IS DHS EFFECTIVELY IMPLEMENTING A STRATEGY TO COUNTER EMERGING THREATS?

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

FEBRUARY 3, 2012

Serial No. 112–64

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

76–510 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
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California

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

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

MICHAEL T. MCCAUL, Texas, *Chairman*

GUS M. BILIRAKIS, Florida
BILLY LONG, Missouri, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

WILLIAM R. KEATING, Massachusetts
YVETTE D. CLARKE, New York
DANNY K. DAVIS, Illinois
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DR. R. NICK PALARINO, *Staff Director*
DIANA BERGWIN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Subcommittee Director*

CONTENTS

Page

STATEMENTS

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Oversight, Investigations, and Management:
Oral Statement 1
Prepared Statement 3
The Honorable William R. Keating, a Representative in Congress From the State of Massachusetts, and Ranking Member, Subcommittee on Oversight, Investigations, and Management 4

WITNESSES

PANEL I

Mr. Paul A. Schneider, Principal, The Chertoff Group:
Oral Statement 5
Prepared Statement 7
Ms. Sharon L. Caudle, PhD, The Bush School of Government and Public Service, Texas A&M University:
Oral Statement 12
Prepared Statement 13

PANEL II

Mr. Shawn Reese, Analyst, Emergency Management and Homeland Security Policy, Congressional Research Service:
Oral Statement 41
Prepared Statement 42
Mr. David C. Maurer, Director, Homeland Security and Justice Team, Government Accountability Office:
Oral Statement 48
Prepared Statement 49
Mr. Alan Cohn, Deputy Assistant Secretary, Office of Policy, Department of Homeland Security:
Oral Statement 58
Prepared Statement 60

FOR THE RECORD

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Oversight, Investigations, and Management:
Statement of the Texas Border Coalition 32

IS DHS EFFECTIVELY IMPLEMENTING A STRATEGY TO COUNTER EMERGING THREATS?

Friday, February 3, 2012

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

The subcommittee met, pursuant to call, at 10:04 a.m., in Room 311, Cannon House Office Building, Hon. Michael T. McCaul [Chairman of the subcommittee] presiding.

Present: Representatives McCaul, Long, Duncan, Keating, Clarke of New York, and Davis.

Mr. MCCAUL. The committee will come to order. Good morning.

The purpose of this hearing is to examine the strategy documents produced by the Department of Homeland Security pertaining to emergency—emerging threats and the implementation of those strategies. I now recognize myself for an opening statement.

In December 2009 Homeland Security Secretary Janet Napolitano gave a speech to her Department. She said, "I see one DHS as a strong, efficient, and focused department—one where all the talents and skills that we possess as individuals and as components come together and come together in new and exciting ways to serve our missions."

The Department of Homeland Security is the third-largest department in the Federal Government, with more than 200,000 employees and an annual budget of more than $40 billion. Its transformation, according to the GAO, is critical to achieving its homeland security mission. However, the agency has been criticized for excessive bureaucracy, waste, ineffectiveness, and lack of transparency that have hindered its operations and wasted taxpayer dollars.

For example, the DHS inspector general, in a November 2011 report, concluded the Department has major challenges, mainly in the area of management, including acquisition, information technology, grants, and finances. These challenges hinder the Department's efforts to become a cohesive, effective, and efficient organization.

The GAO concludes many DHS management functions are high-risk, including acquisitions, information technology, finances, human capital and integration, all resulting in performance problems and mission delays. Unless we fix these types of problems we

will continue to see failures in DHS programs such as the Secure Border Initiative virtual fence, where in the end taxpayers received little if any return on a $1 billion investment. Secretary Napolitano will certainly not attain her goal of One DHS until financial and management systems are integrated.

Our subcommittee begins a series of hearings examining the challenges DHS faces. We will begin focusing the hearings on three basic questions: One, what challenges does DHS face? Two, why is it taking so long to become One DHS? Three, do DHS shortcomings hinder it from carrying out its core mission of securing the homeland?

Today we begin with the basics by examining the DHS strategy and its implementation to counter emerging threats. What is the DHS strategy? The Congressional Research Service concludes there are several homeland security strategic documents with differing goals, priorities, and definitions. These examples incorporate both White House and DHS strategy documents including the National Strategy for Homeland Security; the National Security Strategy; the National Strategy for Counterterrorism; the Strategic Plan—One Team, One Mission, Securing Our Homeland; the Quadrennial Homeland Security Review; and the Bottom-Up Review.

In the 9/11 Recommendations Act of 2007 Congress mandated DHS to develop a Quadrennial Homeland Security Review to upgrade strategies related to homeland security and align the strategy with the Department's programs and activities. The Department developed a QHSR and supplemented it with a Bottom-Up Review.

The GAO analyzed both of these documents and determined DHS only fully addressed three of the nine 9/11 Commission Act reporting requirements. DHS only partially addressed the other six through the QHSR and other reports.

