. He is also a noted author. Again, it is great to have all of you here today.

This, I think we always try to keep this committee as bipartisan as possible. But I would say that today's hearing will probably be the essence of bipartisanship because everyone on the committee wants the Department to succeed. All of us believe that progress has been made.

There are questions, of course, of where more progress can be made where there are still deficiencies. Each of you is an expert on the issues so we really look forward to your testimony. I know since September 11 we had four Islamist attacks or attempted attacks within the United States. In addition to that, there have been dozens of disrupted terrorist attacks against the homeland.

Just in the last 2 years alone we have had a series of them, including bomb plots against the Capitol Building. There was a young man arrested in Chicago last week. So this is an on-going threat against the United States. I think the fact that none of these attacks has succeeded is at least partially due to the efforts of the Department of Homeland Security and also how it fits into the

overall counterterrorism matrix that has been established since September 11.

Now, the current unrest in the Middle East involving radicals and affiliates of al-Qaeda further underscores how threats from that part of the world impact our counterterrorism efforts to prevent weapons of mass destruction from getting into the hands of those who want to kill Americans in the homeland.

Now, during the 112th Congress, this committee has examined a series of issues. Obviously, there was a lot of publicity and notoriety, or interest, in the hearings we had on the issue of radicalization in the Muslim-American community, steps to address the issue. But we also had a series of other hearings, including cybersecurity, hardening our critical infrastructure, protecting chemical facilities.

The operations of TSA, Chairman Rogers has been especially active on that. That is an area of particular concern to us on both sides of the aisle as far as making the TSA more efficient and also more effective. Also, what it can do to, again, improve its image. Not in the sense of image, but in gaining the confidence of the American people, which it has not been able to do.

Also, we have looked into issues regarding reforms to the Department—in its management, improve employee morale, cut red tape, save taxpayer dollars. Also emergency communications, the effective administration of Homeland Security grants, reduce our vulnerability to attacks on the homeland using IEDs such as the Times Square car bomb.

Also the whole issue of border security along the land and maritime borders. We look forward to building on this oversight. But this hearing today, and your testimony, can, I believe, help guide us in the right direction and provide a more coherent framework for us.

As we consider the road map for DHS, some of the questions we have is: How can the Department use scarce taxpayer dollars? Because unlike after 9/11, when basically the money that was felt was needed was given, the fact is that we do face budget restraints. I believe, in too many cases there has been too much money cut from the Department of Homeland Security.

Whether I like it or not or the Ranking Member likes it or not, for the foreseeable future that is the reality that DHS is going to have to face. Even if the cuts are not as severe in the future as they have been over the last several years, it is going to be a very, very tight, tight budget no matter what.

So how can the Department use the taxpayers' dollars more wisely? How effective are the Department's efforts to counter violent extremism? To what extent is DHS able to work with our allies overseas? To what extent have they become a player in the intelligence community, both here and overseas?

Also, just what recommendations that you believe the Department should make to strengthen the overall homeland security of the United States. Now, there has been progress made in a lot of areas. I am sure you are going to touch on that, and all sides can agree that there has been progress made. Certainly involving FEMA, involving strategic and operational plans, allocating fund-

ing based on risk, raising public awareness about the importance of reporting suspicious activity.

Yet there is so much more work to be done as far as integrating management functions, strengthening information technology and financial management, improving contracting and acquisition practices and controls, ultimately establishing a biometric exit screening system, securing the border using objective measures, enforcing penalties against immigration violators, exercising authority to secure chemical facilities, developing a risk-based approach to screening airline passengers, strategically managing risks and assessing program performance.

Also, I think one thing we all agree on is that Congress has to undertake its own reform. If we are going to be able to effectively oversee the Department of Homeland Security, we can't have this number of committees and subcommittees—depending on what number you want to use, it is in the eighties or nineties, it is more than 100 of committees, subcommittees—commissions, boards that the Department has to report to, often giving the same testimony, just to a different set of Members of Congress; some of whom are just interesting in getting their spot on the evening news on a committee that has, at best, tangential association with the Department of Homeland Security.

So that is really our burden and not yours. But any testimony you could give us to strengthen our case for both sides of the aisle would be greatly appreciated. So I want to thank all of you for being in here today. I look forward to your testimony. This will be, I assume, the last full committee hearing of the year; certainly until after the recess.

I want to thank the Ranking Member. We haven't always agreed, but I believe we have been able to work in a collegial way. I say, that is all Members on the committee. Considering the divisions that there have been in Congress over the past 2 years, while maybe everything isn't perfect on this committee I think we can say we have done, I think, as well if not better than almost any other committee in Congress in trying to find ways to work together.

So with that softball approach, I am recognizing the Ranking Member, the distinguished gentleman from Mississippi, for his opening statement.

Mr. THOMPSON. Thank you very much, Chairman King. I do agree with you on your last statement. We, I think, have set the bar for a lot of other committees on our ability to work. I look forward to continuing to work with you on that.

But there are differences, and I think from time to time those differences are reflected. But the greatness of this country is that people who differ can still come together for the common good. We do that. Again, thank you for holding this hearing.

In March 2003 the Federal Government stood up the Department of Homeland Security in response to the separate 2001 terrorist attack. Today, the Department of Homeland Security is the third-largest agency in the Federal Government, employing about 220,000 people and operating both domestically and internationally.

Prior to the September 2001, the United States used various approaches to handle catastrophic dangers, including National Guard involvement, law enforcement, and emergency management. But the events of 2001 forced us to begin a process aimed at the development of a cohesive homeland security policy.

Over the last 10 years, the concept of homeland security has evolved and expanded. While the need to address terrorism remains central to our understanding of homeland security, we now understand that homeland security must include other catastrophic incidents. We must remain concerned about the risks that may threaten the lives of our people.

But we cannot fail to recognize those things that may threaten the strength of our democracy, the vitality of our economy, as well as the continuation of public and private-sector activities that impact our daily lives. From critical infrastructure protection to cybersecurity, the evolution and expansion of our understanding of homeland security has required us to ask the Department about risk assessment, strategic development, and operational priorities.

From my vantage point, the ability to come to grips with these questions of risk strategy and operations has formed a core of the Department's struggles as well as form the basis for its successes. So as we begin to discuss the Department's road map to the future, we must acknowledge that its presence on GAO's high-risk list remains a continuing cause for concern.

The importance of the Department's high-risk designation, and its ability to implement its plans to resolve the transformation and integration issues that continue to hamper its development into a cohesive organizational unit, cannot be understated. For several years, I have noted the need to strengthen the ability of the under secretary for management to require and enforce uniform administrative practices and procedures through each component.

It seems to me that the lack of power in the management office will continue to permit ineffective and inconsistent practices in procurement and personnel throughout the components. We see the results of these inconsistencies each time we learn about wasted money. We read about the fallout of these inconsistent practices every year when a Department ends up near the bottom of OPM's annual survey of employee satisfaction.

So as we consider the road map forward, let us be sure to consider how the Department can achieve the mission, and improve its internal operations. The biggest challenge, however, is whether Congress will fully fund Homeland Security efforts as opposed to slashing the Homeland Security budget as proposed by the Majority.

While the threat to homeland security has not diminished, the Department of Homeland Security has been required to do more with less. The fiscal 2012 Homeland Security appropriations shortchanged homeland security from border security to aviation security, science, and technology. In particular, the management directorate and the budget environment for fiscal year 2013 has not changed.

In fact, it may have worsened. I would like to also say at this point that Congress hasn't been really helpful in some of these situations because we have not, when I was chair—and now Chair-

man King, since he is back—been able to convince our leadership that a consolidated jurisdiction for the Department of Homeland Security would be in the best interests of this country.

I think we still agree on that, right?

Chairman KING. Absolutely.

Mr. THOMPSON. Okay. Just checking. So I want to make sure that everybody understands that as long as jurisdiction is split the Department is tasked with responding to over 100 committees and subcommittees on this Hill. That is just too much. So I look forward to hearing from our witnesses on these and other issues as we discuss the path forward for the Department.

I yield back the balance of my time.

Chairman KING. I thank the Ranking Member for his statement and for yielding back. Also emphasize again that we stand as one on the whole issue of jurisdictional consolidation. It makes absolutely no sense, the current situation; absolutely none whatsoever.

As I mentioned before, we are pleased to have a distinguished panel of witnesses before us today on this vital topic. It is, again, a privilege to have you here today once again. Let me begin with Mr. Richard Skinner, who was the first Senate-confirmed inspector general of the Department of Homeland Security. He served in that capacity from 2008 to early 2011.

He has held managerial positions in various agencies throughout the Federal Government, including FEMA, the Department of Agriculture, the Department of Justice, the Department of Commerce and the State Department. In 1998, he received the President's meritorious executive rank award for superior accomplishment in management programs of the United States Government.

I would just say, as Chairman and as former Ranking Member, your testimony before our committee has always been extremely helpful. I think we would agree, totally nonpartisan and in the best interests of the country.

With that, the gentleman's recognized for 5 minutes.

Mr. THOMPSON. If the gentleman will yield, we agree on that, too.

[Laughter.]

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

Mr. SKINNER. Well, thank you very much and good morning, Chairman King and Ranking Member Thompson. It is good to see everyone again. It is truly an honor to be here today, and I really thank you very much for this opportunity.

Since its inception in 2003, the Department has worked to accomplish the largest reorganization of the Federal Government in more than a half a century. This task has presented many challenges. While it is making progress, the Department still has much to do to be a cohesive, efficient, and effective organization.

Today, I would like to talk about four often-overlooked management support functions that constitute the platform upon which the Department's programs must operate and are critical to the successful accomplishment of the Department's mission. That is financial management, IT management, acquisition management, and grants management.

Concerning financial management, in 2011 the Department was again unable to obtain an opinion on its financial statements. Numerous material internal control weaknesses were again reported. Although it has reduced the number of material weaknesses and has received a qualified audit opinion on its consolidated balance sheet and custodial activity, it is unlikely this progress will continue unless the Department modernizes its financial systems.

Due to 2012 budget reductions—and also it looks like in 2013, as well—recent modernization initiatives have been on hold indefinitely. It is not clear now when the Department will resume its modernization strategy, nor is it clear whether these initiatives, if and when they are ever implemented, will ensure that financial management systems can generate reliable, useful, timely information for day-to-day decision-making.

In the interim, the Department must continue to use archaic, unreliable systems to manage its financial resources. Also, the Department and its components are still struggling to upgrade and integrate their respective IT infrastructures. According to recent OIG reports as recent as this past July, program and field offices continue to develop information technology systems independently of the CIO, and have been slow to adopt the Department's standard information technology development approach.

As a result, critical systems are not integrated, do not meet user requirements, and do not provide the information technology capabilities that agency personnel and its external partners both in the Federal Government as well as the State and local levels need to carry out critical infrastructures in a timely, effective, and efficient manner.

With regard to acquisition management, Secretary Napolitano and her executive team have demonstrated a genuine commitment to improve the Department's acquisition management function. However, much work remains to be done. Most notably, the Department needs to identify and acquire the resources needed to fulfill its acquisition management responsibilities.

The urgency and complexity of the Department's mission will continue to demand rapid pursuit of major investments in high-risk, complex acquisition programs. To effectively manage these large-dollar procurements, the Department will need a sustained commitment, increased resources, and smarter processes to administer and oversee the contractors' work.

Finally, since its inception the Department has distributed over $18 billion through the Homeland Security Grant Program. Yet, according to an OIG report released earlier this year, the Department does not have a system in place to determine the extent that these funds enhance the State's capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

Consequently, the Department has been awarding Homeland Security Grant funds to States each year for on-going programs without knowing the accomplishments from prior years' fundings or the extent to which additional funds are needed to achieve desired results. Strategic planning, performance measurement, and oversight are essential management controls to ensure that grant funds are

used for their intended purpose and that enhancements in preparedness capabilities are being achieved.

Otherwise, it is impossible to determine whether annual investments are actually improving our Nation's homeland security posture. In today's economic climate, it is critical that the Department concentrate its limited resources on those threats that pose the greatest threat to the country.

In summary, it is evident that the Department's senior officials are well aware of these challenges and are attempting to remedy them. Yet they have actually made headway, Mr. Chairman, as you pointed out. The question is, however: 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 of those efforts, 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 necessary improvements.

Unless the Department and Congress stay focused on these challenges, it will be harder than ever to facilitate solutions to strengthen the Department's critical management support functions and, ultimately, to ensure the success of the Homeland Security mission.

Mr. Chairman, this concludes my prepared statement. I will be happy to answer any questions the committee may have.

[The prepared statement of Mr. Skinner follows:]

PREPARED STATEMENT OF RICHARD L. SKINNER

SEPTEMBER 20, 2012

Good afternoon, Chairman Rogers, Ranking Member Thompson, and Members of the committee. It is truly an honor to be here today to discuss what the Department of Homeland Security needs to do in the years ahead to become a more efficient organization. I thank you for this opportunity.

Since its inception in 2003, the Department has worked to accomplish the largest reorganization of the Federal Government in more than half a century. This task, 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 presented many challenges. While the Department has made progress over the past 9 years, it still has much to do to establish a cohesive, efficient, and effective organization.

The OIG's latest major management challenges report, dated November 10, 2011, continues to address a broad range of issues, including both program and administrative challenges. In total, the OIG identified nine categories of challenges: Financial Management, Information Technology Management, Acquisition Management, Grants Management, Emergency Management, Infrastructure Protection, Border Security, Transportation Security, and Trade Operations and Security. These are essentially the same management challenges that the the OIG reported as early as 2005. Today, I would like to talk about four of those management challenges:

- Financial management,
- Information technology management,
- Acquisition management, and
- Grants management.

These management support functions constitute the platform upon which the Department's programs must operate and are critical to the successful accomplishment of the Department's mission. Some of these challenges were inherited by the Department from the legacy agencies. Nevertheless, the complexity and urgency of the De-

partment's mission have hampered its efforts to make sustainable progress in implementing corrective actions.

Senior officials at the Department recognize the significance of these challenges and understand that addressing them will take a sustained and focused effort. They have, in fact, taken actions over the past several years to implement, transform, and strengthen the Department's management support functions; albeit, in my opinion, at a snail's pace.

FINANCIAL MANAGEMENT

Financial management has been and continues to be a major management challenge for the Department since its creation in 2003. In fiscal year 2011, the Department was again unable to obtain an opinion on its financial statements, and numerous material internal control weaknesses were again reported. These weaknesses, due to their materiality, are impediments to obtaining a clean opinion and providing positive assurance over internal controls at the Department level. 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 the Department modernizes its financial systems, it is unlikely this progress will continue.

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 fiscal year 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 it financial resources, which is unfortunate, particularly in this day and age of budget austerity and the public demand for increased fiscal transparency and accountability.

INFORMATION TECHNOLOGY MANAGEMENT

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.

Integrating the IT systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for effective communications and information exchange remains one of the Department's biggest challenges.

For example, on October 20, 2011, the Assistant IG for Emergency Management Oversight, Matt Jadacki, testified that FEMA's existing information technology systems do not effectively support disaster response activities. FEMA has 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.

According to Mr. Jadacki, there is not an adequate understanding of existing information technology resources and needs throughout the agency. Specifically, FEMA's Office of the Chief Information Officer (CIO) does not have a complete, documented inventory of systems to support disasters. Further, program and field offices continue to develop information technology systems independently of the CIO and have been slow to adopt the agency's standard information technology development approach. As a result, systems are not integrated, do not meet user requirements, and do not provide the information technology capabilities agency personnel

and its external partners need to carry out disaster response and recovery operations in a timely, effective, and efficient manner.

Furthermore, according to a report issued recently by GAO, FEMA does not have an effective system to manage flood insurance and claims data, although it invested roughly 7 years and $40 million on a new system whose development has been halted because it did not meet users' needs.

Most recently, on June 29, 2012, the Assistant IG for Information Technology Audits, Frank Deffer, reported that the information technology environment and the aging IT infrastructure within CBP does not fully support CBP's mission needs. According to Mr. Deffer, 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.

Similar problems also have been reported at the Coast Guard, Citizen and Immigration Services, Immigration and Customs Enforcement, 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 the counter-terrorist and emergency management information critical to ensuring homeland security remains an on-going 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.

ACQUISITION MANAGEMENT

DHS has taken notable action to implement, transform, and strengthen its acquisition management capabilities. During my tenure as the IG of the Department, the Secretary and Deputy Secretary of Homeland Security, and other senior officials demonstrated a genuine commitment to improve the Department's acquisition management function. In its December 2011 strategy for high-risk management, the Department presented detailed plans to address a number of acquisition management challenges. However, much work remains to fully implement these plans and address these challenges. Most notably, the Department needs to identify and acquire the resources needed to implement its acquisition policies.

OIG and GAO audits over the past 9 years have identified problems related 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' mission and objectives; operational requirements; and acquisition program baselines. Additionally, the OIG reported that only a small number of DHS' major acquisitions had validated cost estimates.

The urgency and complexity of the Department's mission will continue to demand rapid pursuit of major investment programs. Between fiscal years 2003 and 2010, the Department spent about 40 percent of its budget through contracts. Although that figure may have decreased over the past 2 years, the Department will continue to rely heavily on contractors to accomplish its multifaceted mission and will continue to pursue high-risk, complex acquisition programs.

The Department must have an infrastructure in place that enables it to effectively oversee the complex and large-dollar procurements critically important to achieving its mission.

Both the OIG and the GAO have reported that the Office of the Chief Procurement Officer needs more staff and authority to carry out its general oversight responsibilities. The GAO recommended that the Department provide the Office of the Chief Procurement Officer sufficient resources and enforcement authority to enable effective, Department-wide oversight of acquisition policies and procedures. The OIG made a similar recommendation.

Common Themes in Audits of Department Contracts

Over the past several years, the OIG and GAO conducted numerous audits of individual Department contracts, such as TSA's information technology services, CBP's SBInet program, the Coast Guard's Deepwater program, and FEMA contracting. Common themes and risks emerged from these audits, primarily poor planning, the dominant influence of expediency, poorly-defined requirements, and inadequate oversight that contributed to ineffective or inefficient results and increased costs. To ensure that its acquisition programs are successful, the Department must lay the foundation to oversee and assess contractor performance, and control costs and schedules. This requires a sustained commitment, increased resources, and smarter processes to administer and oversee the contractors' work.

FEMA Procurements

The Assistant IG for Emergency Management Oversight, Matt Jadacki, testified on October 20, 2011 that FEMA has developed and strengthened acquisition management policies and processes, but it continues to face challenges. For example, weak internal controls have resulted in multi-million dollar contracts with vague and questionable requirements and no performance measures. Agency employees responsible for managing and monitoring the contractors do not always receive written guidance or training on how to evaluate contractor performance or certify billing invoices. Continued improvements are needed in FEMA's oversight of contracts.

During my tenure as the IG, my office issued several reports recommending improvements to FEMA's acquisition processes. Those recommendations have resulted in policies and procedures on contract closeout, transferring contract files from one contracting officer to another, and labeling and organizing contract files so all contract actions are properly documented.

In fiscal year 2010, FEMA deployed Disaster Assistance Employees to accelerate contract closeout efforts for the Disaster Relief Fund, de-obligating $1.2 billion. These contract closeout efforts continue annually and are in direct response to an OIG recommendation. I was pleased to learn that FEMA has created Disaster Acquisition Response Teams, whose focus on contract administration and oversight of large disaster contracts is much needed. My office also reported FEMA's need for an overarching sourcing strategy. Headquarters, regional, and local FEMA representatives were ordering goods without communicating with their counterparts at other locations. This resulted in goods ordered that were not needed, purchased from the wrong source, or at the wrong time. My former office recommended that FEMA adopt the single-point ordering concept, to coordinate all sourcing decisions through the Logistics Section. As a result of this recommendation, FEMA piloted the single-point ordering concept during its response to Hurricane Irene.

Strategic Sourcing

The Department can improve management of its strategic sourcing. In March 2011, the OIG reported that the Department did not have a logistics process in place to facilitate strategic sourcing of detection equipment. Strategic sourcing would require that management standardize equipment purchases for explosive, metal, and radiation detection equipment; identify common mission requirements among components; and develop standard data elements for managing the inventory accounts

of detection equipment. Improving its management of detection equipment will offer the Department opportunities to streamline the acquisition process and improve efficiencies.

Acquisition Workforce

DHS made progress in the recruitment and retention of a workforce capable of managing a complex acquisition program. 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 seeks to develop acquisition leaders, increased 62 percent from 2008 to 2010. Nevertheless, DHS continues to face workforce challenges across the Department. For example, according to GAO, the Coast Guard reduced its acquisition workforce vacancies from approximately 20 percent to 13 percent, and had filled 832 of its 951 acquisition positions as of November 2010. Although acquisition workforce vacancies have decreased, program managers have on-going concerns about staffing program offices. Also, according to its August 2010 human-capital staffing study, program managers reported concerns with staffing adequacy in program management and technical areas. To make up for shortfalls in hiring systems engineers and other acquisition workforce positions for its major programs, the Coast Guard must use contractors.

Likewise, according to the OIG's Major Management Challenges report, dated November 2011, acquisition staff turnover in FEMA has exacerbated file maintenance problems and resulted in multimillion-dollar contracts not being managed effectively or consistently. One of FEMA's challenges is hiring experienced contracting officers to work disaster operations. The majority of FEMA staff at a disaster site work on an on-call, intermittent basis, and, oftentimes, they lack the training and experience to manage large disaster response and recovery contracts.

FEMA also has made great strides in improving its contracting officer's technical representative (COTR) cadre. FEMA has designated staff to oversee the COTR program; developed a tiered system which ties training requirements to dollar values of contracts a COTR can monitor; and established an intranet site containing tools for COTR use. However, many trained COTRs have never been assigned a contract and are unsure of their ability to be effective. And, although they represent the contracting officer, the COTRs' appraisals are completed by their supervisors in the program offices for which they work, rather than the applicable contracting officer, thus leading to divided loyalties.

Finally, the Department has not fully planned for or acquired the workforce needed to implement its acquisition oversight policies. According to a GAO report issued in February 2011, the Department needs to continue its efforts to: (1) Identify and acquire resources needed to achieve key actions and outcomes; (2) implement a program to independently monitor and validate corrective measures; and (3) show measurable, sustainable progress in implementing corrective actions and achieving key outcomes. The Department needs to demonstrate sustained progress in all of these areas to strengthen and integrate the acquisition management functions throughout the Department.

Knowledge Management and Information Systems

According to the OIG's annual Major Management Challenges report, the Department has made progress in deploying an enterprise acquisition information system and tracking key acquisition data. The Department's acquisition reporting system of record, known as nPRS (next-Generation Periodic Reporting System), tracks components' major acquisition investments. It also has capabilities to store key acquisition documents, earned value management information, and risk identification. Component personnel are responsible for entering and updating information, which includes cost, budget, performance, and schedule data. However, components did not complete and report all key information in nPRS. The OIG reported that only 7 of 17 programs (41%) reported Acquisition Program Baseline required milestones. These milestones establish the acquisition cost, schedule, and performance values. Only 13 (76%) programs reviewed contained required key documentation such as mission needs statements, acquisition plans, operational requirements documents, and integrated logistics support plans.

In addition, the Department reported in its December 2011 strategy for high-risk management that senior executives are not confident enough in the data to use the Department's Decision Support Tool which was developed to help make acquisition decisions, address problems meeting cost or schedule goals, and prepare for program review meetings.

Although the Department continues to make progress in improving its acquisition management, it remains a significant challenge, in part because of the magnitude of the number, dollar value, and complexity of its acquisition activity.

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 years 2010 and 2011, the OIG's audits of 105 disaster grants identified $365 million in questionable cost 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 20 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

During fiscal years 2002 through 2011, FEMA distributed over $18 billion through the Homeland Security Grant Program. According to an OIG report released this past July, FEMA does not have a system in place to determine the extent that Homeland Security Grant Program funds enhanced the States' capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Also, FEMA 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, FEMA does not know whether prior year milestones for the projects have been completed. FEMA also does not know the amount of funding required to achieve needed preparedness and response capabilities.

Furthermore, according to the OIG's annual Major Management Challenges report, dated November 2011, FEMA continues to face challenges in mitigating redundancy and duplication among preparedness grant programs, including barriers at the legislative, departmental, and State levels. The preparedness grant application process is ineffective because FEMA does not compare and coordinate grant applications across preparedness programs. Since grant programs may have overlapping goals or activities, FEMA risks funding potentially duplicative or redundant projects.

Public Law 110–53, Implementing Recommendations of the 9/11 Commission Act of 2007, required 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, on March 20, 2012, the assistant inspector general for audits testified that FEMA needs to make improvements in strategic management, performance measurement, and oversight. According to Ms. Richards, FEMA needs to improve its guidance on strategic plans for State Homeland Security Grants. While current guidance for State Homeland Security strategic plans encourages revisions every 2 years, the language is such that it does not require revisions to be made—it is just strongly encouraged. Consequently, many States have outdated strategic plans, and many do not have Homeland Security strategic 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, States have no assurance of the level of effectiveness of their preparedness and response capabilities. Also, States are less capable of determining progress toward goals and objectives when making funding and management decisions. The OIG reported deficiencies in strategic planning in 15 of the 20 State audits completed as of March 2012.

In regard to performance measurement, Ms. Richards said that FEMA needs to improve its guidance on establishing metrics and measuring performance. The OIG continues to report that many States have not received proper guidance and, consequently, have not adequately documented or tracked their progress and performance. Providing guidance on the appropriate metrics and requiring those metrics to be documented would provide the States with tools to help them understand the effectiveness of each grant program. FEMA also needs to strengthen its guidance on reporting progress in achieving milestones as part of the States' annual program justifications. Because of insufficient information on milestones and program accomplishments, FEMA has been annually awarding Homeland Security Grant Program funds to States for on-going programs without knowing the accomplishments from prior years' funding or the extent to which additional funds are needed to achieve

desired capabilities. Tracking accomplishments and milestones are critical elements in making prudent management decisions because of the evolving, dynamic changes that can occur between years or during a grant's period of performance. OIG audits reported problems with performance measurement in 19 of 20 State audits completed as of March 2012.

Finally, Ms. Richards said that FEMA needs to improve its oversight to ensure the States are meeting their reporting obligations in a timely manner to ensure FEMA has the information it needs to make program decisions and oversee program achievements. Further, FEMA needs to improve its oversight to ensure that States are complying with Federal regulations in regard to procurements and safeguarding of assets acquired with Federal funds. In its annual audits of the State Homeland Security Program, the OIG repeatedly found weaknesses in the States' oversight of grant activities. Those weaknesses include inaccuracies and untimely submissions of financial status reports; untimely allocation and obligation of grant funds; and not following Federal procurement, property, and inventory requirements. Delays in the submission of Financial Status Reports hampers FEMA's ability to effectively and efficiently monitor program expenditures and prevents the State from drawing down funds in a timely manner, ultimately affecting the effectiveness of the program.

Strategic planning, performance measurement, and oversight are important management controls for FEMA 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 actually improving our Nation's homeland security posture. Furthermore, without clear, meaningful performance standards, FEMA lacks the tools necessary to make informed funding decisions. In today's economic climate, it is critical that FEMA concentrate its limited resources on those threats that pose the greatest risk to the country.

While some aspects of the Department's management support challenges were inherited from the Department's legacy agencies, the complexity and urgency of the Department's mission has oftentimes exacerbated the Department's ability to address them in a disciplined and effective manner.

It is evident that the Department's senior officials are well aware of these challenges and are attempting to remedy them, and they have actually made some headway. The question is, however: 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.

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.

Chairman KING. Thank you very much, Mr. Skinner, for your testimony.

Our next witness, Stewart Baker, is a partner in the law office of Steptoe & Johnson here in Washington, DC. I first met Mr. Baker when he was the first assistant secretary for policy at the Department of Homeland Security. In that role, he led a staff of 250 people and was responsible for the Department-wide policy analysis as well as the Department's affairs, strategic planning, and relationships with law enforcement and public advisory committees.

Other than that, he had nothing to do. It was a 48-hour-a-day job, and Secretary Baker did an outstanding job. He was named the top lawyer in international security by *Washingtonian* magazine in 2011, and is an exceptionally distinguished attorney and public servant.

I am privileged to recognize Secretary Baker for 5 minutes.

STATEMENT OF STEWART A. BAKER, FORMER ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY

Mr. BAKER. Thank you, Chairman King, Ranking Member Thompson. It is a pleasure to be back here. I have almost recovered from my time in Government. You have seen my prepared testimony. What I thought I would do is just touch on three areas where the Department has big challenges, and actually challenge myself to give the Department a grade. So I will give the Department a grade on these things.

On the question of unity, coordination, making the Department work as a whole, I think a C-minus is the best the Department can get. It gets that because we have had three strong Secretaries in a row who will not be denied when they are paying attention, the components, the Department act more or less as a whole. But the spotlight of Secretarial attention is not the only place that coordination has to take place.

Outside that spotlight, we are not seeing the coordination that is necessary. Probably more important in times of tough budgets than any other because we can no longer afford duplication of effort or initiatives that may meet a particular component's priorities but don't fit into the overall National priorities that the Secretary is setting.

I think Ranking Member Thompson pointed out how important it is that we have a cohesive Department. I couldn't agree more, and we are not there and not even close. As I think the Chairman pointed out, having 100 oversight committees means there is one committee in each body that actually wants a single policy to come out of the Department.

Everybody else sees that the Secretary and the Secretary's priorities as potentially getting in the way of their ability to oversee some component of the Department. So having reform of jurisdiction is absolutely essential if you are going to get that grade above a gentleman's C-minus.

Let me turn to something where I think the story is very good, in contrast, and where I would give the Department an A. That is in carrying out the vision of the Homeland Security Act, of thinking seriously about keeping terrorists from crossing our borders. That used to be spread among three or four different agencies, and none of them thought that was their most important mission.

Putting all of those authorities in one place has led to a transformation of the way we think about border security. The way we have transformed that is in getting more data about the people who are coming across the border—whether it is the ESTA or PNR or the overseas interviews that Customs and Border Protection does, or for the first time—we actually know whether the people who are coming from other countries are criminals or not, something we never knew.

None of that would have happened because all of it came with a privacy resistance, an international resistance that three Secretaries in a row have stood up to, to build a much clearer sense of who is coming across our borders so we focus our attention on the

riskiest travelers. Chairman King, you mentioned all of the domestic attacks, many of them thwarted.

What is little covered—although I think this committee knows it quite well—is that in practically every one of those CBP, thanks to its data programs, knew something about, and contributed to the thwarting of, those attacks, or the apprehension of the attackers. That is a complete change from where we were when the Homeland Security Act was passed.

Finally, let me turn to someplace where I would give the Department, I guess, a B-plus for defending its turf but a D-plus for actually making us safer. That is in cyber. We are not safer than we were when the Homeland Security Act was passed. Things have gotten worse there.

We need to be doing much more. I believe that more regulatory authority is necessary. Certainly the Department needs a better relationship with NSA than they have today. But I think even without taking on the regulatory issue, there are ways to work with the private sector to build a better information-sharing system than we currently have without having to go back and change some of the privacy laws that have made it hard to do that.

By opening up the resources of the private sector to actually fund more investigations. I won't dwell on that, but I think the Department, if they are serious about this, can make a big difference in cyber. But they are going to need to improve their workforce substantially.

Thank you.

[The prepared statement of Mr. Baker follows:]

PREPARED STATEMENT OF STEWART A. BAKER

SEPTEMBER 20, 2012

Thank you, Chairman King, Ranking Member Thompson, and distinguished Members of the committee, for this opportunity to testify on the state of the Department of Homeland Security.

This is a timely hearing. We are approaching the tenth anniversary of the Homeland Security Act that created the Department. It's time to ask what the Department has done well, where it has failed, and how it can do better in the future.

WHERE DHS STILL FALLS SHORT

I will cut to the chase. The Department's biggest unmet challenge is making sure that its components are working together to the same goal. This was a central objective of the Homeland Security Act. It combined many agencies into a single Department so that all of them would use their authorities cooperatively in the fight against terrorists.

That may seem obvious, but this is Washington, and doing the obvious is not easy. The coordination efforts of a 10-year-old Department do not always impress component agencies that can trace their origins to the founding of the Republic.

The good news of the last 10 years is that the Department has had three Secretaries who had no doubt about who was running the Department and who insisted on the cooperation of all parts of the Department to implement their highest priorities. The bad news is that, in my view, these accomplishments owe more to the Secretaries' personalities than to the institutions they have built. In general, the offices that support the Secretary, from the various management offices to the office of policy, have not created a framework that can coordinate the big, proud components of DHS on issues that are outside the spotlight of Secretarial attention.

The need to strengthen those institutions is especially pressing now. We face a possible change of leadership at DHS no matter who wins the next election. And the Department faces a difficult budget outlook. Even in a time of record deficits, DHS's budget has hit a ceiling. There is almost no prospect of overall budget increases in the future, and cuts are likely. Budget decisions simply must be based

on how each component's expenditures fit the Department's highest priorities. The Department will have to identify redundancies and may have to eliminate programs with 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.

THREE CASE STUDIES

That, of course, is a very general evaluation. Let me be more specific about several important DHS initiatives.

1. Data-based security screening

One of the Department's unquestionable successes is 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 other priorities. DHS realized early that it couldn't spend even 5 minutes with every traveler who was crossing the border. Instead, it had to concentrate on the riskiest travelers, and to do that it needed more information about travelers, as far in advance as possible. As with so much at the Department, this has been a bipartisan priority; Secretary Napolitano has preserved and improved many data programs launched under earlier Secretaries. And DHS's data programs have contributed to the identification and apprehension of several travelers seeking to commit acts of terror on U.S. soil in recent years.

This initiative has been a great success—one that could not have been achieved without the Department. The use of travel reservation ("PNR") data to screen travelers has come under constant attack on bogus privacy grounds from the European Union, which has torn up its earlier agreement to honor the program every time a new Secretary has been sworn in. Every time, the new Secretary has insisted on maintaining the program.

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, every participating country other than Japan has a "PCSC" agreement with the United States, that will provide access to travelers' criminal records. The Department has also implemented ESTA, a "reservation" system that allows the Department to screen VWP travelers for potential risk before they begin their trips.

The Department has further expanded available information by launching Global Entry, which speeds clearance at the border for travelers who have been vetted in advance. Going forward, it will have background information on frequent travelers from a number of foreign partners, including the Netherlands, South Korea, Germany, Australia, and Brazil. As a result, DHS can focus more resources on riskier travelers.

Finally, DHS has begun gathering more data in foreign airports, successfully posting U.S. Government officers there to interview and in some cases to pre-clear travelers, a security enhancement that benefits both the individual traveler and the host government.

These data programs have improved the efficiency of border screening while also speeding most travelers across the border more quickly. Despite the hostility of privacy campaigners, 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.

That does not mean that it is perfect. In my view, our international negotiation strategy needs a coherent plan, with priorities, to make sure we get the most important information about the riskiest travelers at least cost to the United States. I also fear that our last PNR agreement accepted too many of Europe's limitations on PNR while surrendering too many protections for the program. And I'm disappointed that we have not persuaded Japan to supply information about the yakuza, or professional criminals, who may be traveling to the United States. 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. Everyone likes to criticize TSA, and one of the most valid criticisms is that it treats all of us like suspected terrorists. What's less known is that this treatment was more or less mandated by privacy campaigners, who persuaded Congress that TSA could not be trusted with the same travel reservation data that our border officials use every day. Lacking any information about travelers, TSA had no choice but to treat them all alike.

Now that the use of data for screening at the border has proven itself, the dam is beginning to break for TSA as well. TSA now has access to each traveler's name, gender, and date of birth. Increasingly, it also knows about the traveler's travel history, based on the voluntary provision of frequent flier data. It has shown how this data allows risk-based variations in screening, using date of birth to reduce screening hassles for children under 12 and seniors over 75. And overseas, in response to the Christmas day bomb attempt, CBP and TSA are combining forces to do data-based screening of passengers on U.S.-bound foreign flights. Finally, TSA is using Global Entry and other data to create a known traveler screening process for domestic flights.

This is all great progress, though more is needed. In the next 5 years, TSA should expand its use of data-based screening further, expediting travel for the great majority while demonstrating that it can be trusted with personal data. Because of past privacy limitations, it is likely that TSA will need Congressional assistance to achieve this goal.

2. CYBERSECURITY

Sometimes it's easier to persuade the team to give you the ball than to actually run with it. That is DHS's problem in cybersecurity right now.

DHS seems to have successfully fended off the many agencies and committees that wanted to seize parts of its cybersecurity mission. Whether DHS can carry out the mission, though, remains uncertain.

Although the Homeland Security Act clearly gave DHS authority over civilian cybersecurity issues, it did not give DHS the kind of trained personnel it needed. 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. With the exception of a handful of officials, DHS has not yet built a cadre of employees who can match their counterparts at NSA or Goldman Sachs. This is critical. If DHS fails in personnel, it will likely fail in the rest of its cybersecurity-related activities.

There are other challenges for DHS in cybersecurity. They include:

- *Building a better relationship with NSA*.—The outlines of a working relationship with NSA are obvious. DHS should provide policy guidance based in law and prudence for any cybersecurity mission affecting the civilian sector, but it must rely heavily on NSA's technical and operational expertise. 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 legislative authority to cajole and convene the private sector in the name of cybersecurity. It's been doing that for 10 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. That is one reason that DHS needs at least some authority to demand that industry respond to the cybersecurity threat, especially where it poses risks to civilian life that are not adequately recognized by the market. 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. That's a reason to be cautious about how Government approaches the private sector. But it's not a reason for Government to ignore the risk of a cybersecurity meltdown. It's worth remembering that, for a couple of decades, we were told that the financial derivatives trade was too complex for traditional Government regulation and a major driver of economic growth, and that the private sector could do a better job of internalizing risk than any Government regulator. We should not wait for the cybersecurity equivalent of the financial meltdown to give DHS a larger role in cybersecurity standards.

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. Most of the soft quasi-regulatory provisions that business groups rejected in talks with the Senate will likely be incorporated into an Executive Order that they will have little ability to influence. Even worse from their point of view, the pressure for legislation is likely to continue—and will become irresistible if we suffer a serious infrastructure failure

as a result of hacking. In that event, the cybersecurity legislation that Congress adopts will have to go beyond the Executive Order and into the territory of much tougher regulation. By failing to adopt more limited legislation now, Congress is sowing the seeds for more aggressive regulation in the future.

Moving beyond the fight over "regulation".—That said, DHS cannot wait for a National consensus on its regulatory role. There are many other steps that DHS could take to improve cybersecurity without touching the regulatory third rail. Let me outline a few of them here:

- *Information-sharing*.—It should be obvious why the targets of cyber attacks need to share information. We can greatly reduce the effectiveness of those 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. It must be automated and must occur at the speed of light, not at the speed of lawyers or bureaucrats.

  I supported 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 going to be blocked for a time by privacy objections, as seems likely, we need to ask a different question: Can the automated information-sharing system that we need be built without rewriting those aging privacy laws? I believe that it can; we simply need a more creative and determined approach to the law. Administration lawyers, who have taken an unnecessarily rigid view of existing law, should be sent back to find ways to build automated information sharing under existing law.
- *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 thicker and thicker defenses to protect ourselves. The obvious alternative is to identify the attackers and to find ways to punish them. But many information security experts have grown skeptical of this alternative. As they point out, retribution depends on attribution, and attribution is difficult; attackers can hop from country to country and from server to server to protect their identities.

  That skepticism is outmoded, however. Investigators no longer need to trace each hop the hackers take. Instead, they can find other ways to compromise and then identify the attackers, either by penetrating hacker networks directly or by observing their behavior on compromised systems and finding behavioral patterns that uniquely identify the attackers. It is harder and harder for anyone to function in cyberspace without dropping bits of identifying data here and there. If our security is inherently flawed, so too is the security of our attackers. This means that it is realistic to put attribution at the center of our response to cyberattacks.

  We should take the offense, surrounding and breaking into hacker networks to gather 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. DHS's intelligence analysis arm should be issuing more such reports and fewer bland generalities about terrorism risks for local law enforcement agencies.
- *Use DHS law enforcement authorities more effectively*.—Law enforcement agencies have a vital role to play in cybersecurity—even when the prospect of actually arresting the attacker is remote. Law enforcement agencies have investigative authorities, including search warrants and wiretaps, that can help identify attackers. Those authorities should be used strategically to aid in the overall attribution effort.

  The best way to achieve that goal is for DHS's cybersecurity office to be fully coordinated with law enforcement agencies that have criminal investigative authorities. By pooling information, authorities, and resources, these agencies should pursue a common strategy—one that identifies the bad guys, first to disable their attacks and eventually to bring them to justice. Coordination between DHS and the FBI may have its challenges, but today it seems that there is only modest coordination even between DHS's cybersecurity office and its own cybercrime investigators. Certainly I have seen no sign that ICE and Secret Service investigations are prioritized strategically based on guidance from the DHS cybersecurity office. The result is wasted opportunities and wasted resources. Instead, ICE and Secret Service cybercrime investigators should be de-

tached to a task force ran by the cybersecurity office as a way of dramatizing the need for an all-of-DHS approach to the problem.

Law enforcement authorities create a second opportunity that we are not fully exploiting. Increasingly, it is law enforcement that tells businesses they have been compromised. But usually the first question from businesses is one best directed towards the cyber defenders rather than the cyber cops: "What can we do to get the attacker out?" 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. Currently, however, DHS's cybersecurity office and its cybercrime investigators do not present themselves as a unified team when visiting the victims of attacks. Better coordination within the Department would pay dividends and provide a model for coordination across Department lines.

- *Recruit private-sector resources to the fight*.—In my private practice, I advise a fair number of companies who are fighting on-going intrusions at a cost of $50 or $100 thousand a week. The money they are spending is going almost entirely to defensive measures. 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's a treadmill. Like me, these companies see only one way off the treadmill: To track the attackers, figure out who the attackers are and where they're selling the information, and then sanction the attackers and their customers. When private companies' cybersecurity executives were surveyed recently, "more than half thought their companies would be well served by the ability to 'strike back' against their attackers." W. Fallon, Winning Cyber Battles Without Fighting, Time (Aug, 27, 2012). And the FBI's top cybersecurity lawyer just this week called our current strategy a "failed approach" and urged that the Government enable hacking victims "to detect who's penetrating their systems and to take more aggressive action to defend themselves." *Washington Post* (Sep. 17, 2012).

  He's right. But under Federal law, there are grave doubts about how far a company can go in hacking the hackers. I happen to think that some of those doubts are not well-founded, 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 D.C. 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 crimes that have a higher priority.

  In my view, that's a mistake. The Department, drawing on the resources of the entire Government, should do some full-bore criminal and intelligence investigations of private-sector intrusions, especially those that appear to be state-sponsored. We can identify the attackers, and we can make them pay.

  But if we want do that at scale, we have to let the victims participate in, and pay for, investigations that the Government will never have the resources to pursue. Too many Government officials have viewed such 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 finds himself 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 or of vigilante justice. Every one allows the victim to supplement law enforcement while preserving social control and oversight.

  DHS could probably experiment with that solution tomorrow if it chose, as could the FBI. Its law enforcement agencies often have probable cause for a search warrant or even a wiretap order aimed at cyber intruders. I know of no legal barrier to obtaining such an order, then relying on a private contractor paid by the victims to actually carry out the search or the tap, as long as that happens under Government supervision. (The Antideficiency Act, which arguably prohibits the Government from accepting 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 unleashed the creativity and resources of the private sector that attackers are victimizing?

Mr. Chairman, that concludes my prepared testimony. I will be pleased to answer any questions the committee may have.

Chairman KING. Thank you, Secretary Baker.

Our next witness, Frank Cilluffo, is associate vice president at George Washington University, where he directs the Homeland Security Policy Institute. I have had the privilege of being out there. You know, it is accurate to say that Mr. Cilluffo was present at the creation.