But most notably, DHS did not identify how these reports are consistent with other National and DHS strategies. All these different strategies are confusing to both Congress and, more importantly, the components which have to implement these strategies.

Just as important as identifying what the strategy is, is understanding how DHS will implement it. How does DHS translate words into reality?

The Wharton Business School has a model of best practices for successful strategy implementation. Specifically, is there an action plan? Is the headquarters' organizational structure the correct size? Is there monitoring and control from headquarters for implementing the strategy? Are core missions and initiatives linked together to prevent duplication?

The bottom line is that DHS needs a single strategic document which subordinate agencies can follow and make sure the strategy is effectively and efficiently implemented. This single document should conform to the National Security Strategy in the United States, and if the agencies do not have a clearly-established list of priorities it will be difficult to complete assigned missions.

We understand DHS has a wide diversity of missions including controlling our borders, securing transportation, protecting the President, conducting sea search and rescue, and researching radi-

ation technology, to name just a few. Because of this diversity it is important to have a single comprehensive strategy.

Additionally, we must ensure each agency, whether it is Customs and Border Protection, Secret Service, TSA, or Coast Guard, is effectively implementing the strategy by making sure headquarters has the proper monitoring and controls in place. We ask these questions today to assist the Department and determine what Congress can do to move the Department toward the goal, as the Secretary said, of becoming One DHS.

So with that, I recognize the Ranking Minority Member who appeared at this hearing in just the nick of time.

Bill, welcome.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

JANUARY 25, 2012

In December 2009, Homeland Security Secretary Janet Napolitano gave a speech to her Department. She said, "I see One DHS as a strong, efficient, and focused Department—one where all the talents and skills that we possess as individuals and as components come together and come together in new and exciting ways to serve our missions."

The Department of Homeland Security (DHS) is the third-largest Department in the Federal Government with more than 200,000 employees and an annual budget of more than $40 billion. Its transformation, according to the Government Accountability Office (GAO), is critical to achieving its homeland security mission. However, the agency has been criticized for excessive bureaucracy, waste, ineffectiveness, and lack of transparency that have hindered its operations and wasted taxpayer dollars.

For example:

- The DHS Inspector General, in a November 2011 report, concludes the Department has major challenges mainly in the area of management, including acquisition, information technology, grants, and finances. These challenges hinder the Department's efforts to become a cohesive, effective, and efficient organization.
- The Government Accountability Office (GAO) concludes many DHS management functions are high-risk, including acquisitions, information technology, finances, human capital, and integration, all resulting in performance problems and mission delays.

Unless we fix these types of problems we will continue to see failures in DHS programs such as the Secure Border Initiative virtual fence, where in the end taxpayers received little if any return on a $1 billion dollar investment. And Secretary Napolitano will certainly not attain her goal of "One DHS" until financial and management systems are integrated.

Our subcommittee begins a series of hearings examining the challenges DHS faces. We will be focusing the hearings on three basic questions:

- What challenges does DHS face?
- Why is it taking so long to become "One DHS?" and
- Do DHS shortcomings hinder it from carrying out its core mission of securing the homeland?

Today we begin with the basics by examining the DHS strategy and its implementation to counter emerging threats. What is the DHS strategy?

The Congressional Research Service concludes there are several homeland security strategic documents with differing goals, priorities, and definitions. These examples incorporate both White House and DHS strategy documents including:

- 2007 National Strategy for Homeland Security,
- 2010 National Security Strategy,
- National Strategy for Counterterrorism,
- Strategic Plan—One Team, One Mission, Securing Our Homeland,
- Quadrennial Homeland Security Review, and
- Bottom-Up Review.

In the 9/11 Recommendations Act of 2007, Congress mandated DHS develop a Quadrennial Homeland Security Review, a QHSR, to update strategies related to homeland security and align the strategy with the Department's programs and ac-

tivities. The Department developed a QHSR and supplemented it with a Bottom-Up Review (BUR).

The GAO analyzed both of these documents and determined DHS only fully addressed three of the nine 9/11 Commission Act reporting requirements in the QSHR. DHS only partially addressed the other six through the QHSR and BUR reports. Most notably DHS did not identify how these reports are consistent with other National and DHS strategies.

All these different strategies are confusing to both Congress and more importantly the components which have to implement the strategies.

Just as important as identifying what the strategy is, is understanding how DHS will implement it.

The Wharton School of Business has a model of best practices for successful strategy implementation. Specifically, is there an action plan, is the headquarters' organizational structure the correct size, is there monitoring and control from headquarters for implementing the strategy and are core missions and initiatives linked together to prevent duplication?

The bottom line is that DHS needs a single strategic document which subordinate agencies can follow and make sure the strategy is effectively and efficiently implemented. This single document should conform to the National Security Strategy of the United States of America. If the agencies do not have a clearly established list of priorities it will be difficult to complete assigned missions.