Shortly after the 9/11 attacks, Mr. Cilluffo was appointed by the President to the Office of Homeland Security, and served as the principle advisor to Governor Tom Ridge. Prior to his White House appointment, Mr. Cilluffo served in policy positions at the Center for Strategic and International Studies.

His work has been widely published in academic, law, business, and policy journals, as well as magazines and newspapers around the world. Without giving away too much, I can tell you often, before we prepare our committee agenda or look into topics we are going to cover, we look at what you have been saying on it lately. We certainly appreciate your wisdom and input.

With that, Mr. Cilluffo, I am privileged to recognize you for 5 minutes.

STATEMENT OF FRANK J. CILLUFFO, FORMER PRINCIPAL ADVISORY TO GOVERNOR TOM RIDGE, WHITE HOUSE OFFICE OF HOMELAND SECURITY

Mr. CILLUFFO. Thank you, Mr. Chairman. Thank you for the opportunity to appear before you today. Mr. Thompson, good to see you again, as well. Let me also, before jumping in—and I was asked to talk on the threat-related issues—thank you for your leadership in this committee. I mean, you really have taken on the hard issues facing this country.

I think you have tackled them head-on. Not an easy set of issues. I will be very brief, not my strong suit as I have never had an unspoken thought. But what I thought I would do is touch on some of the counterterrorism issues that we see and the current terrorism threat, as well as some of the cyber challenges where I am very much in agreement with Stewart's prognosis.

Firstly, as the recent terrorist attack in Benghazi clearly demonstrated, as well as unrest not only the Middle East, in North Africa, but also in Southeast Asia, there is no time to be lulled into a sense of complacency. A set of issues that I think a lot of people have been.

Yes, we have had a number of successful counterterrorism events of late. Most notably, the successful strike against Osama bin-Laden, Anwar al-Awlaki, Ilyas Kashmiri, probably the most dangerous unknown terrorist out there. But by no means does this mean that ding-dong, the witch is dead.

Unfortunately, what we have seen is the threat metastasize. It has morphed. Today, it comes in various shapes, sizes, flavors, and forms, ranging from al-Qaeda senior leadership, still operating out of the Fatah as well as its affiliates, most notably al-Qaeda in the Arabian Peninsula; home to probably the world's most dangerous

bomb maker, in Ibrahim al-Asiri, to al-Qaeda and the Islamic Maghreb, which is growing leaps and bounds not only across the Maghreb but also throughout the Sahel, as well as like-minded jihadi organizations in the African continent as a whole.

Ansar al-Dine in Mali, you are seeing Mauritania being taken over by Islamist groups, all the way through to the Horn of Africa, with Al Shabaab in Somalia. So the prognosis is not very good. Actually, if you have seen the way it has spread, I am not sure that some of our traditional counterterrorism instruments are the most appropriate right now.

Moreover, the reason you have seen some success in the Fatah is because we have—think of it as—suppressive fire. It is based on our successful counterterrorism initiatives. If we ease off that gas pedal, don't think that that vacuum isn't going to be instantaneously filled not only by al-Qaeda, but other like-minded individuals.

Bottom line here is, is the more time they are looking over their shoulder the less time they are plotting, training, and executing attacks. So I just warn the Congress to be able to support some of our counterterrorism measures. African continent, I can get into that in greater depth later.

But you literally are seeing swaths; the entire Maghreb, northwest Africa, all the way through from Mauritania to the Horn of Africa, in Somalia. These are areas where you are seeing Jihadi groups take advantage of under- and un-governed spaces. Why any of these regions? Because they are un-governed spaces.

I would also note that you have seen the homegrown threat in the United States. This is not an insignificant set of issues. We have had 58 cases, 58 plots, that have been prevented since 9/11. Some of those very significant. In New York City, for example, Naji Bolazazi. That was a very significant plot.

That was blinking red as red could be red. Faisal Shahzad, also a very significant plot. So as much as we can lean forward and support our State and local law enforcement authorities, I think we need to be able to do so very quickly on cyber. I think it is fair to say that our cyber community is where homeland and counterterrorism community was shortly after 9/11.

We have a lot to do. Long on nouns, short on verbs. We have been talking about it, but we are not actually addressing some of the most significant issues. To rack and stack the threat, you have got countries that are integrating computer network attack and computer network exploit into their warfighting capabilities.

Russia, China, at the top of the list. But also, you have countries like North Korea, Iran, who are increasingly becoming a terrorist threat. Their proxies, Hezbollah, are of great concern. What they lack in capability they more than make up for in intent. In the cyber domain, you can buy capabilities.

Intent and cash can take you a long way, something I think we need to be thinking about. Finally, in terms of recommendations—and I will be very quick here—one policy recommendation. The biggest, biggest missing dimension of our counterterrorism statecraft thus far, in my eyes, has been, "It is the ideology." To paraphrase Bill Clinton, it is not, "the economy, stupid," but, in this case, "the ideology, stupid."

We have got to get a comprehensive approach that exposes the hypocrisy of the jihadists and ultimately helps facilitate it fall under its own weight. Think of negative political campaigning. We need to do more in this respect. We also need to start focusing on the victims, not only the perpetrators.

Ultimately, to me, this is where we have an awful lot we should and can do beyond the traditional battlefields. Second, a structural one. That Department of Homeland Security, I would argue, needs an office of net assessment; someone who is not fettered by day-to-day intelligence needs, not fettered by day-to-day policy needs, but has the ability to step back, think big, ask the what-ifs, look for the game-changers.

That doesn't currently exist because everyone is running out of their inboxes daily. A very tactical one, NPPD as well as intelligence and analysis at DHS. I think they have a very unique thing that they can bring to the counterterrorism fight. That is, coming up with new intelligence products that are very oriented around critical infrastructures.

No one else in the intelligence community has that capability. We need to make that a reality. Information sharing, we have got to move at least the CISPA bill that Mr. Rogers and others had proposed, if you ask me. Is it enough? Probably not. But at the very least, we need to move on those measures.

Finally, in the cyber domain we are never going to firewall our way out of the problem. At the end of the day, the initiative stands with the offender, on the offense. So we have got to clearly articulate a cyber deterrent strategy, one that is actor-specific. Because right now, we are lumping China and Russia with a kid operating out of his basement, drinking a lot of Jolt Cola or whatever they drink nowadays.

But at the end of the day we need to get to the point where we can actually have a clearly articulated cyber deterrent strategy, and one that we are willing to act when red lines are crossed.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Cilluffo follows:]

STATEMENT OF FRANK J. CILLUFFO

SEPTEMBER 20, 2012

Chairman King, Ranking Member Thompson, and distinguished Members of the committee, thank you for the opportunity to testify before you today. Throughout your tenure as Chairman of this committee, Congressman King, you have consistently taken on the hard issues facing our country, and have committed to addressing them. Thank you for your leadership. Turning to the timing and subject of today's hearing both are well-selected. As recent events from the Middle East and North Africa through to Southeast Asia regrettably illustrate, violent extremism continues to thrive. With the United States and its interests still in the cross-hairs of jihadi and Islamist militants across the globe, the present moment is sadly opportune to assess the activities of the Department of Homeland Security (DHS) and give careful consideration to a roadmap for its future. Despite significant progress, especially on the counterterrorism front, the existing and projected threat climate is such that continued vigilance and a robust as well as proactive posture is needed—not only at DHS but throughout Government, at all levels, and supported by approaches that effectively integrate the private sector and the efforts of individual citizens too.

THE THREAT ECOSYSTEM OF TODAY AND TOMORROW: CHALLENGES FOR DHS AND BEYOND

Al-Qaeda (AQ) has been a shrewd practitioner of the art of stoking, piggybacking upon, and exploiting local grievances in order to further AQ's own goals and objectives and the broader global jihad. In a military context, this is referred to as tactical, operational, and strategic "swarming"; and it has clearly been adopted by others as well, as recent incidents around the globe have unfortunately demonstrated. Usama bin Laden may be dead, but the toxic ideology that he left behind lives on, and the narrative that it informs continues to resonate powerfully in certain quarters. Today perhaps the most significant locus of his legacy and methods is in Africa; though Pakistan's Federally Administered Tribal Areas, better known as FATA, remain a combustible region, one where it would be imprudent to ease up on U.S. pressure against militants.[1]

In Africa, al-Qaeda in the Arabian Peninsula (AQAP), al-Qaeda in the Islamic Maghreb (AQIM), Al Shabab (Somalia), Ansar al-Dine (Mali), Boko Haram (Nigeria), and their ilk persist in sowing discord and violence in a cross-continental swath ranging from east to west, leaving not even Timbuktu untouched. Indeed, even Yemen, the subject of significant counterterror efforts on the part of the United States (and others), remains home to AQAP and to one of the world's most dangerous bomb-makers, Ibrahim al-Asiri. Notwithstanding U.S. and allied counterterrorism efforts that have yielded a good measure of success, these terror affiliates remain committed to carrying forward the mantle of bin Laden, and to exploiting both ungoverned and under-governed spaces. The latter tactic pre-dated the Arab Spring, but evidenced reinforcement and magnification thereafter. The tragic violence of recent days, beginning in Benghazi and directed against U.S. personnel and interests (and those of allies), may come to further prove this point, though key facts remain under investigation.

As observed in a report on Mauritania published earlier this year by the Carnegie Endowment for International Peace, Africa is a hot spot because of the confluence of multiple factors, including poverty, corruption, and weak governance. The ensuing void left in countries like Mauritania, where state infrastructure like the education system is weak, offers an opening to "mahadras" (religious schools) propagating violent ideologies, which in turn spur the growth of militancy. The outlook for the Continent is not entirely bleak however; as the study points out, "there is a high level of distrust between black Africans and AQIM, a movement led and dominated by Arabs"—which portends a recruitment challenge for al-Qaeda forces in the area, at least in the longer term.[2] The outcome is not predetermined, though, as AQ was able to surmount and ingrain itself into the tribal populations indigenous to the FATA by pursuing a concerted strategy of marrying into these clans. Whether a similar or other course might further pave the way for inroads into African countries remains to be seen and merits continued U.S. vigilance, as well as that of our allies.

The various terrorist organizations cited above are exhibiting, moreover, an increasing willingness to reach out and partner with one another, as well as with others, who may be able to help build their indigenous capacities and further their particular goals. The twin phenomena of violent extremism and cross-group cooperation of such forces is assuredly not limited to Africa, and extends to the veritable witch's brew of forces that ranges from Iraq, Pakistan, and the Caucasus, to Mali, Nigeria, and Somalia—where militants linked to al-Qaeda tried to kill the country's new President just last week in a double suicide/homicide blast. Pakistan is especially complex, and dangerous. Groups that were once regionally focused now subscribe ever-more to al-Qaeda's goals and the broader global jihad. This toxic blend includes the Haqqani network,[3] Laskhar-e-Taiba (LeT), Tehrik-i-Taliban Pakistan, Harkat-

[1] U.S. military actions, including the use of drones, have had significant operational effects on al-Qaeda (and associated entities) by disrupting foreign fighter pipelines to the region, activities of key facilitators, and training camps. Think of it as suppressive fire. The more time al-Qaeda and associated entities spend looking over their shoulders, the less time they have to train, plot, and execute terrorist attacks. And with al-Qaeda senior leaders on their back heels, now is the time to exploit this unique window of counterterrorism opportunity by maintaining the operational tempo to consolidate these gains.

[2] Anouar Boukhars, The Drivers of Insecurity in Mauritania *Carnegie Paper* (April 2012) *http://carnegieendowment.org/2012/04/30/drivers-of-insecurity-in-mauritania#.*

[3] Recently designated a Foreign Terrorist Organization by the Department of State (a too-long delayed move, though one rightly supported by the Chairman of this Committee). *http://translations.state.gov/st/english/article/2012/09/20120907135632.html#axzz26kbUie00;* see also Frank J. Cilluffo, "U.S.-India Counterterrorism Cooperation: Deepening the Partnership"

Continued

ul-Jihad al-Islami (HuJI), Jaish-e-Mohammed, and the Islamic Movement of Uzbekistan; all of which cooperate with al-Qaeda on a tactical and sometimes strategic basis, linked by an affinity for militant Islamist ideology—with United States, Indian, Israeli, and Western targets increasingly in their cross-hairs. Historically, collaborative efforts among such groups were primarily linked to covert logistical support, including the provision of money, safe havens, and arms, as well as the movement back and forth of key personnel from one entity to another.

Not so today, where the relationships between terrorist groups are becoming more overt and strategic in nature. As events on the ground in Syria demonstrate, there will be no shortage of opportunities for foreign fighters who wish to travel to jihadi conflict zones. Consider also Africa, where the head of U.S. Africa Command General Carter Ham has stated that "the linkages between AQIM and Boko Haram are probably the most worrisome in terms of the indications we have that they are likely sharing funds, training and explosive materials that can be quite dangerous."[4] So too closer to home, where the Commander of U.S. Southern Command General Douglas M. Fraser has observed a similar type of convergence (based on convenience) between terrorist and criminal organizations in the Tri-Border area of Argentina, Brazil, and Paraguay.[5] Within the Continental United States, furthermore, the New York City Police Department has expanded its decade-plus focus on core al-Qaeda, affiliates, and the homegrown threat (inspired by AQ), to include Iran and Hezbollah—as part of NYPD's continuing efforts to build a robust and independent counterterror posture for the City of New York.[6] In turn, the Los Angeles Police Department recently elevated the government of Iran and its proxies (notably Hezbollah) to a Tier I threat.[7] This last development is particularly concerning given Iran's on-going drive to achieve nuclear weapons capability, and the statement this month of Lebanese Hezbollah leader Sayyed Hassan Nasrallah to the effect that there will be no distinction drawn between Israel and the United States in terms of retaliation, should Israel attack Iran to halt its progress toward the nuclear goal: "If Israel targets Iran, America bears responsibility."[8] Both the Director of the (U.S.) National Counterterrorism Center and the Director of National Intelligence have underscored concern about Iran and their proxies, suggesting respectively in recent testimony (the former before this committee) that "Iran remains the foremost state sponsor of terrorism"[9]; and that Iran is "now more willing to conduct an attack in the United States."[10]

All this to say there is little ground for complacency, as toxic forces converge and cooperate in multiple spots across the globe, more than ever before; as ideology and narrative continue to inspire, including those here in the United States—recall that 58-plus homegrown jihadi terrorism plots have been discovered in this country since 9/11; and as foreign fighters return to their homelands battle-hardened and armed with Western passports—10 feet tall in the eyes of those who admire their exploits, and more importantly, a direct threat to Western security given their familiarity with potential targets they may select to attack.[11] Where foreign fighters are concerned, so-called "bridge figures" are of special importance, as they ensure that par-

---

Hearing before the House of Representatives Committee on Foreign Affairs, Subcommittee on Terrorism, Non-proliferation and Trade (September 14, 2011) *http://www.gwumc.edu/hspi/policy/testimony9.13.11_cilluffo.pdf*.

[4] Tristan McConnell, "Triple threat: Coordination suspected between African terrorist organizations" *Global Post* (June 26, 2012) *http://www.globalpost.com/dispatches/globalpost-blogs/africa/triple-threat-coordination-suspected-between-african-terrorist-or*.

[5] Statement before the Senate Armed Services Committee (March 6, 2012) *http://www.armed-services.senate.gov/statemnt/2012/03%20March/Fraser%2003-13-12.pdf*.

[6] Testimony of Mitchell D. Silber before the U.S. House of Representatives Committee on Homeland Security *Iran, Hezbollah, and the Threat to the Homeland* (March 21, 2012) *http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Silber.pdf*.

[7] Frank J. Cilluffo, Sharon L. Cardash, and Michael Downing, "Is America's view of Iran and Hezbollah dangerously out of date?" FoxNews.com (March 20, 2012) *http://www.foxnews.com/opinion/2012/03/20/is-americas-view-iran-and-hezbollah-dangerously-out-date/*

[8] Reuters, "Nasrallah: Iran could strike US bases if attacked" *The Jerusalem Post* (September 3, 2012) *http://www.jpost.com/IranianThreat/News/Article.aspx?id=283706*.

[9] Matthew G. Olsen, "Understanding the Homeland Threat Landscape" Hearing before the House Committee on Homeland Security (July 25, 2012) *http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Olsen.pdf*.

[10] James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence" (January 31, 2012) *http://intelligence.senate.gov/120131/clapper.pdf*.

[11] Frank J. Cilluffo, "Open Relationship" *ForeignPolicy.com* (February 15, 2012) *http://www.foreignpolicy.com/articles/2012/02/15/open_relationship?page=0,0;* and Jerome P. Bjelopera "American Jihadist Terrorism: Combating a Complex Threat" *CRS Report for Congress* (November 15, 2011) *http://www.fas.org/sgp/crs/terror/R41416.pdf* (but note that numbers have increased since the Report was published).

ticular fighter pool is replenished, by helping to inspire, radicalize, and motivate. These figures exude charisma, and exhibit cultural and linguistic fluency as well as other skills that propel them to positions of leadership, guidance, and prominence. Abdullah al-Faisal, a Jamaican with ties to shoe bomber Richard Reid and to (attempted) Times Square bomber Faisal Shahzad, is but one example.[12]

Just as the threat has gravitated and metastasized to areas in the physical world that will best support the ideology and activities at issue, so too has the threat taken hold in (and of) the cyber domain—where terrorists are still afforded too much freedom of maneuver. Being squeezed in Pakistan's FATA, the Sahel, Yemen, or elsewhere, does not mean "game over" when the internet offers a transnational base and springboard for a variety of operations, including fundraising, recruitment, planning, training, and even implementation and execution of plots and plans.[13] As I outlined in testimony before the Senate 5 years ago: "Extremists value the internet so highly that some have adopted the slogan 'keyboard equals Kalashnikov'. Terrorist groups now have their own media production arms (al-Qaeda relies on As-Sahab and the Global Islamic Media Front, for example). Terrorists produce their own television programs and stations, websites, chat rooms, on-line forums, video games, videos, songs, and radio broadcasts."[14] Having said that, and as I have indicated in further Senate testimony, this one more than a decade ago: "Bits, bytes, bugs, and gas will never replace bullets and bombs as the terrorist weapon of choice."[15]

However, as kinetic measures (U.S. and allied) generate gains in the real-world, this may lead al-Qaeda and its sympathizers to enter even more deeply into the cyber domain. Indeed, al-Qaeda and their jihadi ilk may be surfing in the wake of "Anonymous" and other such groups, to learn from and perhaps also exploit their actions. The cyber threat writ large is much broader and more multifaceted, though. It may emanate from individual hackers, "hacktivists," criminal or terrorist groups, nation-states or those that they sponsor. Moreover, the threat spectrum affects the public and private sectors, the interface and intersections between them, as well as individual citizens. From a homeland security perspective, foreign states are (by and large) our principal concerns in the cyber domain, at least in terms of sophistication; specifically those countries that pose an advanced and persistent threat, namely Russia and China. Their tactics may also be exploited by others.[16] Furthermore, as laid out in my testimony to a joint hearing of two subcommittees of this body in April 2012, the government of Iran and its terrorist proxies are serious concerns in the cyber context. What Iran may lack in capability, it makes up for in intent; and our adversaries do not need highly sophisticated capabilities—just intent and cash—as there exists an arms bazaar of cyber weapons, allowing our adversaries to buy or rent the tools they need or seek.[17]

The cyber threat (and supporting technology) has markedly outpaced our prevention and response efforts. Use of cyber means as a force multiplier for kinetic activities, which would represent the convergence of the physical and cyber worlds, constitutes probably the area of greatest concern over the next 5 to 10 years. Foreign militaries are increasingly integrating computer network attack (CNA) and computer network exploitation (CNE) capabilities into their warfighting, and military

---

[12] Frank J. Cilluffo, Jeffrey B. Cozzens, and Magnus Ranstorp, *Foreign Fighters: Trends, Trajectories & Conflict Zones* (October 1, 2010 *http://www.gwumc.edu/hspi/policy/report_foreignfighters501.pdf*.

[13] The George Washington University Homeland Security Policy Institute (HSPI) and the University of Virginia Critical Incident Analysis Group (CIAG), *NETworked Radicalization* (Special Report: May 2007) *http://www.gwumc.edu/hspi/policy/NETworkedRadicalization.pdf*.

[14] "The Internet: A Portal to Violent Islamist Extremism" (May 3, 2007) *http://www.gwumc.edu/hspi/policy/testimony5.3.07_cilluffo.pdf*.

[15] "Critical Infrastructure Protection: Who's In Charge" (October 4, 2001) *http://www.gwumc.edu/hspi/policy/testimony10.4.01_cilluffo.pdf*.

[16] Frank J. Cilluffo, "The U.S. Response to Cybersecurity Threats" *American Foreign Policy Council (AFPC) Defense Dossier* (August 2012) *http://www.afpc.org/files/august2012.pdf;* see also Office of the National Counterintelligence Executive (NCIX), *Foreign Spies Stealing U.S. Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009–2011* (October 2011) *http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf*.

[17] "The Iranian Cyber Threat to the United States" *Statement before the House of Representatives Committee on Homeland Security, Subcommittees on Counterterrorism and Intelligence, and on Cybersecurity, Infrastructure Protection, and Security Technologies* (April 26, 2012) *http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20-Cilluffo.pdf*.

planning and doctrine.[18] Such activity may involve "intelligence preparation of the battlefield," to include the mapping of perceived adversaries' critical infrastructures. To my mind, the line between this type of reconnaissance and an act of aggression is very thin, turning only on the matter of intent. Foreign intelligence services, too, are engaging in cyber espionage against us, often combining technical and human intelligence in their exploits. Here, everything from critical infrastructure to intellectual property is potentially at risk. These exploits permit others to leapfrog many bounds beyond their rightful place in the innovation cycle, by profiting from (theft of) the research and development in which private and public U.S. entities invested heavily. At worst, these exploits hold the potential to significantly degrade our National defense and National security, and thereby undermine the trust and confidence of the American people in their Government.

New opportunities for resilience, generated by forces including changing technologies, will assuredly present themselves. Indeed it is this ability to reconstitute, recover, and get back on our feet is in fact perhaps the best deterrent. The storms that battered the National Capital Region this summer leaving close to a million people without power during a week-long heat wave are instructive in terms of our shortcomings on resilience. Mother Nature may be a formidable adversary, but just imagine the level of damage and destruction that a determined and creative enemy could have wrought. There is no lack of trying, as a recently published DHS report makes clear, noting the spike in attacks (from 9 incidents to 198) against U.S. critical infrastructure from 2009 to 2011.[19] The good news, on the other hand, is that the most serious of these incidents could have been avoided through the adoption of basic security steps and best practices. The bad news, of course, is that these fundamental measures were not yet put into place.

DHS: A LOOK BACK AND AHEAD

Looking ahead, U.S. and allied counterterrorism efforts that achieved localized successes must be woven into a larger, sustained, and strategic effort; one that continues to apply targeted pressure to deny adversaries the time and space to maneuver, including in cyberspace. Since the threat now comes in various shapes, sizes, and forms—ranging from al-Qaeda's Senior Leadership (Ayman al-Zawahiri and his top deputies), to its principal franchises and affiliates, to individuals inspired by (if not directly connected to) al-Qaeda's ideology, which includes the "home-grown" threat—the U.S. response, and that of DHS in turn, must be at once both sufficiently comprehensive in scope and sufficiently nimble in approach to address effectively the multi-dimensional threat landscape of today as well as tomorrow.

Unfortunately our efforts to counter and defeat the jihadist ideology have been lacking, with the result that the terrorist narrative lives on, and continues to attract and inspire those who wish us harm. A sustained, comprehensive, integrated, and effective effort to combat violent Islamist extremism is, in my view, the biggest element missing from U.S. statecraft on counterterrorism. Although the Department of State's Center for Strategic Counterterrorism Communications (CSCC) is doing some good work and represents a positive development in this space, now is the time to double down, do more, and hit back harder. The power of negative imagery, as in a political campaign, could be harnessed to hurt our adversaries and further chip away at their appeal and credibility in the eyes of peers, followers, and sympathizers. A sustained and systemic strategic communications effort aimed at exposing the hypocrisy of Islamists' words versus their deeds, could knock them off balance, as could embarrassing their leadership by bringing to light their seamy connections to criminal enterprises and drug-trafficking organizations. The increasingly hybrid nature of the threat presents additional opportunities in this last regard, as drugs and arms trafficking are used to finance terrorism, and so too kidnapping for ransom (think Abu Sayyaf and AQIM). Brokering in-fighting between and among al-Qaeda, its affiliates, and the broader jihadi orbit in which they reside, will damage violent Islamists' capability to propagate their message and organize operations both at home and abroad. Locally administered programs are especially significant, as many of the solutions reside outside the U.S. Government and will require communities policing themselves. In short, we could and should do more to drive wedges

---

[18] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage,* Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation (March 7, 2012) p. 54 *http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf*.

[19] Suzanne Kelly "Homeland security cites sharp rise in cyber attacks" CNN.com (July 4, 2012). *http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/*.

and foment distrust (including by exploiting points of conflict between local interests and the larger global aims of AQ); encourage defectors; delegitimize and disaggregate our adversaries' narrative; and above all, remember the victims.[20]

As the distinction between home and abroad increasingly blurs, due in part to technologies and tools such as social media, it is important to study and ultimately institutionalize counterterrorism lessons learned elsewhere, including about tactics, techniques, and procedures. In the aftermath of the "26–11" Mumbai attacks, for instance, the Los Angeles, Las Vegas, and New York City Police Departments each sent a team of experts to Mumbai. The objective was to meet with Indian counterparts to learn about Mumbai's response model and then-existing loopholes, which knowledge LAPD, LVPD, and NYPD could then apply to their home cities, with an eye to closing gaps in their own counterterrorism strategies and operations. More initiatives of this kind are needed, as is the continuation of those that already exist (such as police exchanges). Endeavors of this type are particularly important in a resource-scarce environment, as they can help avoid the need to reinvent the wheel.[21]

To obtain a truly "rich picture" of the threat in this country, we must focus on the field—not the Beltway. As recent history shows, the military and intelligence communities have come to just such a field bias. For the counterterrorism community to do otherwise is to risk stifling and stymieing the good work being done where the rubber meets the road. State and local authorities can and should complement what the Federal Government does not have the capacity or resources to collect (or is simply not best-suited to do) in terms of intelligence; and thereby help determine the scope and contours of threat domains in the United States. Further leveraging our decentralized law enforcement infrastructure could also serve to better power our Fusion Centers, which should be given ample opportunity to flourish. The equivalent of Commanders' Intent, which gives those in the field the leeway to do what they need to do and which incorporates an honest "hotwash" after the fact to determine what went wrong and how to fix that, is needed in present civilian context for counterterrorism and intelligence purposes. Moreover, opportunities still exist to tap and apply intelligence and information from the field of organized crime to the field of counterterrorism, and vice versa. Hybrid thinking that marries up the two fields in this way, in order to further build our reservoir of knowledge on the counterterrorism side could prove valuable.

Straightforward yet powerful steps remain to be taken. This was revealed starkly in multiple rounds of survey work—first with the major metropolitan intelligence chiefs and later with the fusion centers—that the Homeland Security Policy Institute (HSPI) recently completed in an attempt to bring a little science to the art of intelligence. For example, too few Fusion Centers currently do threat assessments. This is unacceptable, especially in a climate of limited resources in which allocation decisions (regarding human, capital, and financial resources) should be priority-ordered, meaning that scarce resources should be directed to those counter-threat measures, gaps, and shortfalls that constitute areas of greatest need. And Fusion Center-specific threat assessments are just a start. Regional threat assessments are also needed. Our adversaries do not respect local, State, or even National boundaries hence our response posture must be similarly nimble and cohesive. Yet according to HSPI survey research published in June of this year, only 29% of Fusion Center respondents reported that their Center conducted a regional threat assessment on at least a yearly basis. Almost half reported that their Centers simply did not conduct regional threat assessments. Furthermore, those working in the Fusion Centers have yet to be invested with the analytical skill-craft and training necessary for them to accomplish their mission. Current incentive structures place too much emphasis on information processing and not enough on analytical outcome. Greater resources should be allocated to the professional development of those working in the Centers. Within them lies untapped collection and analysis potential. Realizing and unleashing that potential will further bolster State and local law enforcement efforts, and help develop anticipatory intelligence to prevent terrorist attacks and the proliferation of criminal enterprise operations.[22] In tandem, and with-

---

[20] Frank J. Cilluffo, "The Future of Homeland Security: Evolving and Emerging Threats" *Hearing Before the Senate Committee on Homeland Security & Governmental Affairs* (July 11, 2012) *http://www.gwumc.edu/hspi/policy/Testimony%20-%20SHSGAC%20Hearing%20-%2011%20July%202012.pdf*.

[21] Cilluffo, "U.S.-India Counterterrorism Cooperation."

[22] Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing, and Keith D. Squires "Counterterrorism Intelligence: Fusion Center Perspectives" HSPI Counterterrorism Intelligence Survey Research (CTISR) (June 2012). *http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism-*

Continued

out taking anything away from the Fusion Centers, Joint Regional Intelligence Groups (JRIGs) also have a role to play, including by helping to place National threat information into State and local context.

DHS continues to mature over time. However its capacities generally still remain reactive in nature. As a result, the Department's internal capabilities to assess future threats and then take actions are not yet evolved to the level that the security ecosystem demands. This is a significant shortfall, especially relative to the cyber domain where threats may morph and metastasize in milliseconds. Volume and pace in the cyber arena alone make for a serious challenge, including the potential for damage to critical U.S. infrastructure such as water and power systems, and telecommunications and finance. Since (as mentioned above) cyber tools/attacks may also be leveraged, acting as a force multiplier in connection with kinetic actions undertaken by our adversaries, the ability to look over the horizon and think creatively, including through the eyes of those of those who may bear hostile intent towards this country, is to be prized. Yet DHS does not currently have the built-in structural capacity to do so. Precisely because the Department must be able to respond to a wide range of threats that may materialize quickly, an Office of Net Assessment (ONA) could and should be created.

The ONA would fill the much-needed role of brain trust, while remaining unfettered by the "crisis du jour" or the day-to-day demands flowing from intelligence needs and operations. The ever-shifting and unpredictable security environment facing the United States requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable, all in order to identify game changers. The ONA should take a comprehensive, multi-disciplinary approach to its analysis, looking at the full range of factors which will alter and shape the security environment of the future, including social, political, technological, economic, demographic, and other trends. The duties of ONA should include studying existing threats in order to project their evolution into the future; studying trends in the weapons, technologies, modalities, and targets utilized by our adversaries (i.e., the events that can transform the security landscape); reviewing existing U.S. capabilities in order to identify gaps between current capabilities and the requirements of tomorrow's threats; conducting war games and red team scenarios to introduce innovative thinking on possible future threats; assessing how terrorist groups/cells could operate around, and/or marginalize the effectiveness of, policies and protective measures. Admittedly, this is a tall order. The alternative, however, is to walk into the future partly blind and thus remain more vulnerable than we need to or should be.

This proposal is not new, I should add. To the contrary, it appeared in the January 2007 Homeland Security Advisory Council Report of the Future of Terrorism Task Force, for which I served as Vice Chairman together with Chairman Lee Hamilton.[23] Now is the time—indeed it is well past time—to take this recommendation off the page and enact it. Our adversaries are patient and they are long-term thinkers whose horizons extend well beyond weeks and months. To help counter them effectively, we must not lose sight of the long game either. Indeed, the general qualities needed from an organizational standpoint (U.S./DHS) mirror many of the traits that our adversaries have exhibited over time. They are proactive, innovative, well-networked, flexible, patient, young and enthusiastic, technologically savvy, and learn and adapt continuously based upon both successful and failed operations around the globe. We and our Government must be and do likewise. Our institutions, both their structure and culture, must be responsive to the ever-changing threat environment. This entails much more than rearranging boxes on an organization chart. Together with policy and technology, people are a crucial component of the equation. Organizational change will not take root unless supported by cultural change, which in turn takes time, leadership, and both individual and community commitment. Many at DHS have worked long and hard to bring about a cohesive and collaborative culture that drives mission success; but we would do well to keep striving on that front, if only because sustaining an end-state can be as difficult as arriving at it in the first place.

The type of forward-leaning assessment and evaluation described above could have a range of salutary knock-on effects, including the possibility of better-calibrated budgeting, operational planning, and acquisitions, through the provision of a foundation from which forward-estimates may be derived. As things now stand,

---

%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf. See also Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing "Counterterrorism Intelligence: Law Enforcement Perspectives" CTISR (September 2011). *http://www.gwumc.edu/hspi/policy/HSPI%20Research%20Brief%20-%20Counterterrorism%20Intelligence.pdf.*

[23] *http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf.*

the Department still has a ways to go in terms of aligning actions with future threats—although the Quadrennial Homeland Security Review (QHSR), while less than perfect, has served as a useful starting point. Still, as a mechanism and process for helping to bring DHS resources and plans into sync with the threat environment, the QHSR is not as forward-leaning as it could or should be. The country would be better served by a more robust posture and process, one that anticipates threats before they manifest, and that allows the Secretary to determine what tools are needed for meeting them, what force structure is needed (at the Federal, State, and local levels), and what resources are needed from Congress to make that plan a reality. Importantly, we do not yet have a true "rich picture" of the domestic threat landscape because the National Intelligence Estimate (NIE) does not fully elaborate upon that dimension. This gap must be remedied, with State and local officials at the heart of that exercise, because they are best-positioned to undertake the task.

Cyber threats in particular manifest in nanoseconds, and we need to be able to enact cyber response measures that are almost as quick. This means developing and implementing an "active defense" capability to immediately attribute and counter attacks and future threats in real-time. Although much work remains to be done on the counterterrorism side, the country has achieved significant progress in this area. In contrast, the U.S. cybersecurity community's state of development is akin to that of the counterterrorism community as it stood shortly after 9/11. Despite multiple incidents that could have served as galvanizing events to shore up U.S. resolve to formulate and implement the changes that are needed, and not just within Government, we have yet to take those necessary steps. Officials in the homeland security community should therefore undertake contingency planning that incorporates attacks on U.S. infrastructure. At minimum, "red-teaming" and additional threat assessments are needed. The latter should include modalities of attack and potential consequences. Working together with DHS Intelligence and Analysis colleagues, the Department's National Protection and Programs Directorate (NPPD) could and should do more in terms of threat and intelligence reporting, especially in relation to critical infrastructure, where DHS is well-positioned to add real and unique value given the Department's relationship with and responsibilities towards the private sector. Consider the cyber-attacks on Saudi Aramco and Qatari RasGas this past summer, which hit thousands of computers at these critical oil and gas producers with a virus. As events unfolded, one would expect that counterpart industries here in the United States would have welcomed DHS products that directly assessed these events and kept U.S. owners and operators abreast of latest developments, their broader significance and potential follow-on implications.

The United States should also develop and clearly articulate a cyber-deterrence strategy. Such a deterrence policy should apply generally, and also in a tailored manner that is actor/adversary-specific. A solid general posture could serve as an 80 percent solution, neutralizing the majority of threats before they manifest fully. This, in turn, would free up resources (human, capital, technological, etc.) to focus our limited resources and bandwidth on the high-end of the threat spectrum and on those which are most sophisticated and persistent. To operationalize these recommendations, we must draw lines in the sand. Preserving flexibility of U.S. response by maintaining some measure of ambiguity is useful, so long as we make parameters clear by laying down certain markers or selected redlines whose breach will not be tolerated. More investment needs to be made in our offensive capability as well, in order to support the foregoing proposals in terms of practice and at the level of principle (to signal a credible commitment). Cybersecurity by definition is transnational in nature and will require some level of transnational solutions, yet it must not be approached like an arms control treaty (i.e., attribution and verification are still a ways away). Notably NPPD, which manages the cyber-portfolio for DHS, has done some good work in the international arena, including cyber-specific capacity-building efforts and exercises, in multilateral settings and with bilateral partners. However, as the Department's Inspector General noted in a report issued just this month,[24] DHS must continue to build on its *Cybersecurity Strategy*

[24] DHS Office of Inspector General, *DHS Can Strengthen Its International Cybersecurity Programs (Redacted)* (August 2012) *http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr__12-112__Aug12.pdf*.

of November 2011,[25] such as by clearly delineating "roles and responsibilities" for NPPD.[26]

Plainly we have not yet made the requisite business case for the private sector to undertake and implement needed cybsecurity measures. This represents a fundamental problem, given that the majority of critical infrastructure in this country is owned and operated by the private sector. The urgency for making this case needs no further explanation, but we must take care to strike just the right balance of carrots—such as tax breaks, priority in Government contracting opportunities, and indemnification of liability, allowing those who have done what has been asked of them to avoid costly litigation—and sticks; and of measures that ensure both privacy and security. To help ensure compliance with standards and best practices, a "Good Housekeeping" seal of approval could be granted to those who meet the bar. To the extent that this encourages industry-wide adoption and robust outcomes, such measure could spur the insurance and reinsurance sectors to step into the fray. In addition, the Federal Government has a responsibility to share threat information (i.e., signatures, hostile plans and techniques to degrade, disrupt or destroy systems) that places our critical infrastructures at risk. The pilot program introduced within the confines of the defense industrial base offers a solid starting point, and an example of a promising information-sharing environment.[27] It probably should go without saying, but part of leading by example also entails the U.S. Government striving to place its own house in order, as a crucial corollary to meeting the threat.

In conclusion, the challenges that lie on the horizon remain substantial, but with the requisite will and leadership—to lean forward and exhibit a field bias towards military, intelligence community, and law enforcement experts on the front lines—the country can and will continue to make progress towards meeting those imperatives. Again, I wish to thank the Committee and its staff for the opportunity to testify today, and I would be pleased to try to answer any questions that you may have.

Chairman KING. Thank you, Mr. Cilluffo.

Our final witness is Mr. David Maurer. He is a GAO director in the Homeland Security and Justice Team, where he leads GAO's work reviewing DHS and DOJ management issues. His recent work in these areas includes DHS management integration, the Quadrennial Homeland Security Review, Secret Service financial management, DOJ grant management, Federal prison system, and an assessment of technologies for detecting explosives in the passenger rail environment.

Mr. Maurer has testified before this committee several times and, surprisingly, he has agreed to come back again. So we thank you very much for your testimony, and look forward to it. Thank you for your service.

STATEMENT OF DAVID C. MAURER, DIRECTOR, HOMELAND SECURITY AND JUSTICE, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. MAURER. Great. Thank you very much. Good morning, Chairman King, Ranking Member Thompson, other Members and staff. I am pleased to be here today to talk about DHS's on-going efforts to build a unified Department and position itself for the future.

Since it began operations nearly a decade ago, DHS has made significant strides. Today, it has almost $60 billion in budget authority to carry out a wide variety of critical missions. Fending off

---

[25] *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.*

[26] Mickey McCarter, "NPPD Lacks Strategy To Guide International Cybersecurity Efforts" *Homeland Security Today* (September 4, 2012) *http://www.hstoday.us/index.php?id=3392&no_cache=1&tx_ttnews%5Btt_news%5D=25801.*

[27] Frank J. Cilluffo and Andrew Robinson, "While Congress Dithers, Cyber Threats Grow Greater" *Nextgov.com* (July 24, 2012) *http://www.nextgov.com/cybersecurity/2012/07/while-congress-dithers-cyber-threats-grow-greater/56968/.*

terrorist threats, securing the border, safeguarding cyberspace, and providing disaster relief.

However, DHS has considerable work ahead to address weaknesses in its current operations and management that hinder the Department's ability to achieve its full potential. As a result, DHS remains on our high-risk list. My main message today is this. At the root of many of the Department's problems is a fundamental cross-cutting and significant challenge; namely, DHS needs to do a better job managing its resources.

Specifically, DHS needs a strong, unified management foundation that enables its components to execute their vital missions. DHS also needs to ensure that increasingly scarce resources are strategically managed and aligned with risk-based priorities. Making tough, informed resource decisions is important because DHS will never have enough people, money, and systems to fully address every threat.

DHS has a lot of work ahead to achieve these goals. Two years ago, to help DHS with that task we identified 31 actions and outcomes that are critical to addressing the Department's challenges. DHS agreed to achieve these outcomes, and has taken actions to do so. But DHS isn't there yet.

It currently lacks vital management capabilities to integrate the Department into something greater than the sum of its parts. For example, nearly every major DHS acquisition program has experienced funding instability, workforce shortfalls, and/or changes to their planned capabilities. DHS morale scores consistently among the lowest in the Federal Government.

DHS has twice attempted, and failed, to build an integrated Department-wide financial management system. The Department has also struggled to achieve strategic visibility over how it allocates its resources. For example, Congress has appropriated nearly $40 billion for DHS grant programs, however DHS has limited visibility over how these funds are used, does not effectively coordinate across its various programs, and lacks mechanisms for assessing grant effectiveness.

DHS also does not know how much it spends on research and development activities, and lacks policies to define and coordinate R&D across the Department. DHS says it plans to spend $167 billion on major acquisition programs in the coming years. But that is, at best, an educated guess.

Most programs lack validated cost estimates, and DHS is still in the early stages of grappling with strategically managing these programs as a portfolio rather than on an individual basis. In recent years, DHS has worked hard to fix problems like these, and has achieved some key successes. For example, DHS obtained a qualified audit opinion on its balance sheet for the first time since its operation last year.

It has significantly lowered its senior leadership vacancy rates. It has developed a promising new approach for reviewing its IT investments. We have also seen substantial senior-level support for a series of plans to help ensure that DHS's missions are supported by a sound management infrastructure.

In particular, the Department's June 2012 strategy for addressing its high-risk designation is a good road map for taking DHS to

where it wants to be. Looking ahead, DHS needs to show continued progress executing this ambitious agenda. Now, I know that "management" is not the most exciting word in the world, but it is vital.

In fact, management is the glue that holds DHS together, the daily missions of the various DHS components, and the threats that they address very widely. To ensure the Department works as one, DHS needs a clear common vision, a unified management structure, and the ability to make tough, risk-based resource decisions to ensure that strategies drive budgets and not the other way around.

DHS has made important strides achieving these goals, but the Department still has a great deal of work ahead. Improving how it manages its resources will help DHS carry out its vital missions and help secure the homeland.

Mr. Chairman, thank you for the opportunity to testify this morning. I look forward to your questions.

[The prepared statement of Mr. Maurer follows:]

PREPARED STATEMENT OF DAVID C. MAURER

SEPTEMBER 20, 2012

DEPARTMENT OF HOMELAND SECURITY.—CONTINUED PROGRESS MADE IMPROVING AND INTEGRATING MANAGEMENT AREAS, BUT MORE WORK REMAINS

GAO–12–1041T

Chairman King, Ranking Member Thompson, and Members of the committee: I am pleased to be here today to discuss the Department of Homeland Security's (DHS) efforts to strengthen and integrate its management functions. DHS now has more than 200,000 employees and an annual budget of almost $60 billion, and its transformation is critical to achieving its homeland security and other missions. Since 2003, GAO has designated the implementation and transformation of DHS as high-risk because DHS had to combine 22 agencies—several with major management challenges—into one Department, and failure to effectively address DHS's management and mission risks could have serious consequences for our National and economic security.[1] This high-risk area includes challenges in strengthening DHS's management functions—financial management, acquisition management, human capital, and information technology (IT)—the effect of those challenges on DHS's mission implementation, and challenges in integrating management functions within and across the Department and its components.

In November 2000, we published our criteria for removing areas from the high-risk list.[2] Specifically, agencies must have: (1) A demonstrated strong commitment and top leadership support to address the risks; (2) the capacity (that is, the people and other resources) to resolve the risks; (3) a corrective action plan that identifies the root causes, identifies effective solutions, and provides for substantially completing corrective measures in the near term, including but not limited to steps necessary to implement solutions we recommended; (4) a program instituted to monitor and independently validate the effectiveness and sustainability of corrective measures; and (5) the ability to demonstrate progress in implementing corrective measures.