We understand DHS has a wide diversity of missions including controlling our borders, security transportation, protecting the President, conducting sea search and rescue and researching radiation technology, to name just a few. Because of this diversity, it is important to have a single comprehensive strategy. Additionally we must insure each agency—whether it is the Customs and Border Protection, Secret Service, Transportation Security Administration, or the Coast Guard—is effectively implementing the strategy by making sure headquarters has the proper monitoring and controls in place.

We ask these questions today to assist the Department and determine what Congress can do to move the Department toward the goal of becoming "One DHS."

Mr. KEATING. Thank you, Mr. Chairman. I want to thank you for convening this hearing.

I would also like to thank our witnesses for their participation and giving their time with us this morning.

Eleven years ago the heinous attacks of September 11 served as the impetus for changing the way we approach homeland security in the United States. Following the tragic day, 22 separate agencies, many with challenges all their own, were combined to form the Department of Homeland Security. The Department was tasked with carrying out the strategy that defined the Nation's homeland security agenda.

Since that time, numerous National strategies were released and further refined through time. Last year the Department of Homeland Security released its first-ever Quadrennial Homeland Security Review, which we will refer through acronyms, which I hate afterwards, so try and remember all that that was. The framework of this document, along with the President's National Security Strategy, which, for the first time, included homeland security as an integral component of our National security, has set the Nation on a course to address not only counterterrorism but emerging threats, such as National disasters Nationally, climate change, and cybersecurity, as well.

Now that a more comprehensive National strategy approach is defined, what are we doing now to really ensure that this is going to be carried out? That is the question we are asking today, but before we do that we have to determine whether the requirements, roles, and responsibilities at the Federal, State, and local levels are properly aligned, and above all, the proper resources are allocated.

This past Congress the Department of Homeland Security has suffered significant cuts, especially at the management level. Furthermore, the Office of Policy, which is responsible for the preparation of the QHSR and for developing and assessing the implementation of the Department's long-term strategy, was one of the hardest-hit office in the last rounds of cuts. Adding insult to injury, the Department is still without a financial management system that is integrated, functional, and up-to-date, resulting in Department-wide struggles with fund balances, improper payments, and Anti-deficiency Act violations.

Although improvements have been made, the workforce responsible for acquisition oversight is understaffed and its procurement, information technology, and human capital functions remain high on GAO's risk list. Furthermore, we are still many years and many more dollars away from finishing what was started in terms of consolidating the Department's headquarters at St. Elizabeths.

These challenges may seem unrelated to strategy, but unless these management challenges are fixed-mission execution will suffer. That all being said, I look forward to today's hearing and testimony, and, Mr. Chairman, I yield back my time.

Mr. MCCAUL. I thank the Ranking Member.

Other Members of the subcommittee are reminded that opening statements may be submitted for the record. We have two very distinguished witnesses on the first panel, and I would like to go ahead and introduce them before their testimony.

The first is the Honorable Paul Schneider. He is a principal at the Chertoff Group, which focuses on the defense and aerospace industries, cybersecurity, systems engineering, and major acquisition procurement and financial management.

Prior to joining the Chertoff Group, Mr. Schneider was the deputy secretary for the Department of Homeland Security, where he managed the day-to-day operations of a Department with over 200,000 employees and an annual budget of over $52 billion. While at DHS he was also under secretary for management.

Thank you, and welcome to our committee.

Next we have Dr. Sharon Caudle, who is the faculty member at a school that is near and dear to my heart, the Bush School of Government and Public Service at Texas A&M University, where she teaches in the master of public service and administration program and the certificate in homeland security program. Before joining the Bush School she was with the U.S. GAO where she focused on homeland security and National preparedness strategic policies and programs.

So welcome, both of our witnesses.

With that, the Chair now recognizes Mr. Schneider for his testimony.

STATEMENT OF PAUL A. SCHNEIDER, PRINCIPAL, THE CHERTOFF GROUP

Mr. SCHNEIDER. Thank you, Mr. Chairman, Congressman Keating, and Members of the subcommittee. It is a pleasure to appear before you today.

Based on my observations, former position, and years of experience, I am here to provide my views about DHS's current strategy

and what direction they should be—they should consider taking in the future. I believe the most serious dangers facing our Nation today involve biological, cyber, and nuclear threats. I know DHS takes these threats very seriously and has instituted several programs to address these dangers, but I am concerned that in some cases fiscal reality will limit the resources that are available to counter these threats.

Biological is at the top of the list in terms of risk because of the relative ease of accessibility to materials and know-how, the potential consequences, and relatively low level of National preparedness. Cyber, because of its pervasiveness and difficulty in pinpointing attribution, has rapidly emerged as a threat to all critical infrastructure areas.

Both nuclear and biological threats—for these what we need is a very strong National preparedness posture comprised of a very highly integrated group of stakeholders supported by realistic plans and frequent exercises that provide confidence in our preparedness and ability to respond.