On the basis of our prior work, 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 to address the high-risk designation.[3] These key actions and outcomes include, among others, obtaining and then sustaining unqualified audit opinions for at least 2 consecutive years on the Department-wide financial

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

[2] GAO, *Determining Performance and Accountability Challenges and High Risks,* GAO–01–159SP (Washington, DC: November 2000).

[3] See appendix I for a summary of the 31 actions and outcomes.

statements; validating required acquisition documents in accordance with a Department-approved, knowledge-based acquisition process; and demonstrating measurable progress in implementing its IT human capital plan and accomplishing defined outcomes.[4] In January 2011, DHS issued its initial *Integrated Strategy for High-Risk Management,* which included key management initiatives (e.g., financial management controls, IT program governance, and procurement staffing model) to address challenges and the outcomes we identified for each management area. DHS provided updates of its progress in implementing these initiatives in later versions of the strategy—June 2011, December 2011, and June 2012. Achieving and sustaining progress in these management areas would demonstrate the Department's ability and on-going commitment to addressing our five criteria for removing issues from the high-risk list.

My testimony this morning, as requested, will discuss our observations, based on prior and on-going work, on DHS's progress in achieving outcomes critical to addressing its high-risk designation for the implementation and transformation of the Department.

This statement is based on prior reports and testimonies we issued from June 2007 through September 2012 and letters we submitted to DHS in March and November 2011 providing feedback on the Department's January and June 2011 versions of its *Integrated Strategy for High-Risk Management.*[5] For the past products, among other methodologies, we interviewed DHS officials; analyzed DHS strategies and other documents related to the Department's implementation and transformation high-risk area; and reviewed our past reports, issued since DHS began its operations in March 2003. All of this work was conducted in accordance with generally accepted Government auditing standards; more-detailed information on the scope and methodology from our prior work can be found within each specific report. This statement is also based on observations from our on-going work related to DHS IT investments.[6] For this work, we analyzed recent cost and schedule performance for DHS's major IT investments as reported to the Office of Management and Budget as of March 2012. We will report on the final results of this review later this month. We are conducting 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS HAS MADE PROGRESS IN ADDRESSING ITS MANAGEMENT CHALLENGES, BUT HAS SIGNIFICANT WORK AHEAD TO ACHIEVE HIGH-RISK OUTCOMES

Since we designated the implementation and transformation of DHS as high-risk in 2003, DHS has made progress addressing management challenges and senior Department officials have demonstrated commitment and top leadership support for addressing the Department's management challenges. However, the Department has significant work ahead to achieve positive outcomes in resolving high-risk issues. For example, DHS faces challenges in modernizing its financial systems, implementing acquisition management controls, and improving employee satisfaction survey results, among other things. As DHS continues to mature as an organization, it will be important for the Department to continue to strengthen its management functions, since the effectiveness of these functions affects its ability to fulfill its homeland security and other missions.

Financial management.—DHS has made progress in addressing its financial management and internal controls weaknesses, but has been unable to obtain an unqualified audit opinion on its financial statements since the Department's creation and faces challenges in modernizing its financial management systems. DHS has, among other things,

---

[4] An unqualified opinion states that the audited financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with generally accepted accounting principles.

[5] See the related products list at the end of this statement.

[6] This review is being conducted at the request of this Committee's Subcommittee on Oversight, Investigations, and Management; and Senator Thomas Carper, Chairman, Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security of the Senate Committee on Homeland Security and Governmental Affairs.

- reduced the number of material weaknesses in internal controls from 18 in 2003 to 5 in fiscal year 2011;[7]
- achieved its goal of receiving a qualified audit opinion on its fiscal year 2011 consolidated balance sheet and statement of custodial activity for the first time since the Department's creation;[8]
- established a goal of obtaining an audit opinion on all of its fiscal year 2012 financial statements; and
- expanded the scope of the annual financial audit to the complete set of fiscal year 2012 financial statements, which DHS believes will help it to obtain an unqualified opinion for fiscal year 2013.[9]

However, DHS continues to face challenges in financial management. For example, DHS anticipates difficulties in providing its auditors transaction-level detail to support balances reported in its fiscal year 2012 financial statements in order to obtain an opinion on its financial statements. This is due to, among other things, components not retaining original acquisition documentation or enforcing policies related to recording purchases and making payments. DHS also anticipates its auditors issuing a disclaimer in their fiscal year 2012 report on internal controls over financial reporting due to material weaknesses in internal controls, such as lack of effective controls over the recording of financial transactions related to property, plant, and equipment.

In addition, in December 2011, DHS reported that the Federal Emergency Management Agency (FEMA), U.S. Coast Guard (USCG), and U.S. Immigration and Customs Enforcement (ICE) have an essential business need to replace their financial management systems, but DHS has not fully developed its plans for upgrading existing or implementing new financial systems at these agencies. According to DHS's June 2012 version of its *Integrated Strategy for High-Risk Management,* the Department plans to extend the useful life of FEMA's current system by about 3 years, while FEMA proceeds with a new financial management system solution, and is in the process of identifying the specific approach, necessary resources, and time frames for upgrading existing or implementing new financial systems at USCG and ICE. Without sound processes, controls, and systems, DHS faces long-term challenges in obtaining and sustaining an unqualified opinion on both its financial statements and internal controls over financial reporting, and ensuring its financial management systems generate reliable, useful, timely information for day-to-day decision-making. We currently have on-going work related to DHS's efforts to improve its financial reporting that we expect to report on in the spring of 2013.[10]

Acquisition management.—DHS has made progress in the acquisition management area by enhancing the Department's ability to oversee major acquisition programs. For example:

- DHS has established eight Centers of Excellence for cost estimating, systems engineering, and other disciplines to bring together program managers, senior leadership staff, and subject matter experts to promote best practices, provide expert counsel, technical guidance, and acquisition management tools; and each DHS component has established a Component Acquisition Executive (CAE) to provide oversight and support to programs within the component's portfolio. According to DHS, as of June 2012, 75 percent of the core CAE support positions were filled.
- In March 2012, DHS completed the development of a Procurement Staffing Model to determine optimal numbers of personnel to properly award and admin-

---

[7] A material weakness is a significant deficiency, or a combination of significant deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

[8] A qualified opinion states that, except for the effects of the matter(s) to which the qualification relates, the audited financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with generally accepted accounting principles. The matter(s) to which the qualification relates could be due to a scope limitation, or the audited financial statements containing a material departure from generally accepted accounting principles, or both.

[9] DHS's complete set of financial statements consist of the Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, and Statement of Custodial Activity.

[10] We are doing this work at the request of the Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security of the Senate Committee on Homeland Security and Governmental Affairs.

ister contracts. In June 2012, DHS reported that it is taking steps to implement the staffing model throughout headquarters and the components.

- DHS included a new initiative (strategic sourcing) in its December 2011 *Integrated Strategy for High-Risk Management* to increase savings and improve acquisition efficiency by consolidating contracts Department-wide for the same kinds of products and services. The Office of Management and Budget's Office of Federal Procurement Policy has cited DHS's efforts among best practices for implementing Federal strategic sourcing initiatives. Earlier this month, we reported that the Department has implemented 42 strategically-sourced efforts since the Department's inception.[11] According to DHS data, the Department's spending through strategic sourcing contract vehicles has increased steadily from $1.8 billion in fiscal year 2008 to almost $3 billion in fiscal year 2011, representing about 20 percent of DHS's procurement spending for that year.

However, DHS continues to face significant challenges in managing its acquisitions. For example:

- Earlier this week, we reported that 68 of the 71 program offices we surveyed from January through March 2012 responded that they experienced funding instability, workforce shortfalls, and/or changes to their planned capabilities over the programs' duration.[12] We have previously reported that these challenges increase the likelihood acquisition programs will cost more and take longer to deliver capabilities than expected.[13]
- Our recent review of DHS acquisition management also identified that while DHS's acquisition policy reflects many key program management practices that could help mitigate risks and increase the chances for successful outcomes, it does not fully reflect several key portfolio management practices, such as allocating resources strategically.[14] DHS plans to develop stronger portfolio management policies and processes, but until it does so, DHS programs are more likely to experience additional funding instability, which will increase the risk of further cost growth and schedule slips. We recommended that DHS take a number of actions to help mitigate the risk of poor acquisition outcomes and strengthen the Department's investment management activities. DHS concurred with all of our recommendations and noted actions it had taken or planned to address them.

Human capital management.—DHS has taken a number of actions to strengthen its human capital management. For example:

- DHS issued human capital-related plans, guidance, and tools to address its human capital challenges, including a *Workforce Strategy for 2011–2016;* a revised *Workforce Planning Guide,* issued in March 2011, to help the Department plan for its workforce needs; and a *Balanced Workforce Strategy* tool, which some components have begun using to help achieve the appropriate mix of Federal and contractor skills.
- The Department implemented two programs to address senior leadership recruitment and hiring, as we reported in February 2012.[15] While DHS's senior leadership vacancy rate was as high as 25 percent in fiscal year 2006, it varied between 2006 and 2011 and declined overall to 10 percent at the end of fiscal year 2011.[16]
- DHS developed outreach plans to appeal to veterans and other underrepresented groups.

While these initiatives are promising, DHS continues to face challenges in human capital management. For example:

- As we reported in March 2012, based on our preliminary observations of DHS's efforts to improve employee morale, Federal surveys have consistently found that DHS employees are less satisfied with their jobs than the Government-wide average.[17] DHS has taken steps to identify where it has the most significant employee satisfaction problems and developed plans to address those problems, such as establishing a Department-wide Employee Engagement Executive

---

[11] GAO, *Homeland Security: DHS Has Enhanced Procurement Oversight Efforts, but Needs to Update Guidance,* GAO–12–947 (Washington, DC: Sept. 10, 2012).

[12] GAO, *Homeland Security: DHS Requires More Disciplined Investment Management to Help Meet Mission Needs,* GAO–12–833 (Washington, DC: Sept. 18, 2012).

[13] GAO, *Department of Homeland Security: Assessments of Complex Acquisitions,* GAO–10–588SP (Washington, DC: June 30, 2010).

[14] GAO–12–833.

[15] GAO, *DHS Human Capital: Senior Leadership Vacancy Rates Generally Declined, but Components' Rates Varied,* GAO–12–264 (Washington, DC: Feb. 10, 2012).

[16] GAO–12–264.

[17] GAO, *Department of Homeland Security: Preliminary Observations on DHS's Efforts to Improve Employee Morale.* GAO–12–509T (Washington, DC: Mar. 22, 2012).

Steering Committee, but has not yet improved employee satisfaction survey results. We plan to issue a final report on our findings later this month.[18]

- As we reported in April 2012, changes in FEMA's workforce, workload, and composition have created challenges in FEMA's ability to meet the agency's varied responsibilities and train its staff appropriately.[19] For example, FEMA has not developed processes to systematically collect and analyze agency-wide workforce and training data that could be used to better inform its decision making. We recommended that FEMA, among other things, identify long-term quantifiable mission-critical goals, establish lines of authority for agency-wide workforce planning and training efforts, and develop systematic processes to collect and analyze workforce and training data. DHS concurred with our recommendations and reported actions underway to address them.

Information technology management.—DHS has made progress in strengthening its IT management, but the Department has much more work to do to fully address its IT management weaknesses. Among other accomplishments, DHS has:

- strengthened its enterprise architecture;[20]
- defined and begun to implement a vision for a tiered governance structure intended to improve program and portfolio management, as we reported in July 2012;[21] and
- established a formal IT Program Management Development Track and staffed Centers of Excellence with subject matter experts to assist major and non-major programs.

Based on preliminary observations from our review of DHS's major at-risk IT acquisitions we are performing for the committee, these improvements may be having a positive effect. Specifically, 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).

DHS has made progress, but the Department has much more work to do to fully address its IT management weaknesses. For example, the Department needs to:

- finalize the policies and procedures associated with its new tiered governance structure and continue to implement this structure, as we recommended in our July 2012 report;[22]
- continue to implement its IT human capital plan, which DHS believed would take 18 months to fully implement as of June 2012; and
- continue its efforts to enhance IT security by, among other things, effectively addressing material weaknesses in financial systems security, developing a plan to track and promptly respond to known vulnerabilities, and implementing key security controls and activities.

Management integration.—DHS has made progress in integrating its individual management functions across the Department and its component agencies. For example, DHS has put into place common policies, procedures, and systems within individual management functions, such as human capital, that help to integrate its component agencies, as we reported in September 2011.[23] To strengthen this effort, in May 2012, the Secretary of Homeland Security modified the delegations of authority between the Management Directorate and their counterparts at the component level. According to DHS, this action will provide increased standardization of operating guidelines, policies, structures, and oversight of programs. Additionally, DHS has taken steps to standardize key data elements for the management areas across the Department to enhance its decision making. For example, in April 2012, the under secretary for management appointed an executive steering committee and tasked this committee with creating a "Data Mart" to integrate data from disparate sources and allow the dissemination of timely and reliable information by March 2013. Further, consistent with our prior recommendations, DHS has implemented mechanisms to promote accountability for management integration among Depart-

---

[18] We are doing this work at the request of this Committee's Subcommittee on Oversight, Investigations, and Management; and Senator Susan Collins, Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs.

[19] GAO, *Federal Emergency Management Agency: Workforce Planning and Training Could Be Enhanced by Incorporating Strategic Management Principles,* GAO–12–487 (Washington, DC: Apr. 26, 2012).

[20] An enterprise architecture can be viewed as a blueprint for organizational transformation and IT modernization.

[21] GAO, *Information Technology: DHS Needs to Further Define and Implement Its New Governance Process,* GAO–12–818 (Washington, DC: July 25, 2012).

[22] GAO–12–818.

[23] GAO, *Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11,* GAO–11–881 (Washington, DC: Sept. 7, 2011).

ment and component management chiefs by, among other things, having the Department chiefs develop written objectives that explicitly reflect priorities and milestones for that management function.[24]

Although these actions are important, DHS needs to continue to demonstrate sustainable progress in integrating its management functions within and across the Department and its components and take additional actions to further and more effectively integrate the Department. For example, DHS recognizes the need to better integrate its lines of business. The Integrated Investment Life Cycle Model (IILCM), which the Department is establishing to manage investments across the Department's components and management functions, is an attempt at doing that. DHS identified the IILCM as one of its most significant management integration initiatives in January 2011. However, the June 2012 update reported that this initiative is in its early planning stages, will be phased in over multiple budget cycles, and requires additional resources to fully operationalize. In September 2012, DHS reported that it has developed draft policy and procedural guidance to support implementation of the IILCM and now plans to begin using aspects of this new approach to develop portions of the Department's fiscal years 2015 through 2019 budget.

DHS strategy for addressing GAO's high-risk designation.—In January 2011, DHS issued an agency-wide management integration strategy—the *Integrated Strategy for High-Risk Management*—as we recommended in our March 2005 report on DHS's management integration efforts.[25] DHS's most recent version of the strategy, issued in June 2012, greatly improved upon prior versions and addressed feedback we previously provided by, for example, identifying key measures and progress ratings for the 18 initiatives included in the strategy and the 31 outcomes.[26] We believe the June 2012 strategy, if implemented and sustained, provides a path for DHS to address our high-risk designation.

DHS can further strengthen or clarify its *Integrated Strategy for High-Risk Management* to better enable DHS, Congress, and GAO to assess the Department's progress in implementing its management initiatives by, among other things: Determining the resource needs for all of the corrective actions in the strategy; communicating to senior leadership critical resource gaps across all initiatives; and identifying program and project risks in a supporting risk mitigation plan for all initiatives.

Going forward, 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. We will continue to monitor, assess, and provide feedback on DHS's implementation and transformation efforts through our on-going and planned work, including the 2013 high-risk update that we expect to issue in January 2013.

Chairman King, Ranking Member Thompson, and Members of the committee, this concludes my prepared statement. I would be pleased to respond to any questions that you may have.

APPENDIX I: SUMMARY OF ACTIONS AND OUTCOMES FOR ADDRESSING THE IMPLEMENTING AND TRANSFORMING THE DEPARTMENT OF HOMELAND SECURITY HIGH-RISK AREA

On the basis of our prior work, in a September 2010 letter to the Department of Homeland Security (DHS), we identified 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, thus addressing the high-risk designation. This appendix provides a summary of the 31 actions and outcomes.

FINANCIAL MANAGEMENT

1. Maintain top management commitment to correcting weaknesses.
2. Address internal control, business process, and systems weaknesses.
3. Commit sufficient resources to implement financial system modernization and complete a full-scope audit of the Department's basic financial statements.
4. Expand scope of financial statement audit to include an opinion on all of the Department's basic financial statements.
5. Sustain clean opinions for at least 2 consecutive years.
6. Comply with the Federal Financial Management Improvement Act of 1996.

---

[24] GAO, *Department of Homeland Security: Actions Taken Toward Management Integration, but a Comprehensive Strategy Is Still Needed,* GAO–10–131 (Washington, DC: Nov. 20, 2009).

[25] GAO, *Department of Homeland Security: A Comprehensive and Sustained Approach Needed to Achieve Management Integration,* GAO–05–139 (Washington, DC: Mar. 16, 2005).

[26] GAO–10–131.

7. Embrace best practices for financial system modernization.
8. Establish contractor oversight mechanisms for financial system modernization.
9. Successfully implement new or upgrade existing financial systems as needed throughout the Department, including the U.S. Coast Guard (USCG), Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE).

ACQUISITION MANAGEMENT

1. Validate required acquisition documents in a timely manner at major milestones, including life-cycle cost estimates, in accordance with a Department-approved, knowledge-based acquisition process.
2. Improve component acquisition capability.
3. Establish a Joint Requirements Council or a similar body.
4. Ensure a sufficient number of trained acquisition personnel are in place at the Department and component levels.
5. Establish and demonstrate measurable progress in achieving goals that improve programs' compliance with the Department's established processes and policies. For major acquisitions, demonstrate that actual cost and schedule performance are within baseline thresholds.

HUMAN CAPITAL MANAGEMENT

1. Implement a human capital strategic plan.
2. Link workforce planning to other Department planning efforts.
3. Enhance recruiting to meet current and long-term needs.
4. Base human capital decisions on competencies and performance.
5. Seek employees' input to strengthen human capital approaches and activities.
6. Improve scores on the Office of Personnel Management's Federal Employee Viewpoint Survey.
7. Assess and improve training, education, and development programs.

INFORMATION TECHNOLOGY MANAGEMENT

1. Demonstrate achievement of stage 4 of GAO's Enterprise Architecture Management Maturity Framework (that is, completing and using an enterprise architecture for targeted results).
2. Establish and implement information technology (IT) investment management best practices.
3. Establish and implement IT system acquisition management processes.
4. Show progress in implementing the IT strategic human capital plan.
5. Demonstrate for at least two consecutive investment increments that cost and schedule performance is within the established threshold baseline for major investments.
6. Enhance the security of internal IT systems and networks.

MANAGEMENT INTEGRATION

1. Implement actions and outcomes in each management area.
2. Revise management integration strategy to address characteristics we previously recommended, such as set implementation goals and a time line to monitor progress.
3. Establish performance measures to assess progress made in achieving Department-wide management integration.
4. Promote accountability for management integration among Department and management chiefs through the performance management system.

Chairman KING. Thank you, Mr. Maurer.

Now I will recognize myself for questions. I would ask this question of each of you. Mr. Baker gave the Department an A as far as thinking seriously about keeping terrorists out. I would like to ask each of you, though, how effective do you think DHS has been in making itself part of the counterterrorism community, the intelligence community, and receiving the cooperation from the other big players?

What appeared to be my personal experience at the time, at least anecdotally, they were not getting the respect early on. They were

considered, you know, the new kids on the block. Has that improved, and how well-integrated are they into a cohesive counterterrorism system?

Mr. Skinner.

Mr. SKINNER. I do agree that early on they did not get the respect that they should have. At the time I left, I think they were still facing challenges with bringing something to the table, so to speak, in the intelligence community. A lot of this dealt with the simple issues of trust. Other issues were just the mere nature of what they were bringing to the table.

It was historic data. It wasn't something, a strategic dialogue, as to where the challenges were. I think someone hit on this earlier today. That we need to do a better job of actually stepping back and thinking the what-ifs that can occur in this country. Also the things that we can be doing better with regard to infrastructure.

So in my assessment, I think we have a very, very long way to go yet in the intelligence community as far as being a major player, at least at the time I left about 18 months ago.

Chairman KING. Thank you.

Secretary Baker.

Mr. BAKER. Well, I used to say that—at the beginning of DHS, your assessment is quite correct. I once described hiring Charlie Allen as the equivalent of the Mets hiring Casey Stengel. It gave us more credibility than we had before, but we still have a long way to go.

DHS is an unusual participant in the intelligence community. There are a lot of participants who are basically takers of intelligence and analysts of the intelligence that they get. Then there are some very big producers of intelligence. DHS is neither of those things. It does analyze intelligence, and it does produce intelligence of a sort. Particularly travel data.

That has proven to be increasingly useful. So my sense is that, indeed, there is a little bit of tension between them and NCTC over who is in charge of gathering and using this data. You know, if you have turf tension that suggests you are contributing something that somebody else would like to be contributing.

So I think they have moved forward substantially. One area they are not yet maximizing their opportunities in is cyber, where we know a lot about the attackers. We learn that by using law enforcement authorities. DHS has all these law enforcement investigators, Secret Service and ICE, that should be carrying out law enforcement investigations strategically to learn more about our attackers and then embarrass them as dramatically as possible.

My sense is that the law enforcement guys are all overdoing their investigations without a lot of coordination and a lot of strategy from NPPD and the cyber operations. We could contribute more if we were a little more strategic about how we used our law enforcement resources.

Chairman KING. Thank you.

Mr. Cilluffo.

Mr. CILLUFFO. Clearly, intelligence is the lifeblood for our campaign against terrorism in all facets. I would argue that I probably take a less positive view in terms of where the Department is writ large. First, I don't think we have the equivalent. We all know Na-

tional intelligence estimates in terms of racking and stacking capabilities of our adversaries overseas.

We have intelligence estimates that look at threats to the homeland. But what do we have where you have a legitimate homegrown threat? The foreign-domestic divide is blurring today. Social technology and everything else makes it very difficult. The word over here has an effect over there, and vice versa.

So I would argue the emphasis should be pushing out our capabilities to support and enable our fusion centers on the front lines. State and local law enforcement is ultimately best positioned and, in many cases, most competent to deal with these issues.

The joint regional intelligence groups that the FBI is standing up, we have got to find ways to make sure that all these pieces can, in fact, come together. To take National data, to put it into local context. Ultimately, that is translating that data for our State and local authorities who are best positioned to address these issues.

On the cyber side, we have a long ways to go. I mean, if you look back since 9/11, I would argue the greatest breakthroughs which no one is really talking about in our counterterrorism efforts have been the synchronization of Titles 10 and Title 50; basically, where the intelligence community meets the defense establishment.

Cyber. This is an area where we clearly need to look at some of those same synchronizations of authorities and capabilities. Doesn't exist at the State and local. Then when you start looking at the homeland, in particular, I think Stewart captured it. NSA has got the capability, DHS has the authority. NSA doesn't have many of the authorities, and DHS doesn't have many of the capabilities.

How do we start bridging that gap in a way that is true to who we are as a country from a privacy perspective? I think that is the big issue we are all struggling with right now.

Chairman KING. Thank you.

Mr. Maurer.

Mr. MAURER. Yes. Mr. Chairman, I mean obviously, over the course of the last decade there have been a number of substantial changes in the overall structure of the intelligence community. I mean, sort of operating in parallel with a stand-up in operation of DHS was the creation of the NCTC, the standing up of OD&I, the fundamental restructuring and refocus of the FBI.

All these things were happening simultaneously. DHS is clearly at the table as part of this on-going effort. I wouldn't characterize them as playing their leading role. In some respects, appropriately so. FBI is late on some things, for example. We issued a report earlier this morning looking at DHS's central efforts to improve information sharing of terrorist-related information.

What we found there was encouraging. We think that DHS is on a good path on that front. They have shown good leadership. We are concerned about their lack of metrics to be able to establish whether or not they are making progress towards their goals. But we think they are off to a good start in that respect.

So we will be certainly watching that area, as well. That is another one of our high-risk issues, and DHS is one of 5 main agencies that play in that realm.

Chairman KING. Thank you.

My time has expired. I would ask you if you could get back to me in writing. I have two quick questions. No. 1: How significant is it that the Saint Elizabeths project has been pushed back? How important is it for the Department to have, you know, one coherent central location?

Second: Is there any way that the progress of DHS could be compared to the growth of the Defense Department after World War II? Are they on the same path?

With that, I yield to the gentleman. If you can get back to me in 30 days, in writing, I would appreciate it.

The gentleman from Mississippi.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Some will argue that the direction of this Department mirrors the direction it receives. Part of that direction comes from Congress. I have shared with you my concern about jurisdiction. But since we have four very qualified individuals to talk about the subject of jurisdiction and the Department, can you just share individually whether or not you believe it is a good thing for Congress to vest jurisdiction for DHS within one committee like a number of other departments have?

Agriculture, just to talk a little bit about one, there are some small pieces elsewhere. But primarily, jurisdiction is there. I will start with you, Mr. Skinner.

Mr. SKINNER. Absolutely. My own experiences when I was the IG at DHS, people talk about over 100. I dealt with about 88 committees and subcommittees. This is very time-consuming, resource-intensive. We receive, constantly, mixed messages as to the direction the Congress wanted the Department to go.

It created, in my opinion, a lot of problems. Not only for our office, but this is also compounded when you look at it from a Department-wide perspective. Having to answer to so many different committees, so many different directions. The time spent, I think, can be better spent in building a better Department.

But yes, absolutely. I think it would be very worthwhile if we could consolidate some of this oversight into one committee.

Mr. THOMPSON. Mr. Baker.

Mr. BAKER. I completely agree. It is a sign of lack of seriousness that the Congress did not accept even the 9/11 Commission recommendations on this regard. It is very disappointing that it has continued as long as it has, very strong.

I do agree. Imagine trying to run a company and you have 88 outside boards of directors you are held accountable to, none of whom agree in the common end-state. Well, everyone agrees that we want to make the country more safe, but with changes.

I think it is debilitating. I don't think the Department can mature when it has so many different approaches in terms of oversight. The big issue, I would also suggest, is to be able to align budgets to priorities. You have got to also look at the appropriator-authorizer connect, which—I know, I chuckle myself.

I sometimes say we have three parties in this country—Republicans, Democrats, and Appropriaters. But at the end of the day——

Mr. THOMPSON. You are correct.

Mr. BAKER [continuing]. That is a big issue.

Mr. CILLUFFO. That has certainly been an issue that DHS has—been a burden for them from the time the Department has been created. But I think as you know that, you know, GAO works for the Congress as a whole. Obviously, we are strong advocates of very aggressive and hands-on oversight.

So we don't take a position on how Congress divides up its jurisdiction, other than to say that we are there to support making those decisions. So if there is any information we can offer to help with that, we would be glad to offer that. I will say that this problem is not necessarily unique to DHS, but it is probably unusual relative to other departments in the Executive branch.

Mr. THOMPSON. Thank you. I would like just to go on the record in support of what Mr. Baker and the others have said. That the 9/11 report, Commission report, this is really the only thing that is still left outstanding. Is that somehow we all agree that it is outstanding, but we can't agree to do it.

I think that is a failure on Congress' part to step up. I will just say for the record again, Mr. King—whether you are Chair or I am Chair—we need to send that letter again to our leadership, jointly signed by us, saying it should be done and already has been made part of the record. We agree on it.

I look forward in January to authoring or coauthoring a letter indicating a continuing interest on our part for that consolidated jurisdiction.

I yield back.

Chairman KING. The Ranking Member yields back.

I recognize the gentleman from Alabama, the subcommittee Chairman, Mr. Rogers.

Mr. ROGERS. Thank you, Mr. Chairman.

It is good to have Mr. Skinner and Mr. Baker back before us, as they have been many times in the past. I look forward to hearing from our other witnesses. As you all are aware, I chair the TSA subcommittee. We have held, as a part of our hearing process, three hearings on the procurement acquisition process, which has a problem in TSA. But it has a problem Department-wide, as you all know.

GAO just released its most recent report examining this acquisition process. One of the most disappointing facts, which we also found in our hearings, was that most of DHS's major programs reported their planned capabilities changed well into the procurement process. Which obviously costs money, but not just for the Department. But it costs money for the private sector.

When you throw out these requests for proposals without talking to anybody first about what is possible, and then when they come back and say, "Well, we can't do that, but here is what we can do,"—and they have spent several hundred thousand dollars—you say, "Well, that is not what we want," and they pull it back, it is completely unfair to the private sector.

But it also doesn't help us achieve the goals that we are trying to achieve with the Department. I am interested in your thoughts on what we can do to remedy that. What is practical?

Let us start with Mr. Baker.

Mr. BAKER. I will not pretend to be an acquisition expert. But my overall view of the acquisition process of the various parts of

the Department is, this has turned out to be something that only a truly mature agency can do well. CBP certainly has problems, but has managed its procurements better than most of the components of the Department.

TSA, as a new agency, doesn't have the kind of depth of staff and experience to do it as well as CBP.

Mr. ROGERS. Right. Well, that is one of the things I have mentioned to them in the hearings, is you are exactly right. A mature department does it well. And the best example is DoD. They found all the potholes in the road, and they know how to get around them.

I have urged TSA and DHS as a whole to model their process after DoD, and they pushed back hard against it. I don't understand why.

Mr. BAKER. You know, it is the process, it is certainly true, where DoD has been in every pothole that you can find out there. Part of it is just personnel. You need personnel who have been doing this and made some mistakes, and understand how those mistakes are going to play out, and who are not wooed away by contractors to get new business in the future.

I have often thought that we ought to find a way to penalize people who hire our procurement officials in the first 5 years of their service. Because part of the problem is having a real depth of staff.

Mr. ROGERS. Anybody else? Mr. Maurer.

Mr. MAURER. Yes, I think the first thing that DHS needs to do is just follow their own policies and procedures on acquisition. One of the things we found in the report that was issued yesterday was that we actually gave their policies pretty good marks. Their best practice, the problem has been they haven't been consistently following them. If they followed their own rules they would have better outcome.

Mr. ROGERS. Why do you think that is?

Mr. MAURER. Well, I think in the early years of the Department, and it continues even today, there is an overriding sense of urgency, which is important. It is part of their mission. But it leads to——

Mr. ROGERS. Purchasing puffer machines.

Mr. MAURER. Puffer machines that don't work. It leads to rushing to failure. There has been a whole host of those. SBInet and ASP and CAARS. There is a whole alphabet soup of failed acquisitions that DHS has had over the years. This report is the latest example of that.

I know the subcommittee—Mr. McCaul's subcommittee—tomorrow is having a hearing on this to talk more in depth. So I think, yes, first-off DHS needs to follow their policies. I think they have some real shortages in terms of qualified staff to help oversee and review these acquisition programs.

The third issue they really have to come to terms with is that they probably signed themselves up to purchase more acquisition programs than they are likely to be able to afford in outyears. I mentioned in my statement, there is almost $170 billion in sort-of total life-cycle costs.

That is a rough guess. I mean, they don't really know what they have signed themselves up for. If we are going to continue to face

tough budget times, they are going to have to make some really hard decisions on where they are going to put their resources.

Mr. ROGERS. I agree. One of the things I have pushed them to do, though, and it is hard to get them to do, is to start conversing with the private sector in advance. To call the private sector in, do a notice on FedBizOpps or whatever. Bring them in, and say, "Listen, these are the things we are trying to accomplish. What is possible?" Get some dialogue going.

Yes, sir.

Mr. CILLUFFO. Mr. Rogers. Beyond simply as it affects TSA, but generally speaking, metric performance measures. I don't mean to get too philosophical, but at the end of the day what gets measured gets done. But are we measuring what matters? It is that second set of questions that I think you can see improvement in the future.

Wherein the Quadrennial Homeland Security Review aligns with a bottom-up review so you can actually—a policy without resources is rhetoric. But if you can actually match up the priorities from a budgetary standpoint, that is kind of the way the Department of Defense does it with the Palm process and with the QDR.

One thing I might note though, that it took the Goldwater-Nichols Act to be able to really prioritize those needs that were purple, that were across services, that were unique beyond any particular military service. The Department doesn't have a COCOM-like structure. Maybe it should. That is a different set of questions. But it doesn't at this point.

Mr. ROGERS. Excellent. Thank you.

I yield back.

Chairman KING. The gentleman yields back.

The gentleman from Michigan, Mr. Clarke, is recognized for 5 minutes.

Mr. CLARKE of Michigan. Thank you, Mr. Chairman.

Just to all of those who are testifying, my major concern is about the security of our power systems, our power grid, or airports, especially our municipal drinking water and sewage systems. A cyber attack on the industrial control systems that govern these assets could have a devastating impact on areas like metropolitan Detroit, especially if there was a cyber attack against our municipal drinking water and sewage system.

If any of you have some thoughts on the type of policies that we could implement here to better protect the American people from such a cyber attack, that is information I would like to hear. I do have some specific questions. One issue, raised by Mr. Baker, about the role that private companies who are victims of a cyber attack could play in terms of funding Federal investigations into those attacks.

Also, Mr. Cilluffo raised the issue of Iran and Hezbollah. Are there any specific instances or concerns that we should have regarding Iran and Hezbollah regarding a cyber attack on our country?

I yield back my time.

Chairman KING. The gentleman——

Mr. CLARKE of Michigan. Well, I would like to get a response, and then I yield back my time afterwards.

Mr. BAKER. In terms of industrial control systems, you are absolutely right that practically everything that civilized life in Detroit or any other American city depends on is an industrial control system. Those systems, as the Stuxnet attack on Iran's Natanz enrichment facility shows, are vulnerable to attacks that can break the systems.

No major city is going to survive in an orderly fashion if it has no power and no water and the sewers are not functioning properly. You can break all of those things with a properly designed attack. To prevent that, we need to make sure that our systems, to the extent possible, have been pulled off of the internet and that there are not internet connections.

We need to talk to the software manufacturers and hold them to high standards in terms of how secure those systems are. They have never been secure because they didn't think they were connected to the internet. They are now discovering that they are. The hardware in those systems is also not secure, and we need a research agenda that will improve the security of the hardware.

Finally, in my personal view we are probably putting far too much emphasis on smart grid deployments today. We talked earlier, Mr. Maurer talked, about rushing to failure. Smart grids are connecting our power systems, and they offer some real savings. But they are connecting our entire power system to the internet in ways that we could end up regretting.

So those are all things that I would suggest we begin immediately to pursue. I will come back to the private-sector issue if others finish in time.

Mr. CILLUFFO. Mr. Clarke, thank you for your question. I mean, this is a multifaceted set of issues. Clearly, we have seen attempts, and successful hacks, on supervisory data and acquisition systems. The underpinnings of our critical infrastructure is not only overseas, but those attempts are spiking domestically, as well.

So in terms of critical infrastructure, yes. But I think you have got a bigger issue. Back to some of the acquisition questions, we haven't baked security into the design of our architectures. That is why I think, rightfully so, the House Intelligence Committee is asking very tough questions vis-a-vis Huawei, ZTE, and anyone else who could potentially have access to our backbone, our very critical infrastructures, that are most significant for computer network exploit, espionage, or potential attack.

More needs to be done there. We have got to figure out what are the right carrots and what are the right sticks. We have talked a lot about the sticks, but I think there are some carrots; tax incentives, liability protections, if you meet a certain standard in BAR. Which I think should be initiated by a third party. I call it a Good Housekeeping seal of approval.

So it is looking at what are the right carrots and sticks. Some critical infrastructures are more critical than others. Those that really affect our ability and could impede our ability to project power, deploy forces and, from a National security standpoint, I think take on a different set of issues.

Very, very, very briefly on Iran. Yes, we have seen a lot of activity in this space. I recently testified—I see Mr. Lungren here—before one of his committee hearings specifically on Iran before all

these unhelpful leaks in terms of what we have seen on the cyber side. They have stood up a cyber army, the Baseez and some of their proxies have been involved. There is a cyber Hezbollah that is involved in primarily intelligence collection.

So there is reason to be concerned. There are attacks going on as we speak on some of our banking sectors that some people aren't sure where they are necessarily generating from; notably Bank of America, Chase, and others. So I think that is an area we need to be concerned about.

But let us not treat all attacks the same. Hacking a website is like graffiti in cyberspace. It is bad, but it is not the same as attacking the very critical infrastructures or damaging the data that those systems run. So we have got to take some of those issues into consideration.

Finally, there were attacks this summer on Saudi Aramco and on Qatari RasGas. To me, this is where I was talking about what sorts of products NPPD and INA could provide to the critical infrastructure owners. They should have taken those lessons learned and be able to share some of the signature data with our own critical infrastructures.

I might note that a big thing I have been pushing is the Defense Industrial Base pilot, which right now is primarily focused on the defense contractors. I really feel that should be expanded to our critical infrastructure owners and operators; at least the most critical infrastructure owners and operators.

Mr. CLARKE of Michigan. Mr. Chairman, if we do have time I would like Mr. Baker—the opportunity to——

Chairman KING. Actually, we are running on this. I appreciate it, but let me just say I want to thank you for your service on the committee, Mr. Clarke. No one knows what the future holds, but it has been a privilege having you work with us on the committee. Even if you are on that side, and ask some tough questions sometimes.

Mr. CLARKE of Michigan. It is an honor to serve our country here, and it is an honor to serve with you in this panel. Thank you.

Chairman KING. Thank you.

The gentleman from California, our leader on cybersecurity, Mr. Lungren.

Mr. LUNGREN. Thank you very much. Thank the panelists.

I hope I am not contrarian in this. I have been on this committee for 8 years now, and been part of the oversight for the Homeland Security Department. Frankly, I think they are better now than they were back then. I think there has been improvement, there has been some maturation.

I guess the question is: How far along are we in the maturing process? When we compare this to DoD, as was mentioned, it took a long time for us to have the reorganization of DoD to get where we are today. So I, frankly, have seen what I consider to be improvement.

I believe we are safer today because of DHS, even with all the warts and the shortcomings that we have. So I wanted to start with that.

The second thing I wanted to say is fusion centers. We have a fusion center in my district, which I have been out to see any num-

ber of times. I am impressed by the level of cooperation, collaboration, exchange of information and respect for all the participants—local, State, Federal, including DHS.

Mr. Baker, have you seen that? What I see in the Sacramento region, is that the same as you have observed or that you have been made aware of around the country?

Mr. BAKER. Yes, there are some very successful fusion centers that are doing great work and that have really built deep relationships between DHS and local and State authorities. I have had people say if you have seen one fusion center you have seen one fusion center. They are very variable, and not all of them are as successful as the one in your district.

But I think they have turned out to be an enduring institution. We may end up seeing consolidation or rationalization of some of them as the budget gets tighter. But it seems to me they have been a very valuable way for DHS to actually make a difference in local policing.

Mr. LUNGREN. See, that is one of the concerns we have. When we look at budgets, there are those who look at things like that as the first thing to go. I don't think it ought to be the first thing to go. I think it ought to be one of the things that we try and make even better. Because in the area of terrorism, as in so much other things, much of the intelligence is gathered by people who weren't looking for terrorists as their first objective.

Mr. BAKER. Right.

Mr. LUNGREN. There are so many more eyes and ears with local law enforcement than there are Federal agents. Part of our job is to make sure that we give the expertise, share the expertise, on the Federal level with those at the local and State level. Then, with the analysts—perhaps they are Federal analysts, perhaps they are analysts that come from other departments—but utilize that, that ability.

I fear that when we run into these tough budget times that is the first thing to go because it is not a fancy gadget, it's not a new thing that comes out of S&T, even though I want things to come out of S&T. So I am concerned about that.

In the area of cyber, one of the concerns I have had has been the tremendous personnel turnover we have seen within the cybersecurity mission within the Department. At the same time, I have been impressed most recently with an added robustness of that element of DHS. In part, because of the infusion of a good number of people from the private sector.

So two questions for you, Mr. Cilluffo, and also Mr. Baker: What is the basis of the difficulty for us keeping people in the cybersecurity arena in DHS, No. 1? No. 2, do you think the failure of the Congress to get a statutory authority and an institutionalization of the lines of authority within the Executive branch on cybersecurity is, in fact, a serious problem? Or is it just something we can take care of by way of Executive Order?

Mr. Cilluffo.

Mr. CILLUFFO. I will start, and I am just going to say one thing on fusion centers. Because we have done a number of surveys, the first surveys, to try to bring a little bit of science to the art of intelligence. I agree with your position 100 percent.

The one thing I would note that they are lacking, and the majority of them suggested as much, was analytical tradecraft and capability, No. 1. Second, their ability to do threat reporting on the cyber side is weak, and they need to build that up.

But to your question on cyber retention, it is a huge issue. Not only at the Department of Homeland Security, but across the Department of Defense and the intelligence community. Because you have so many greater opportunities in the private sector. Not only financial, but sometimes less bureaucratic. One of the things I think we need to start thinking about in terms of authority is our active defenses, where you give other entities the ability to respond in real time, in certain circumstances, in accordance with our laws.

So I don't think an Executive Order—I mean, this is an issue that is so important for our country, it is so important for all branches of Government to be able to acknowledge and recognize that this is a significant set of issues. I don't think you can just pay for it forward by Executive Order. I think it requires a debate, it requires a discussion.

It is extremely important, looking to future, that you—I don't think you can promulgate it through an Executive Order alone. I think Congress has not only an opportunity, a responsibility, to address these issues.

Mr. BAKER. On personnel, look, this is a hot field and people who do well in it in Government are going to get lots of job offers. We do need to face the fact that we will have turnover at some point. I will note that NSA, where I have also worked, has addressed that issue by and large as a culture where they expect people to come in and spend 25 or 30 years doing what NSA does. They get some very talented people.

They lose people, but they have held onto their people better than DHS cyber has. My suggestion would be, on this as on many other things, DHS needs to be borrowing personnel and capability from NSA, bringing them over, making them part of the career progression within NSA so that they can get the benefit of the talented folks that NSA has.

On the question of Executive Order versus legislation, legislation would be better but I am a realist. I actually think the Homeland Security Act gave a lot of authority, at least within the civilian arm of the Federal Government, to DHS. What we have seen is, the President by and large seems prepared to back that up by saying no, I really want you to do what the Homeland Security Act conveyed to you.

That is progress. So I have supported an Executive Order, I think it is a good idea. There are things that can't be fixed. The Rogers bill, CISPA would be a much better solution than any private or Executive Order solution to the information-sharing problem. I frankly think, though, we are in for a period of a year or more in which nothing is going to happen in Congress so we need to be looking at everything that can be done within the Executive.

I don't think we have gotten to the end of the things the administration can do to improve cybersecurity.

Chairman KING. The time of the gentleman is expired.

The gentleman from New York, Mr. Turner. I am sorry, how did I forget? Here I am talking away to the temporary Ranking Member, who has ascended very quickly to the throne.

The gentlelady from California, who has been a very close bipartisan worker on this committee, Ms. Hahn.

Ms. HAHN. Thank you, Chairman King. I will start by adding my shout-out to my colleague from California, Mr. Lungren, on the necessity of our fusion centers. There is one in the Los Angeles region, as well, that is very significant.

I would dare say many of the plots that have been foiled over the last years were a result of the information that was cobbled together in our fusion center. I think we, as Members of this committee, ought to be very clear and very precise in advocating for the continence of our fusion centers.

I have appreciated the gentlemens' testimony, and your knowledge about our Department of Homeland Security and the future. I have a district that borders the largest port complex in our country, Los Angeles and Long Beach. To that end, I have been concerned about port security.

In fact, my very first hearing here in the Homeland Security Committee was the 9/11 report card. At that time, it had come out that probably we were a little lacking. I would like to hear Mr. Baker's grade for port security in this country.