I have several recommendations. First, emphasize cybersecurity in the private sector with practical help. While DHS continues to focus its funding on defending the Federal Government networks there is an additional need for investment support to identify, prevent, and mitigate threats to our mostly privately-owned critical infrastructure and key resource systems as well as the State and local governments and infrastructure providers.

I recommend establishing public-private partnerships in order to perform the following: Create and institute IT portals that easily convey Government requirements to large and small businesses that will enable them to easily explain what they have to offer. That is the seat of innovation in this country.

Set up programs with and for small and mid-size businesses as well as State and local governments to educate them about what they can do to protect their networks. Help in the creation of private sector-run security operation centers to provide cybersecurity services for small and mid-sized businesses and for certain public sector utilities and entities that will allow them to protect their network.

Establish a robust modeling and simulation effort. Focus on resilience. Examine the need for more agile contracting strategies to work inside of the stimulus-response cycle that is needed for cyber issues.

No. 2: Restructure the focus of science and technology. Significant budget cuts imposed on the Department's S&T effort has led me to conclude that the whole nature of this function has to change dramatically. After accounting for the existing manpower levels, major laboratories, university research centers, there are very little discretionary funds left to use.

So what I recommend doing in that particular case is to do a restock and prioritization of the efforts that they focus on. I know it is hard to make some adjustments, especially in manpower, but in this budget scenario it certainly dictates that.

We need to have a more focused and deliberate test and evaluation effort in order to inform users of whether or not the stuff they are buying works. It is not clear to me what State and local and

private organizations do in terms of buying equipment that there is any competent technical authority has said that the stuff is okay. That means shifting to threat-based T&E as opposed to standards-based T&E, which is driven by the industry.

I think you have to—they have to recognize that the Department of Defense has a tremendous amount of talent, and so what I think we need to be doing is harvesting that talent. I would put together a team of people made up of the laboratories at DOD, FFRDCs, DHS operational people, DHS FFRDCs, and look at each of these operational areas and see what technology could be immediately harvested.

No. 3: Consolidate the information technology effort under the CIO. No matter what system you are talking about, DHS—the underpinnings are a massive IT system. Frankly, they all are interdependent, multiple databases, but yet individual programs.

This needs to be consolidated. Put the funding under the CIO. Then not just let programs individually decide what modernization has to take place, but rather, let the CIO move the Department in an integrative phase approach to maximize the use of resources.

Fourth, consolidate the operations. When I was the dep sec I was asked about basically: Should the Department have a Goldwater Nichols? I always said at the time that at some point it should, but it was too premature. At this point in time I think it is important to start seriously considering how to go do that.

Department of Defense did that in 1986 followed by the DMR in 1989, and the fact of the matter is it now works. So from an operational warfare—from an operational law enforcement standpoint and from a headquarters integration standpoint that is the thing to do. I realize that that is very hard to do, and it would enable some operating components to lose some individuality, but the fact of the matter is it needs to be done.

I think the Department has come a long way since its origin and will continue to improve over its years. I think as we look to the future we need to make some of these improvements.

I want to conclude by thanking you for the opportunity to be here today, your significant support of the Department and its thousands of people, and I would be happy to answer any questions that you might have.

[The statement of Mr. Schneider follows:]

PREPARED STATEMENT OF PAUL A. SCHNEIDER

FEBRUARY 3, 2012

Thank you Mr. Chairman, Congressman Keating, and Members of the subcommittee. It's a pleasure to appear before you today.

It has been approximately 3 years since I have left office as the Deputy Secretary of the U.S. Department of Homeland Security (DHS). Since that time, I been consulting for the U.S. Government (except for DHS); am a Principal in The Chertoff Group which is a company that provides consulting, security, and merger and acquisition (M&A) advisory services for clients in the security, defense, and Government services industries around the world; and, I also currently serve on several boards and advisory groups, including as Chairman of the Board of Directors of the Applied Science Foundation for Homeland Security. My role with the Foundation and other small companies is done on a pro bono basis.

Since leaving my position at DHS, I have had the opportunity to observe the changing and challenging budget environment and assess its impact on DHS operations and those of the homeland security enterprise. Based on my observations,

former position, and years of experience, I am here today to provide my views about DHS' current strategy and what direction they should consider taking in the future.

THREATS

I believe the most serious dangers facing our Nation today involve biological, cyber, and nuclear threats. As you know it is very difficult to convince the general public of the importance of these threats. I know DHS takes these threats very seriously and has instituted several programs to address these dangers, but I am concerned that in some cases, fiscal reality will limit the financial resources that are available to counter these threats.

Biological is at the top of the list in terms of risk because of the relative ease of accessibility to the materials and know-how; the potential consequences; and relatively low level of National preparedness. Cyber because of its pervasiveness and difficulty in pinpointing attribution has rapidly emerged as a threat to all critical infrastructure areas.

For both nuclear and biological threats (and the wider range of catastrophic threats) what we need is a very strong National preparedness posture comprised of a highly integrated group of stakeholders supported by realistic plans and frequent exercises that provide confidence in our preparedness and ability to respond.