To that end, I will say thanks to Chairman King, and a real bipartisan support. I was able to pass my first bill this year, on asking the Department of Homeland Security to report back to Congress on assessment of our port security. I would love to hear your analysis of how we are doing.

I tend to think it is still a very vulnerable entryway into our country through our Nation's ports. Specifically, I would like to know, generally, how you feel about that. But specifically, speaking of managing our resources, I have heard from a number of ports across this country that the port security grants, which I am a big advocate of.

We have done things in this committee to continue port security grants. But some of the deadlines, some of the requirements, some of the, you know, burdens that, apparently, we are putting on port authorities to actually use these port security grants in an efficient way are hindering what I believe ultimately is the securing of our Nation's ports.

So I would love to hear your assessment specifically of port security, and how we are managing our port security grants.

Mr. BAKER. So I can't give you much useful information about the grant management because I think I am out-of-date on that. I did participate heavily in the Port Security Act process and the implementation of that, and it's been continued by the next administration.

On the whole, I would give that effort about a B. I think, given the amount of attention that has been put on that and the number of authorities—not just CBP, but also Coast Guard, that are available—the Department has done a reasonably good job of trying to improve port security. You know, obviously it has not been able to move inspection for nuclear weapons overseas the way one would like, and that isn't going to happen anytime soon.

Not because of incompetence on the Department's part, but because, you know, we have to persuade our negotiating partners to do that. One of my biggest worries is that if we are looking for nuclear weapons, which is a fundamental part of our port security program, that may be smuggled into the United States we have pretty good mechanisms—not perfect, but pretty good mechanisms—for identifying those weapons if they come in in containers through the ports.

We are much less well-protected against the possibility that someone will put that into a private jet and just file a plan for Teterboro and never get to Teterboro. Just set it off before they land it in the United States. We need an approach to nuclear weapon smuggling that looks not just at ports, but at all the ways people might smuggle stuff in.

The joke is, the best way to get it in is to wrap it in a bale of marijuana. We need to be looking at all of those. I think actually we have done a better job of securing our ports against that threat than most of the other mechanisms by which people would bring a nuclear weapon in.

Ms. HAHN. Any other members of the panel want to speak on port security?

Mr. MAURER. We issued a report specifically on the Port Security Grant Program about a year or so ago, and highlighted some of the issues you pointed out. Specifically, it takes too long for the money to flow out to the actual recipients. I think the good news there, in a nutshell, is that FEMA and DHS are taking actions to address our recommendations.

My understanding is, they are starting to make progress on that. So that is good news. The second point, real quickly, is, one of my colleagues from GAO, Steve Caldwell, recently testified on the overall state of port security. I think we would agree with Mr. Baker's assessment. Generally speaking, that has been one of the relative areas of success for DHS over the course of the last 10 years.

Ms. HAHN. Thank you.

Mr. CILLUFFO. A very general point. Smuggling is smuggling is smuggling is smuggling, whether it is drugs, weapons, people, or whatever illicit or even licit goods in tough areas. So one area where I think beyond just ports that we need to be doing more is we are seeing hybrid threats. Is it terrorism, is it crime, is it this, is it that?

At the end of the day, I think there is some real opportunity between the counternarcotics community and the counterterrorism community to further cooperate on some of these issues. Because again, the routes are going to be the same. The TTP, the terror tactics, might be the same. So how do we start bringing those worlds together?

Ms. HAHN. Thank you.

I yield back.

Chairman KING. The time of the gentlelady has expired.

Now the gentleman from New York. Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

One of the most important elements here in counterterrorism is intelligence. If you could give us a minute, maybe, on what you think can be done and improved for intelligence sharing. I am par-

ticularly taking this from a view as a New York representative, which comes both ways.

The NYPD, as you may know, has its own intelligence operation. If you have a thought on the efficacy of that, and what are the things that could be improved upon in the next year or two. If you would be kind enough to begin, Honorable Skinner?

Mr. SKINNER. I would be happy to. That is one of the things. I think the biggest concerns I had dealt with the integration of our IT systems and creating a capability to communicate on a real-time basis. The Department, within itself, has problems just communicating across the various component lines.

One of the biggest challenges—and I believe I alluded to this earlier—is our ability to then communicate on a real-time basis with our Federal partners and, particularly, with our State and local partners. The fusion centers, I think, is a good step forward to improving that communication capability. But I still think we have problems with getting access on a real-time basis, giving people the clearances so that they can communicate on a real-time basis, and developing a trust.

Fusion centers, I think some operate very well. But again, we talk about do we need as many as we have? Probably not. Can we do a better job in consolidating those fusion centers and building on a cadre where they are most needed on a risk basis would be, I think, a step forward. But building an IT capability to allow us to communicate, I think, is one step that we need to continue to work on.

Mr. TURNER. How far away are we from that ideal?

Mr. SKINNER. Quite frankly, I think we are very far away.

Mr. TURNER. Thank you.

Mr. BAKER. You know, the New York police department is one of the crown jewels of our counterterrorism effort, and the only non-Federal agency that really provides an alternative model for how you respond to terrorism effectively. I was disappointed to see the Associated Press and a few other folks kind of sniping at NYPD and inviting Federal oversight as a way of kind of making them less effective.

We should have more local law enforcement agencies that were learning from NYPD, that were willing to talk directly to the U.S. intelligence agencies. So I would say they should be a model, rather than somebody subjected to criticism.

On information sharing, let me just highlight an area of information sharing that I think is far worse than the relationship with State and locals. It is information sharing on cyber intrusions where, in fact, law enforcement agencies know an enormous amount about who is doing them, what tactics they are using, why they are targeting people, and who they are targeting.

The targets are in the private sector. The sharing with the private sector at that level of detail, in my view, is nowhere near as good as it with State and locals on the counterterrorism mission.

Mr. CILLUFFO. I think Stewart and I are hanging out too much. NYPD is clearly the gold standard in this business. I might note, though, Ms. Hahn and others that if New York police department is the gold standard, LAPD is the silver standard.

But once you get outside of New York, Los Angeles, Texas and some of these other areas, Arizona, you really have a mixed bag. At the end of the day, that is why I think we really do need to invest in the fusion centers. It could probably afford some culling to be able to build on the best.

The last thing I want is the successful initiatives to be thrown out—the baby thrown out with the bath water—if we see the need to cut, and we are not going to cut the right ones. In essence, you are going to have entities that perhaps ought to be put on life support, and you have got the gems that are going to be stymied.

New York has its own intelligence capabilities. They have an overseas presence. Very few police departments have an overseas presence. So I don't think it is even constructive to compare that—maybe LAPD—with the rest of the country. But as much as can lean forward, enable and support, it has been a target multiple times.

Unfortunately, it is a target almost every day; much of which we don't read about. So I support that 110 percent. One thing on the intelligence picture writ large. I would argue that we need a true domestic intelligence estimate. We don't have regional threat assessments domestically for the Jihadi threat, for Islamist threats. The United Kingdom, for example, does.

I am not suggesting we need a security service or an MI5 in the United States. Actually, quite the opposite. Push the capabilities to our State and local authorities. One area where we are the best in the world, hands down, are JTTFs. But that is only when an investigation is open.

Once we get the blip on the radar screen we are the best, period. But what about in that steady state, to be able to see what that threat environment looks like for the unknown unknowns. That, I think, we still have a lot of work to do. As much as we can invest in our State and local authorities, we ought to.

Mr. MAURER. Very quickly, I think you should know information sharing is one of GAO's high-risk areas. So clearly there is a lot of work that still needs to be done there. We want to see closer collaboration among all the Federal partners and a greater ability to work with State and locals, as well.

Chairman KING. The time of the gentleman has expired.

Again, Mr. Turner will be leaving the committee at the end of the day. I want to thank him for his service. He does an outstanding job, and I want to thank him for his dedication to the committee and to the people of New York overall.

Also, let me associate myself with the remarks of Mr. Baker and Mr. Cilluffo on the NYPD. I just hope that the *Associated Press* and *New York Times* were listening.

With that, I recognize the gentlelady lady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Let me also thank my colleague for his service, as well. I think, as the Ranking Member and the Chairman mentioned at the beginning of this hearing, we are committed in a bipartisan way to the security of this homeland—and, I would like to put on the record—for the greatest country in the world. I heard someone define us as the greatest democracy in the world. I am going to redefine us as the greatest country in the world.

So I am very grateful for our commitment. I also want to associate myself with the comments "maybe one day." I am going to ask for just a yes or no answer. That the streamlining of jurisdiction oversight of homeland security is imperative for a consistent and efficient and effective securing of the homeland.

Mr. Skinner, do you agree?

Mr. SKINNER. Yes.

Ms. JACKSON LEE. Mr. Baker.

Mr. BAKER. Amen.

Ms. JACKSON LEE. Mr. Cilluffo. Do I get it right?

Mr. CILLUFFO. Yes.

Ms. JACKSON LEE. GAO in particular, Mr. Maurer?

Mr. MAURER. You know, we got to be agnostic on that one because we serve the whole Congress. I don't say that to dodge the question, but because I know this has been an issue that has been debated among the Members across the various——

Ms. JACKSON LEE. We will give you a pass.

Mr. MAURER. Okay.

Ms. JACKSON LEE. Let me also indicate that I look forward, if we all return by way of election, to really look at this regional security threat concept. I think that is a very important new note to hear.

I am going to try and ask a number of fast-moving questions, and try to get through all of you. May not, but let me start with Mr. Maurer. I hope you can comment that investing resources, or the utilization of resources funding, is crucial to some of the assessments that you have made.

Do we need to continue the right and reasonable and effective and continued funding for Homeland Security?

Mr. MAURER. Absolutely. You are going to need resources to achieve many of the things the Department wants to do. They are making——

Ms. JACKSON LEE. That are still not done.

Mr. MAURER. That are still not——

Ms. JACKSON LEE. And are crucial to securing the Nation.

Mr. MAURER. Absolutely. They have made good progress so far to date. One of the biggest criticisms we have had of their plans to date, frankly, is the fact that they have resource limitations in executing those plans. Now some of that rests in the Department, quite frankly, and setting priorities on where they are going to spend the money that Congress appropriates to them.

Ms. JACKSON LEE. The border, which is something that I have been particularly attentive to because I come from the State of Texas. Have we made improvements since, for example, 2005? I particularly remember enhancing the Border Patrol agent census, or population; adding more, and giving them enhanced equipment. Has that made a difference?

Mr. MAURER. Yes, it has. There are certainly many more Border Patrol agents on the Southwest Border as well as the Northern Border. DHS continues to invest in enhancing the training that they receive, as well as the acquisition tools and the systems that they use in the course of their job.

We still have a number of concerns about the technology enhancements DHS plans to make on the Southwest Border. The collapse of SBInet was a major failure for the Department, and we are

watching what they are doing on that front very carefully right now.

Ms. JACKSON LEE. I think we would be very eager to know that even though we have the rise of drug cartels, gun trafficking, which we just heard the IG's report that I think I can put on the record. That the attorney general had no knowledge of the gun trafficking and the Fast and Furious issue.

But we do know that there are elements that were not effective. But with all of that, getting those other agencies to collaborate, we can see in the future a secure border or a securer border?

Mr. MAURER. It definitely depends on the execution among the various departments and agencies. That is certainly our hope, and we will be there to provide oversight to help assist the Congress in its own deliberation.

Ms. JACKSON LEE. All right. Gentlemen, I am going to give three questions and I would like you to answer. I see my time is—and I ask the Chairman for an indulgence. They could pick the ones that they would like.

I do want to indicate that I would like to see the CERT1 program improved—I don't think the outreach goes to minority communities sufficiently—and that is the response program during disasters. I think the procurement is way in need of repair in terms of outreach to small businesses.

But these are the questions I would like. We have seen a rash of attacks or threats to universities, bomb threats. I believe we need an ombudsman or a focus inside Homeland Security that is an immediate response team to our universities. Some of these, obviously, are prank calls. Or at least they have been determined as that.

But with the rash of incidences that have occurred, I would appreciate your comment. I would appreciate your comment on the importance of reaching out to Muslim-Americans and retaining and hiring them in the security process. I would appreciate your comment on the importance of homeland security and civil liberties.

Anyone want to start first?

Chairman KING. I would ask the gentlemen if they would try to, you know, give brief answers. Try to keep it in the next 2 or 3 minutes.

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

Mr. Baker, you are up.

Mr. BAKER. Okay. So I would say ombudsman to universities, or at least a place to call after you get a call you can't tell is crank or not, absolutely it is a great idea. It should be part of information sharing. Outreach to Muslims has been going on, should continue to go on and I think, on the whole, has been successful for the Department and the U.S. Government generally.

On civil liberties and privacy, frankly if there were a job I wanted in Government it would be chief privacy skeptic. I think the privacy groups have not, on the whole, treated DHS well or its programs. We probably should be more skeptical about privacy claims than we are.

Ms. JACKSON LEE. All right. Well, Mr. Skinner.

Mr. SKINNER. I have nothing to add to what Mr. Baker just said. Very well put.

Mr. CILLUFFO. Just that I agree on the university side we need a bellybutton. I am not sure exactly how that looks like, but I am standing where I sit. I am at George Washington University now.

Second, in terms of civil liberties, I don't think the debate has been cast as an either/or proposition. I don't think that is healthy. You can, and must, have both. When you start looking in the cyber domain in particular, there are going to be a lot of questions.

But I agree with Stewart. Many of them are red herrings. A lot of them are not necessarily—that is not to suggest we don't take it seriously. We do. But I think most of the people, having been on the inside you hear more from your lawyers than you hear from the ops guys in terms of what it is you can and cannot do.

That creates, to some extent, a chilling effect. Which is why, again, Congress, I think, has an opportunity and a responsibility to address some of these issues and move some legislation.

Ms. JACKSON LEE. You should not take privacy lightly, however.

Mr. CILLUFFO. Absolutely not. It is you build too many walls, the bad guys win by default because our way of life has been lost. That is what we are, is a federalist democracy, of course.

Ms. JACKSON LEE. Mr. Maurer.

Mr. MAURER. You definitely want to consider civil liberties as part of the overall approach to cybersecurity. Absolutely in agreement on that. Outreach to the Muslim community is absolutely vital. I agree with that, as well. I think it is an interesting concept you talk about for an ombudsman, and certainly worth looking into.

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

I yield back.

Chairman KING. The time of the gentlelady has expired.

The gentleman from Texas, chairman of the Oversight Subcommittee, Mr. McCaul.

Mr. MCCAUL. I thank the Chairman.

I want to follow up on something Mr. Lungren talked about. That is, you know I think one of the greatest disappointments I think I, and this committee I think, share in is that the Congress did not pass cybersecurity legislation, which is so important. Every day that goes by without those authorities, more Americans are at risk.

So I hope that if we can't get it done in this Congress we can certainly get it done next Congress. A very small point, and I want to go on to two other points.

But, Mr. Baker, you mentioned an interesting idea. I think part of the problem is the perception that DHS just doesn't have the capability that NSA has. That probably is reality, too. So to put that faith and trust in DHS because I personally think, and I think Mr. Lungren and the Chairman agree, that a civilian authority is the more appropriate in a domestic sense rather than a military.

Now, NSA can work with DHS and that is what you want. But how do you get NSA, you know, capability or NSA employees to come to DHS?

Mr. BAKER. So, in fact, some of that is happening. You know, I am an alumnus of both organizations, and may be the only one who has had a political appointment in both. But I don't think that you can bring staff over from NSA, detail them in. They are oper-

ating under DHS authorities and constraints, but they are bringing a raft of technical capability that otherwise it would be very hard for the Department to hire.

What we need is enough technically competent people at the Department so they feel that they can take advice from NSA employees without fearing that they are getting a whole bunch of policy advice they don't see buried in the technical——

Mr. MCCAUL. I like the detail approach. Because I think, again, they kind of have to earn the respect of the Congress for the Congress to give them those authorities. I think there is an issue with that. I personally think it should be more under civilian control.

So, quickly, to move on, I am chairing a hearing tomorrow—I think, Mr. Maurer, you are going to be there—on acquisition, procurement. You know, we still see all the silos that Mr. Skinner talked about. Yet, you know, it is still a very solid F in terms of the acquisitions. So we don't see—there were these recommendations that were made, you know, several years ago.

But they don't seem to be followed. So you got a procurement process that has become very wasteful in its management. I mean, so overall how do you integrate this management together? But then how do you fix the procurement process? If you could answer it in a fairly short manner I would appreciate that.

Mr. MAURER. Sure, absolutely. First off, I want to give good credit to my colleague, John Hutton. He will be the GAO witness tomorrow at your hearing. So he is taking the lead on this issue at GAO.

But how to address the problem? First and foremost, DHS needs to follow its own rules. They haven't been doing that, that has been at the root of the problem. Second, they do need to do a better job of managing the overall portfolio, and start making the hard decisions and figuring out what they can actually afford out in the future.

But a third issue, they need to do a better job of coming up with life-cycle cost estimates. That sounds wonky and down in the weeds, but what it basically means is figuring out the price tag. What is it going to cost to procure these different systems, and over how many years is that going to take? Until they come to grips with all three of these issues they are going to continue to have problems.

Mr. MCCAUL. Okay. A final a point is, Mr. Cilluffo, you talked about regional threats. I think that is a very smart approach. I led a delegation down to Latin America, and we went to, you know, the tri-border area, a Jewish community center in Buenos Aires. As you know, the Saudi ambassador applied the Quds forces. They were going to hit the embassies—and Israel, Saudi, and Argentina.

So we look a lot at the Middle East, but there is a lot going on right here, too. My kind of nightmare scenario is a strike from Israel, against Iran. With everything that is happening right now already, with these embassies already being targeted, you throw that cocktail on top of everything and it is a Molotov cocktail.

I can see, you know, there will be ramifications to that. There will be a response. I can see the Hezbollah operatives not only there but in this hemisphere which we know are here. I can see them lining up.

So is DHS prepared? Do you think they are even looking at this issue and planning to defend?

Mr. CILLUFFO. Mr. McCaul, you raise a number of very important points. I think as much as you can raise awareness in terms of the challenges you saw in the tri-border area would be helpful to the American people. Because we do have problems on our hands.

It is not just in the tri-border area. Hezbollah has got a presence in the United States. In fact, the Los Angeles police department elevated the government of Iran and its proxies, notably Hezbollah, as a Tier I threat; highest threat level. NYPD has been leaning forward in terms of addressing some of these challenges.

So I don't think it is only in response to some actions that Israel or others may take. I think that you are seeing an uptick in activity that, even short of that, warrants greater concern from the U.S. National security.

Mr. MCCAUL. Then, in closing, I hope the Department is focused on this very aggressively in terms of defending the Nation rather than responding, or reacting to, a crisis.

Mr. CILLUFFO. I can tell you some are. I am not sure that is percolating throughout the entire Department. But I have worked with some folks who are recognizing that as a challenge.

Mr. MCCAUL. I thank the Chairman.

Chairman KING. The gentleman yields back.

I would just point out, as Mr. McCaul knows, and he was part of the hearing, we held a hearing—at least one hearing, full committee also, I think, some subcommittee involvement—on the whole issue of Hezbollah in this country. My impression was the same as yours. It is a serious threat not being taken seriously enough by everyone. By some, but not by all.

With that, the gentlelady from California, Ms. Richardson, is recognized for 5 minutes.

Ms. RICHARDSON. Yes, thank you, Mr. Chairman.

I just have two questions for Mr. Skinner. One, in fiscal year 2011 the Department entered into over 133,000 procurement transactions and over 81,000 thus far in 2012. I am concerned about the oversight of these transactions. On your watch, during the Department, we have obviously heard, and learned of, various problems of the procurement process, including contracts with SBInet, Deepwater, and Federal Protective Service contracts and Guard contracts.

Yet the Department's management budget appears to leave little room for improved oversight during the procurement process. How can you improve upon your contract oversight?

Mr. SKINNER. It is, I think, very basic. That is, increased staffing. Because I think the acquisition management function within the Department when it stood up, and even today, as much as they are trying to build a capability is still grossly understaffed. I think as part of the procurement process, when you develop your strategic plans, your operational plans, as to what you are going to be buying in the outyears and in the current years, that we need to budget in, or factor in, the cost of the total procurement.

Just not the cost that we pay the contractor, but the cost to provide oversight of those contracts. It is all part of the contract administration process.

Ms. RICHARDSON. Has that——

Mr. SKINNER. I do not think that is being done right now.

Ms. RICHARDSON. Is there anything you need us to do to be able to assist you to have that happen?

Mr. SKINNER. The authorities are there, the guidelines are there, the policies are there. They just simply need to be implemented. I think with additional staffing, we could do a better job of managing the contracts as opposed to just simply awarding and then reacting to problems.

Ms. RICHARDSON. Okay. So, Mr. Chairman, if you would be willing maybe the committee would want to consider requesting of the Secretary that as contracts are distributed that, as Mr. Skinner has suggested, that the oversight be included in the overall cost that is being considered.

Then that way, they might be able to have adequate staffing to take control of the taxpayers' money, which I know you and all of us here are very concerned about.

Chairman KING. We will certainly consider that, and I will work with you and your office to try to bring that about.

Ms. RICHARDSON. Thank you, Mr. Chairman.

The second question is: Mr. Skinner, on a scale of 1 to 10, how would you rate the Department of Homeland Security on its cybersecurity efforts? Meaning, where are there improvements most needed from the Department's perspective, and what legislation could we do to help you to better achieve those results?

Mr. SKINNER. First, let me say I am probably the least qualified person to ask that question on this panel. But based on my observations when I was serving with the Department, they are making modest progress through their hiring efforts, their attention to the cybersecurity issues. But on a scale of 1 to 10, I would have to give them something around a 4.

We have a long, long way to go. I think one of the primary things, and it has been repeated several times this morning, is that we definitely could use legislation to help guide the Department.

Ms. RICHARDSON. Okay. Would anyone else like to give a very brief response that wanted to chime in?

Mr. CILLUFFO. Just to piggyback Mr. Skinner's comments, General Alexander, when asked very specifically where the U.S. readiness was on a scale from 1 to 10, said a 3. So it is pretty much in line with some of that thinking. He is the commander of Cyber Command, and director of the National Security Agency.