I think it is appropriate for DHS to accelerate "fixing" critical infrastructure issues. The tiered approach to identifying the critical facilities can serve as a map to developing and implementing a mitigation plan.

EMPHASIZE CYBER SECURITY IN PRIVATE SECTOR WITH PRACTICAL HELP

I am pleased that cyber security continues to receive the political and financial support it does from the Congress. However, the extent of this problem is huge. While the Department of Homeland Security continues to focus its funding on defending the Federal Government networks (the .gov domain), there is an additional need for investment and support to identify, prevent, and mitigate threats to our mostly privately-owned critical infrastructure and key resource systems, as well as State and local governments and infrastructure providers.

I find it amazing that within a 50-mile radius of this building there is a nexus of expertise in this area that is without peer: The Ft. Meade complex, major cyber security centers set up by the major corporations, cyber incubators in the State of Maryland, the University of Maryland Cyber Research and Development Center, etc.

To support the constantly evolving and persistent cyber threat, I would recommend establishing a public-private partnership in order to perform the following:

1. Create and institute IT portals that easily convey Government requirements to large and small businesses that enable them to easily explain what they have to offer. The rigid small business methods and forums cannot match the near-real-time speed that is required to keep up in this world; and yet there is a tremendous amount of innovation and capability that can be tapped.
2. Set up programs with/for small and mid-size businesses, as well as State and local governments, to educate them about what they can do to protect their networks.
3. Help in the creation of private-sector-run security operations centers to provide cybersecurity services for small and mid-sized business, and for certain public sector entities, that will allow them to protect their networks.
4. Establish a more robust modeling and simulation effort that allow relevant parties to strategize the threat space, model the implications and determine risk mitigation approaches.
5. Consistent with the Critical Infrastructure Protection (CIP) implementation program, focus on resilience to look at means to quickly recover from a cyber-incident.
6. Examine the need for more agile contracting strategies that work inside the stimulus-response cycle needed for cyber issues.

RESTRUCTURE THE FOCUS OF SCIENCE AND TECHNOLOGY

The budget cuts imposed on the Department's Science and Technology Directorate (S&T) have led me to conclude that that S&T must change its entire nature in order to reflect its new budget reality. After accounting for the existing manpower levels, major laboratories that are funded by these appropriations and the University Centers of Excellence, very little discretionary funds are remaining.

Therefore I believe the focus of DHS S&T should be as follows:

1. Emphasize a more focused and deliberate test and evaluation program to inform users of the right equipment and systems to deploy for the right mission.

Work with the users to understand the threat environment, their operational concepts for operations to make sure the test procedures and environments are relevant. Right now we have public and private institutions around the country buying stuff and it is not clear if any competent technical authority knows if it is any good.

2. Based on an aggressive T&E program to meet users' needs, develop standards for devices and systems that could be procured by the private and public sectors, not the devices themselves, because it is impractical to think that the Government will get enough procurement dollars to field the equipment themselves. This means using T&E and threat-based standards as the basis to inform users of the right equipment for the right mission application. This moves away from the standards-based (industry-driven) approach which is not the correct approach for this situation.

3. Recognize that State and local governments and the public sector, not just the DHS operational components, are the recipients of S&T investment dollars and include their priorities in the resource allocation process.

4. Aggressively harvest the enormous amount of technology that the Department of Defense has been/is developing and with the correct set of innovative people look at how to adapt it to DHS uses. In this regard I recommend that consideration be given to forming a team with representatives from Department of Defense (DoD) laboratories and Federally Funded Research and Develop Centers (FFRDCs) and the DHS Systems Engineering FFRDC with DHS operational personnel to evaluate specific scenarios that DoD technology could be readily adapted to enhance mission effectiveness.

5. While DNDO is a separate organization, these recommendations also apply to the work and RDT&E they do.Within DNDO, the process was and I believe still is to work with State and local law enforcement to determine how they would use detection systems and then to test them using those Concepts of Operations (CONOPs) against threat material and in operationally relevant environments.

6. Readjust funding allocations from manpower, laboratories, and University centers to S&T that directly and more immediately supports the users.

CONSOLIDATE INFORMATION TECHNOLOGY (IT) UNDER THE CHIEF INFORMATION OFFICER (CIO)

The Under Secretary for Management and the Chief Information Officer (CIO) has made DHS the leader in data center consolidation and the migration to the cloud. Once you have worked with the IT underpinnings of DHS, you realize it is one massive IT system that many different operational users use, with the bulk of the databases serving multiple users under multiple systems and many are interdependent.

So, whether it is E-Verify, US–VISIT, TECS, and TTAC with all of its component systems, there is interlocking because many of the same databases are accessed in order for the Government to make adjudication. Yet, observing on the outside, as I have, systems modifications, modernizations, and upgrades are executed by individual components that happen to be responsible for their programs and systems.

While coordination and oversight can be effective, I think the current environment dictates a different business model of centralized command and control.