I do feel this is a big area that the United States—we are not any further along than our homeland community was shortly after 9/11.

Ms. RICHARDSON. Wow.

Mr. CILLUFFO. The difference is, is we know the risks. So I think we have got a responsibility to move.

Mr. BAKER. I can just add, if the people who are attacking us for getting grades from their governments they would get at least a 6. So we are losing ground to the attackers.

Ms. RICHARDSON. Mr. Chairman, I know that when appropriations come forward in the House, typically where we look to add more programs, Members of Congress will typically take money out of the management and oversight or salary bucket of a particular department. Take money from there and, you know, fund for another program.

I would be more than willing to join you of us educating our colleagues that in this particular area of cybersecurity—we can't speak to every area—but the impacts of these cuts to the staffing in particular is really hindering the ability to move forward. If you would like to join me, or suggestions on how we might do that, I would welcome that.

Thank you, sir.

Chairman KING. Be delighted to work with you. The time of the gentlelady has expired.

Before I go on to Mr. Marino, I just want to acknowledge, in the audience, Robert Matticola, who is homeland security director for the New York waterway ferry in New York, and he has held that position since July 2008. It is obviously a job that is in the line of fire, and I want to commend you for your service.

Now the gentleman from Pennsylvania, former United States attorney, Mr. Marino is recognized for 5 minutes.

Mr. MARINO. Thank you, Mr. Chairman. I apologize for being late. I am trying to get to all of my committee hearings today.

Gentlemen, it is a pleasure. As my distinguished Chairman stated, I have been in law enforcement and I have been there for 19 years. So I know what our men and women go through. I have been out there on the front line with them, I have their backs. I have worked closely with all the agencies throughout my career.

You know, it is easy for us and anyone else to Monday-morning-quarterback our men and women and our agents on the line and in the field. Just unfortunate that much of the information and much of our operations—and I still say "our" because I still feel I am part of law enforcement, I will always be—has to be kept close to the chest because we don't want the enemy knowing what is going on out there.

But each one of you can respond to my question, if you would like to. Are our agents, are our people in the field, fully equipped with what they need to do what we expect them to do? Equipment, training, et cetera?

Mr. Skinner, would you like to start?

Mr. SKINNER. I believe because of the rapid buildup within our law enforcement community, particularly with CBP and ICE over the past 5 to 6 years, that we are still behind the curve as far as providing the types of training and the degree of training that they need.

As far as equipping them, I also believe that our infrastructure is trailing our hiring. We are hiring faster than we can build an infrastructure to support them. Third, as far as supervision and management, as we hire so many people so rapidly that brought some of our more experienced—or what we have done is, in essence, taken very inexperienced individuals and put them in supervisory and management roles.

That was the only alternative they had at that time. That does not mean to be a criticism. But all in all, I think we still have to catch up to the hiring.

Mr. BAKER. I don't have anything to add to that.

Mr. CILLUFFO. I would just underscore field bias, field bias, field bias. As much as we can lean forward, if you look at the military community, the intelligence community, and other communities that have gone through similar issues commanders intent; push the capability down to the pointy end of the spear.

In this case, I think the big potential gap is, we need to enhance our analytical capacity so State and local can—so they are not going in with—not blind, but with less vision, given the fog of crises and situations. So push to State and local. That is my one takeaway. DHS's role in that is significant and important, but it is really about looking at State and local authorities as their force multipliers. They are our boots.

Mr. MAURER. I think DHS definitely deserves some credit, particularly in the last couple of years, in coming to grips with its management problems. It gets right to your question. They are trying to do a better job with procurements, they are trying to do a better job with training, they are trying to do a better job with all the different entities working as one unified whole within DHS as well as their interagency partners.

They are definitely not where they want to be or where they need to be, and they fully recognize that. But I am just encouraged by the fact they are paying more attention to sort of these basic fundamental resource and management issues.

Mr. MARINO. I understand that, being in the field, there are many agencies and many different types of work that has to be done. But can you give me a ball-park figure? We talked about training—and behind the curve on that—to adequately train our people on the front lines. Whether it is ICE, you know, whether it is DEA or whoever is—and Homeland Security protecting our borders, or even overseas.

How much time are we talking about for training?

Mr. MAURER. I don't know if you can put an exact time frame or dollar figure on it because training is an on-going thing. I mean, it is not only bringing in new Border Patrol agents. It is continuing to offer training throughout that person's career.

Mr. MARINO. But I mean, you know, bringing someone in initially. I know training is on-going, and should be. But let me put it this way. I don't think there is any agency with whom I have worked where it is a 6-week training course and you are ready to rock and roll.

Is that a correct statement? A significant amount of time is required?

Mr. SKINNER. Absolutely yes, there is significant time required. I almost equate it to like a boot camp. Because when you bring someone in, you are giving them basic training. But as you progress, you are going to have to receive additional training. That training has to be kept up-to-date.

It is just not a one-shot deal. It is constant.

Mr. MARINO. Totally agree.

Mr. SKINNER. So there is a lot—the more investment we make in our training, the better performance we are going to get from our employees.

Mr. MARINO. Thank you, gentlemen.

I yield back.

Chairman KING. The gentleman yields back.

I want to thank all the witnesses for their testimony today. I think this is one of the most thoughtful and substantive hearings we have had. Your testimony was really invaluable. I think as Members of the committee, we often tend to focus on issues that are particularly important to us, a component to the Department that are important to us, or parts of the Department where particular errors have been made.

I think you were able to bring it together today and really show us the Department as a whole, its weaknesses and its strengths. As Mr. Lungren said, I think significant progress has been made. It is important to keep that in mind. But at the same time, we have to, you know, continue to make more progress. Especially address some of the more significant deficiencies.

But at the same time, I think it is important that we let the public know, really, the overall job that DHS is doing. Because too often, when it comes time for budget cuts or whatever, people look upon DHS as not really contributing that much. The fact is, despite its persistence, al-Qaeda has not been able to perpetrate an attack on the scale of 9/11 in the past 11 years. The DHS has been a vital component of that.

So with that, I want to thank you for your testimony. I would also want to thank the Members of the committee who were here today. Some Members may have additional questions for the witnesses, and we would ask you to respond to those in writing. The hearing record will be held open for 10 days.

Without objection from the distinguished acting Ranking Member——

Ms. HAHN. No objection.

Chairman KING [continuing]. The committee stands adjourned.

[Whereupon, at 12:03 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN PETER T. KING FOR RICHARD L. SKINNER

Question 1. Will you please share your views on the importance of the completion of the St.Elizabeths project to the Department's efforts to consolidate operations and its potential impact on the Department's performance?

Answer. In my opinion, the inability of the Department to complete the St. Elizabeths project as originally planned should have little, if any, impact on the Department's efforts to consolidate operations and, most certainly, should not adversely impact its performance. Consolidating the Department's components "under one roof" so to speak is an issue of convenience, not one of performance, particularly in today's IT environment of borderless networks, where any employee should be able to connect with anyone or any information from anywhere, using any device. Housing "people" in one location may make it convenient for officials to conduct face-to-face meetings, but it will not address the real challenges facing the Department, and that is consolidating and integrating management support systems and operations. Consolidating operations and improving performance are "management" issues, not "logistical or housing" issues.

Question 2a. How would you compare the creation and maturation of the Department of Homeland Security to date to that experienced by the Department of Defense in the decade after its establishment?

Do you believe that now, almost 10 years after its creation, the Department should have matured more quickly and its components should be operating more effectively and efficiently?

Answer. While the creation of the Department of Homeland Security may be the largest Government reorganization since the creation of the Department of Defense, it pales in comparison to the enormity of the challenges faced by DoD upon its creation. Accordingly, in my opinion, the Department of Homeland Security has, and should have, matured more rapidly to date than the Department of Defense in the decade after its establishment.

I believe that now, almost 10 years after its creation, the Department should have matured more quickly and its components should be operating more effectively and efficiently. During its first 3 years of existence, neither the Congress nor the administration gave the Department the resources needed to properly support the programs and operations inherited from its legacy agencies. In particular, its management support functions were shortchanged, i.e., the financial, information technology, acquisition, human resources, and grants management functions. During the second 3 years of its existence, both the Congress and the administration increased the Department's funding for its management support functions, but, while making modest improvements, it fell far short of its goal to establish a cohesive, efficient, and effective organization. For example, the Department is still unable to obtain a clean opinion on its financial statements and internal controls; its components are still struggling to upgrade or transition their respective IT infrastructures; resources needed to implement acquisition policies are still lacking; and, it is impossible to determine whether the Department's grant programs are actually improving our Nation's homeland security posture. During the past 3 years, budget constraints have impeded the Department's ability to make any significant headway and build on the modest improvements made since its creation. The Department's new challenge will be to sustain the progress already made and at the same time continue to make necessary improvements.

Question 2b. How much longer is the argument that bringing together so many Federal agencies a legitimate explanation for the Department's shortcomongs?

Answer. Bringing together so many Federal agencies should no longer be a legitimate explanation for the Department's shortcomings. The Department had many opportunities to address its management challenges, but, for a myriad of reasons, it failed to do so. Although some were out of its control, many opportunities were

lost due to poor management decisions or just plain indecision. Unless the Department stays focused on its shortcomings, it will be harder than ever to find solutions to strengthen critical management support functions and, ultimately, to ensure the success of its homeland security mission.

QUESTIONS FROM CHAIRMAN PETER T. KING FOR STEWART A. BAKER

Question 1. Will you please share your views on the importance of the completion of the St. Elizabeths project to the Department's efforts to consolidate operations and its potential impact on the Department's performance?

Answer. As noted in my testimony before the committee, one of the greatest challenges facing the Department of Homeland Security going forward will be developing a framework to enable proper coordination among all of the Departments big and proud components. Department leadership has done a good job at bringing the various components together to respond to major crises, but coordination on day-to-day issues is very much lacking. The St. Elizabeths Campus project, by bringing together the leaders of all of DHS's components under one roof, is critical to addressing this larger Departmental challenge. Placing component and Departmental leadership in the same office space will, I believe, go far in building a unified organizational culture and providing daily opportunities for DHS components to work together cooperatively.

Question 2a. How would you compare the creation and maturation of the Department of Homeland Security to date to that experienced by the Department of Defense in the decade after its establishment?

Do you believe that now, almost 10 years after its creation, the Department should have matured more quickly and its components should be operating more effectively and efficiently?

Answer. The Department of Defense's history illustrates just how difficult integrating all of the components at DHS will be. When DoD was formed in the late 1940s out of the Department of War and the Department of Navy, both of which had been established in the 1700s, DoD at least had the advantage of an existing unified office space and the recent experience of coordinating operations during World War II. All the same, it took years for DoD's leadership to establish its authority within the entire Department. As late as the Cuban Missile Crisis in 1962, Secretary McNamara's authority over the Navy was still in doubt. When the Secretary asked Admiral Anderson:

"what would happen if a Soviet ship refused to stop or resisted boarding. Anderson answered angrily, 'This is none of your goddamn business. We've been doing this since the days of John Paul Jones, and if you'll go back to your quarters, Mr. Secretary, we'll handle this.'"—Dobbs, One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War (2008).

I'm quite confident that today, just 10 years into the Department, no DHS component head would dare to say that to the Secretary of Homeland Security, even though several of the components have been carrying out their missions as long as the Navy.

Question 2b. How much longer is the argument that bringing together so many Federal agencies a legitimate explanation for the Department's shortcomings?

Answer. The understandable challenges of post-merger integration at DHS, however, do not excuse component or Departmental leadership from fulfilling their missions. Responsibility for building the Department's capacity and accomplishing its objectives still has to lie with individual components or offices at DHS. To the extent that individual parts of DHS are underperforming, they should be held individually accountable for making the necessary programmatic and staffing changes to turn the Department around.

QUESTIONS FROM CHAIRMAN PETER T. KING FOR FRANK J. CILLUFFO

Question 1. Will you please share your views on the importance of the completion of the St. Elizabeths project to the Department's efforts to consolidate operations and its potential impact on the Department's performance?

Answer. While I am not fully up to speed on all of the developments surrounding the St. Elizabeths project, I am of the view that consolidating operations in a single location could have a range of salutary benefits, including the prospect of synergies between and among offices and individuals that derive simply from physical proximity (through increased daily interactions, etc). In addition to tangible advantages, such as the facilitation of communications between and among offices and individuals, there are likely to be intangible advantages as well, such as a greater sense

of unity of mission and the boost to morale that may occur as a result of co-location (which may engender a greater sense of esprit de corps).

However, there are a range of factors that may affect the timing of completion of the St. Elizabeths project, including of course the current budgetary situation; hence it may be some time before the project's benefits come to fruition. Let me underscore, though, that future developments should not come at the expense of the Department's operating budget. Having said that, perhaps the most forceful and vivid argument in favor of timely completion of the St. Elizabeths project is as follows: Just imagine the Department of Defense without the Pentagon, or the CIA without the George (H.W.) Bush Center for Intelligence in Langley, Virginia.

Question 2a. How would you compare the creation and maturation of the Department of Homeland Security to date to that experienced by the Department of Defense in the decade after its establishment?

Do you believe that now, almost 10 years after its creation, the Department should have matured more quickly and its components should be operating more effectively and efficiently?

Question 2b. How much longer is the argument that bringing together so many Federal agencies a legitimate explanation for the Department's shortcomings?

Answer. There are certainly some similarities between the Department of Homeland Security and the Department of Defense in the context described above (creation and maturation a decade after establishment). In both instances, it took time to synchronize each of the following—operations, planning, strategy, etc.—from an organization-wide perspective. Likewise, both cases evidence the pace at which a cohesive organizational culture takes shape; this is not something that appears or grows overnight.

Notably, for the Defense Department, thinking purple is a mindset and action posture that took time to cultivate and instill; and even then, in order to genuinely root itself required legislation (the Goldwater-Nichols Department of Defense Reorganization Act of 1986) and a supporting incentive structure that tied education and training, interagency rotations, promotion and professional advancement to "jointness." Given that DHS initiatives in the realm of education and training, for example, remain nascent, it is no surprise that there are still some bumps in the road when it comes to execution and implementation in an effective and efficient manner. On paper and in principle, 10 years may seem like a long time. Yet that first decade of DHS' existence has been marked by unprecedented and almost constant challenges. The fact that DHS was created at a time of crisis, and also evolved in such a climate, suggests that an extended interval may be warranted in order to judiciously evaluate its progress.

Having said that, DHS as an enterprise needs a sharper focus and a greater prioritization of its activities, to include more and better alignment of budgets with priorities. In addition, DHS has yet to define its Office of the Secretary, writ large. Compare the Defense Department, whose counterpart Office for Policy (OSD/Policy) for example, serves a robust and genuine Department-wide, cross-cutting function. This is the bar which DHS should, and must, aim to reach.

Indeed, the Defense Department today is the gold standard when it comes to plans and planning, after-action reflection, and a range of other matters. Both regional and functional/thematic approaches to a range of complex challenges are successfully integrated and incorporated into outputs, including budgeting for future years. Yet there was a time when DoD's ability to bring these various pieces together so effectively was in some question; and this was so despite the fact that military endeavors permit a type of mandating vis-á-vis Service members that civilian entities do not. The challenge at hand is thus compounded: While DoD is founded upon the science of command and control, DHS must rely instead on cooperation and coordination, and the art of persuasion, to successfully achieve its ends.

Accordingly, I would submit that DHS remains a work in progress, but one that must be evaluated in context, with due regard for the substantial challenges that the Department has faced in past, and which it will continue to face in future—including an inhospitable climate of financial austerity, coupled with a rapidly evolving threat spectrum that encompasses both cyber and kinetic components.

QUESTIONS FROM CHAIRMAN PETER T. KING FOR DAVID C. MAURER

Question 1. Will you please share your views on the importance of the completion of the St. Elizabeths project to the Department's efforts to consolidate operations and its potential impact on the Department's performance?

Answer. We have previously reported that consolidation or co-location of Federal Government offices or functions—a goal of the St. Elizabeths project—may result in several benefits, including more effective and efficient operations. In 2011, we re-

ported that co-locating services can result in improved communication among programs, improved delivery of services for clients, and elimination of duplication.[1] For example, programs can be co-located within one-stop centers or electronically linked, which affords the potential for sharing resources and cross-training staff. In 2006, we reported that DHS's plans to co-locate its headquarters, its component headquarters, and their respective staffs and operations centers at one location could further enhance collaboration among DHS's component agencies.[2] DHS has also identified that consolidating most of its headquarters operations at St. Elizabeths would enhance communication, increase efficiency, facilitate mission integration, and foster a "One DHS" culture.

However, given the constrained budget environment, the future of the St. Elizabeths project is uncertain. In December 2011, DHS estimated the project would take 4 to 5 years longer to complete and cost about $600 million to $700 million more than originally planned, largely due to shortfalls in funding. At that time, DHS estimated that the project would be completed in 2020 or 2021. In March 2012, DHS reported that it was in the process of revising its plan of options for completing the St. Elizabeths project, and would continue analyzing options throughout the summer. One option, which includes large segments based on the original construction plan, would take 6 years longer to complete and cost more than $700 million more than originally planned. Under this option, DHS estimated planned construction will be completed in 2022 at an overall cost of about $4 billion.

In addition, while headquarters consolidation may result in gained efficiencies, under DHS's current plan, not all headquarters offices and components will be located at St. Elizabeths. For example, although all of the Secretary's office and the Federal Emergency Management Agency and the U.S. Coast Guard headquarters staff will be relocated, only the headquarters leadership of five major DHS components—U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, Transportation Security Administration, U.S. Secret Service, and U.S. Citizenship and Immigration Services—will be moved. Headquarters staff from these five components will remain in other locations around the National capital region, which limits the potential benefits of consolidation.

Finally, since the planned completion date of the St. Elizabeths project could be 10 years in the future, DHS will not reap the planned benefits of consolidation for some time. During the interim, we believe DHS should continue to focus on executing its plans for addressing GAO's designation of implementing and transforming DHS as a high-risk issue. Doing so will enhance the management platform for the entire Department and better position DHS to carry out its various missions in a more efficient and effective manner.

Question 2a. How would you compare the creation and maturation of the Department of Homeland Security to date to that experienced by the Department of Defense in the decade after its establishment?

Do you believe that now, almost 10 years after its creation, the Department should have matured more quickly and its components should be operating more effectively and efficiently?

Question 2b. How much longer is the argument that bringing together so many Federal agencies a legitimate explanation for the Department's shortcomings?

Answer. As DHS continues to implement plans to address its long-standing management challenges, it can learn from the experience of other departments, including the Department of Defense (DoD). Specifically, since its creation in 1949, DoD has worked to unify the Department, enhance its management practices, and foster a joint approach to operations and decision making. However, it is also important to note that some of DoD's experiences may not be appropriate for DHS. For example, as of October 2012, 63 years after DoD's creation, it remains on GAO's high-risk list for seven management-related topics, including financial management, weapon systems acquisition, and business systems modernization. In addition, several important aspects of DoD's organization and approach are devoted to deterrence, combat operations, and other National security missions that, while complimentary to DHS's homeland security focus, differ significantly from the day-to-day operations and requirements of DHS's components. DHS can certainly learn from DoD's experience, but should exercise care in appropriately selecting and applying those lessons that can be best applied to DHS.

Prior to DHS's creation, we reported that building a common, unified Department from several legacy agencies represented a significant challenge that would take

[1] GAO–11–92.
[2] GAO–07–89.

several years to achieve.[3] This has proven to be the case. DHS has remained on GAO's high-risk list since it began operations in 2003.

Since its creation, DHS has implemented key homeland security operations and achieved important goals in many areas to create and strengthen a foundation to reach its potential. DHS has made important progress, particularly on the mission side. For example, DHS:

- Implemented the U.S. Visitor and Immigrant Status Indicator Technology program to verify the identities of foreign visitors entering and exiting the country by processing biometric and biographic information;
- Developed and implemented Secure Flight—a program for screening airline passengers against terrorist watch list records—and new programs and technologies to screen passengers, checked baggage, and air cargo;
- Assessed risks posed by chemical, biological, radiological and nuclear threats and deployed capabilities to detect these threats; and
- Created new programs and offices to implement its homeland security responsibilities, such as establishing the U.S. Computer Emergency Readiness Team to help coordinate efforts to address cybersecurity threats.

But at the same time, our work has identified three key themes—leading and coordinating the homeland security enterprise, implementing and integrating management functions for results, and strategically managing risks and assessing homeland security efforts—that have impacted the Department's progress since it began operations.[4] DHS had successes in all of these areas, but our work found that these themes have been at the foundation of DHS's implementation challenges and need to be addressed from a Department-wide perspective. As DHS continues to mature, more work remains for it to strengthen the efficiency and effectiveness of those efforts to achieve its full potential.

Of particular note, DHS continues to face several management challenges. For example, DHS's major acquisitions programs face challenges that increase the risk of poor outcomes, such as cost growth and schedule delays. Additionally, DHS has been unable to obtain an audit opinion on its internal controls over financial reporting due to material weaknesses in internal controls. Further, despite DHS efforts to improve employee morale, Federal surveys have consistently found that DHS employees are less satisfied with their jobs than the Government-wide average.

DHS has several initiatives underway that, if fully implemented and sustained, could help address the Department's management challenges. For example, as I noted in my September 2012 testimony before this committee, DHS's *Integrated Strategy for High-Risk Management* identifies 18 key initiatives and corresponding corrective action plans for addressing the Department's management challenges and improving operational efficiency through better integration of people, structures, and processes. This strategy provides a path for moving DHS from where it is now—a large Department with several management challenges—to where it wants to be—a unified Department, supported by integrated management functions. DHS must now focus on executing the strategy. Doing so is important because building a solid management foundation will help DHS carry out its homeland security missions.

[3] GAO–03–260.

[4] DHS defines the homeland security enterprise as the Federal, State, local, Tribal, territorial, non-governmental, and private-sector entities, as well as individuals, families, and communities, who share a common National interest in the safety and security of the United States and the American population.