The IT area has and will continue to sustain large financial cuts due in some part to the belief that IT is an enabler and therefore iris investment ought to achieve savings. I agree that IT is enabler, but the business management model that governs is as much of an enabler as the technology itself.

Therefore I recommend the following:

1. Consolidate all of the IT funding under the DHS CIO;

2. Empower the CIO and the Under Secretary for Management to determine how best to incrementally phase in a new IT infrastructure building on what they have done with the data center integration and cloud migration, by using the appropriated funds for the individual systems, modulating individual program priorities for the overall good of the Department and the betterment of the overall IT infrastructure.

For this to succeed DHS will have to continue to make substantive and sustained progress in developing a functional command and control, communications, and requirements development.

CHANGE THE BUSINESS MODEL FOR SCANNING EQUIPMENT

Scanning is an essential part of the security architecture for aviation security and in my view the technology is dynamic, driven in large part to significant advances

in the medical field. And as nano technology emerges, to an even greater extent technology enables enhancements in fidelity for screening in terms of quality and speed of the throughput which will be highly desired and valued by DHS. Now, these systems are procured and upgraded by the Government.

Given funding realities and the speed of which the commercial sector can quickly develop and respond, this dictates shifting to a business model whereby the Government specifies the requirements and leases the equipment with stated service-level agreements regarding performance like commercial IT contracts, including upgrade and refresh requirements. DHS would essentially pay for this as a fee-for-service lease. I am acutely aware that OMB has definite views of this type of arrangement that may not be as supportive because of scoring considerations.

In my view however, the changing nature of the technology, evolving threat scenarios and the budget realities, demand that the current business model be changed to one of a more commercial nature.

CONSOLIDATE OPERATIONS

While serving as the Deputy Secretary, I was frequently asked by those Members of Congress who were on Homeland Security Committees and Department of Defense Committees whether or not DHS needed "Goldwater Nichols (GN)" legislation.

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 Pub. L. 99–433, made the most sweeping changes to the United States Department of Defense since the Department was established in the National Security Act of 1947 by reworking the command structure of the United States military. It was subsequently followed by the Defense Management Review of 1989 which fully implemented the Packard Commission's recommendations and the Goldwater-Nichols Act to substantially improve the performance of the defense acquisition system; and to manage more effectively the Department of Defense and our defense resources.

I replied that the time was definitely not correct to do that because DHS was still in its infancy, not all the requirements of GN were appropriate to be considered for DHS, and that the Act's operational and acquisition fundamental changes should ultimately be considered and adapted for use by DHS, but timing was key.

At this point in time I think it is appropriate to start thinking seriously about how to accomplish a modified version of GN for DHS, since I think only a few major provisions as discussed below are applicable at this time. The factor that drives me to this conclusion is that I believe currently, no unified command structure exists for DHS components in the field. Each component has individual field structures with unique geographic boundaries and independent chains of command. These lines of authority do not converge until they reach the Secretary/Deputy Secretary.

Practically speaking, in the field, there are independent operating components. I think this hampers operational effectiveness. While I am aware there are several informal teaming arrangements in various ports and cities, it is not the same as an integrated command-and-control structure. Therefore, I recommend:

1. Develop a unified field structure with appropriate command-and-control or coordination authority. This would provide an opportunity for greater stability in State/local relationships and ability to better coordinate DHS operations in the field.
2. Consideration should include various alternatives, such as States, regions, ports, interfaces with DOD, and unique State and local considerations and authorities.
3. Maximizing the collective effectiveness and use of joint assets, both operationally and in the planning and execution of logistics support functions.

I am aware that certain operating component statutory authorities need to be addressed to make this work, but integration of assets at the pointy end of the spear is essential in order to maximize effectiveness in addressing the evolving threat scenarios.

The second major element of a GN move would be to examine centralizing major acquisition programs in a "DOD Systems Command" type of structure separate from the Operational Components. This would enable operating components to focus on operations and build upon the critical acquisition mass currently available, while ensuring major cross-component acquisition initiatives are executed in an integrated manner (as many current operations are actually executed). As part of this effort a total review of the acquisition process, its successes, lessons learned, and next steps would be a useful step to help shape the structure of this organization. All of this will eliminate redundancy, while complying with an integrated enterprise-wide architecture and offers the potential for tremendous financial economies.

The basis for this recommendation is simple. The majority of DHS operational people wears badges and carry guns. Is it smart to hold a major component head,

for example the head of CBP, with approximately 65,000 people, responsible for his 24-hr×7-day law enforcement responsibilities around the world and at the same time, ask him to be responsible for developing and fielding complex systems that must integrate with other complex systems? Is this the correct model for the future? I think the answer to both questions is no and that is why I think this different structure is much more conducive to enhancing effective operations.

In DoD they learned this a long time ago. That is why the Air Force's Air Combat Command deploys planes and does not develop the F–35, and why the Navy's COMSUBLANT operates submarines but does not develop the Virginia Class Submarines.

I am aware that many organizations within DHS will disagree with these recommendations and argue vociferously against any changes to the status quo to protect their legacy functions and independence. So, it would be the challenge to leadership to steer changes of this magnitude. The DOD was created in 1947; GN was authorized in 1986, but really didn't happen until the DMR in 1989 when the majority of the GN changes took effect. It would be unreasonable to assume that this type of change would be any different in time scale in DHS.

OVERLAPS IN THE ASSIGNMENT/INTERPRETATION OF HOMELAND SECURITY ROLES

I think the issue of ambiguities and overlaps in the assignment/interpretation of homeland security roles, responsibilities, and authorities among Federal stakeholders are a continuing obstacle to unity of effort within the Federal Government and our allied countries. These overlaps and ambiguities also have the effect of fundamentally undermining the credibility and ability of Federal agencies to effectively engage with State and local governments and the private sector.

As you're well aware, this is a very difficult and politically charged issue that is difficult to rationalize. While, barring some major catalyst, a holistic attempt to comprehensively frame and address all roles/responsibilities/authorities issues is near impossible.

What is needed is a systems approach to identifying the overlaps and ambiguities having the most significant implications for our strategic outcomes (e.g., DHS/DOJ re: terrorism prevention and borders; DHS/HHS re: Bio/mass casualty event preparedness & response; DHS/DOD re: catastrophic response support to civil authorities). The challenges with these issues is that agencies and components would rather live with and work around current ambiguities than risk losing equities they consider vital. Yet these same ambiguities significantly undermine unity of effort, and increase risks of failure in preventing or responding to potentially catastrophic events. I doubt many in the administration or Congress have energy on this, but it is a necessary factor that should be addressed.

CONCLUSION

I think DHS has come a long way since its inception and will continue to improve over the next few years. I believe as we look to the future we need to make refinements along the lines I have recommended before you today to meet the many challenges that lie ahead.

I urge you to adapt these recommendations and direct their implementation.

Thank you for your leadership and your continued support of the Department of Homeland Security and its programs, and your support and commitment to the thousands of men and women who dedicate themselves to the defense of our great country.

Thank you for this opportunity to be here today and I am happy to answer any questions that you may have.

Mr. MCCAUL. Thank you, Mr. Schneider. I appreciate your comments about our support for the Department. We do.

The reason we are having these hearings is to find out how we can reform the Department so it works more efficiently and better for its employees. So I appreciate you saying that.

With that, the Chairman now recognizes Dr. Caudle for her testimony.

STATEMENT OF SHARON L. CAUDLE, PH D, THE BUSH SCHOOL OF GOVERNMENT AND PUBLIC SERVICE, TEXAS A&M UNIVERSITY

Ms. CAUDLE. Thank you, Mr. Chairman, for the opportunity to be here today. I will specifically focus my remarks on DHS's National preparedness approach as components of an overall strategic framework, taking a look at what the requirements are, expectations are for the homeland security community—Federal, State, local, private sector, non-Governmental, individuals, families, and communities.

First, there are major themes in DHS's strategy that provide the context for challenges I will mention shortly. These themes include, for example, homeland security, now clearly a part of National security; the whole homeland security community, including the Federal Government, responsible for preparedness, from prevention to recovery, including mitigation; all-hazards and the maximum capacity for a catastrophic event as benchmarks for preparedness; core capabilities and performance targets update past prescriptive, detailed individual tasks, and target capabilities; and finally, another homeland security management system crafted with performance expectations and assessment mechanisms.

There are three challenges I see in the overall preparedness strategy for subcommittee consideration. The first challenge is whether there should be a fundamental change in the capability-based approach to achieve National preparedness to confront threats.

Federal policies to date, reinforced by legislation, center on building and sustaining robust capabilities—skilled people, material, and processes, and partnerships. This approach drew on the experience of the defense community.

Over time DHS has attempted to link the billions of dollars spent on preparedness with the development of these capabilities. However, valid assessment remains elusive.

In my view, Federal funding constraints and similar challenges for other levels of Government and related homeland security partners present an opportune time to consider the cost-effectiveness of other policy options. These would be compared with the current capabilities approach.

I suggest that one option is adopting National and/or international disaster and emergency management system standards. As with management standards, such as the ISO 9000 quality standards, these can be applied to all organizations.

Already in place is DHS's PS–Prep National voluntary program that does apply preparedness standards to the private sector. Also, the current Emergency Management Accreditation Program, EMAP, also based on standards, is targeted at State and local emergency management programs.

If these disaster and emergency management standards were adopted in lieu of the capabilities requirements, the entire homeland security community would share common preparedness standards, language, and assessment parameters. Of course, still to be resolved would be if the standards should be mandated as a National standard of care and how certification or accreditation against the standards might occur.

The second challenge is whether implementation by the whole community for what FEMA calls maximum of maximums, or mega-disaster scenario, is pragmatically achievable. FEMA advocates that modern disaster planning should be for a meta-scenario that overwhelms all levels of government, including the Federal Government. Worse-case planning under this strategy requires the expertise and resources of the entire emergency management community, from the Federal Government, to the private sector, to the NGOs, to individuals and communities.

One visualizes all preparing for a catastrophe akin to a mega-Hurricane Katrina, the Japanese earthquake tsunami and nuclear event, or world-wide pandemic. It is not clear to me how the Federal Government will operationally craft whole-of-community preparedness for such a mega-disaster scenario.

Implementation details to date are sparse regarding how members should interact to achieve mega-disaster capability targets or make decisions regarding the investment of scarce resources. Sound implementation would call for complex, coordinated action, assessment, and the commitment of funding that may be overwhelming and marked by imprecision.

The third challenge is whether DHS should include longer-term emerging threats as priorities for action beyond near-term strategies. Current DHS strategies narrowly target threats, including a meta-scenario, with a distinct beginning and end—think earthquake or terrorist attack. Left out by design are conditions that are longer-term in their emergence as direct threats to National security.

These include, for example, the impacts of global climate change, global illicit trafficking and related transnational crime, social disruptions, and economic and financial instability. It is not clear how near-term threat capabilities will prepare the country for the challenges of these longer-term threats, often called "global shocks." DHS certainly understands the need for action anticipating these global shocks under FEMA's Strategic Foresight Initiative, currently underway.

Throughout these three challenges I urge the subcommittee to consider the opportunity costs in DHS continuing to pursue a comprehensive capabilities approach, insistence that the whole homeland security community is being prepared for a mega-disaster scenario, and delayed action on confronting longer-term threats.

Thank you again for the opportunity, and I look forward to any questions the subcommittee may have.

[The statement of Ms. Caudle follows:]

PREPARED STATEMENT OF SHARON L. CAUDLE

FEBRUARY 3, 2012

Thank you for the opportunity to appear before the subcommittee today. My name is Dr. Sharon Caudle. I am the Younger-Carter Distinguished Policymaker in Residence and Visiting Lecturer, The Bush School of Government and Public Service, Texas A&M University. I am also a Senior Fellow at The George Washington University's Homeland Security Policy Institute. This testimony represents my personal opinions and not necessarily the opinions of the Bush School or the Homeland Security Policy Institute.

Today's hearing focuses on whether the Department of Homeland Security (DHS) is implementing an effective strategy to counter emerging threats to the security of

the Nation. In my statement today, I first highlight the DHS policies and overall approach for preparedness—from protection to recovery—currently in place as the result of Presidential Policy Directive-8 (PPD–8 National Preparedness). Then I focus on what I see as three challenges the subcommittee should consider: (1) Whether there should be a fundamental change in the operational approach to meeting a National preparedness goal, (2) whether implementation of capabilities by the "whole of community" from the Federal Government to individual citizens to address the "maximum of maximums" threats is pragmatically achievable, and (3) whether DHS should include other longer-term, emerging threats as priorities for action in its near-term strategies.

CURRENT NATIONAL PREPAREDNESS STRATEGIES AND APPROACH

In the 5 years following the issuance of President Bush's first National homeland security strategy, the administration and Congress clarified the scope, mission areas, and responsibilities for homeland security. National strategy objectives were consistent in four areas: (1) Prevent and disrupt terrorist attacks, (2) protect the American people, critical infrastructure, and key resources, (3) respond to and recover from incidents that do occur, and (4) continue to strengthen the management foundation of homeland security to ensure long-term success.

President Obama's administration has continued the refinement of homeland security policies and strategies, consistent with Congressional action. In February 2010, DHS released the legislatively-required *Quadrennial Homeland Security Review Report.*[1] As was the case with earlier policies, the Report called for a National framework of collective efforts and shared responsibilities to build and sustain critical homeland security capabilities. The grave security environment (beyond terrorism) identified in the Report clearly supported a broader security stance: It was expected that violent extremist groups would use terrorism to attack United States targets, social, and/or political instability would continue, health threats would be more difficult to prevent, technological developments, and cyber threats would pose threats, climate change would increase weather-related hazards, multiple simultaneous crises were likely, and complacency would be a danger as major crises receded from memory.

As the subcommittee knows, President Obama released a new *National Security Strategy* that reflected the homeland security policies and concepts identified in the Report.[2] The Strategy reaffirmed the "whole of Government" approach, which is the need for all levels of Government, if not the entire country, to strengthen National preparedness. The Strategy retained the earlier policy notions of a homeland security enterprise (Federal, State, local, Tribal, territorial, non-Governmental, and private-sector entities, as well as individuals, families, and communities sharing a common National interest in American safety and security) and a culture of preparedness.

Presidential Policy Directive-8

The 2010 Report and the newer National Security Strategy set the stage for both a restatement and revitalization of the Presidential direction for National preparedness. President Obama's March 2011 Presidential Policy Directive 8 National Preparedness (PPD–8) replaced the 2003 Homeland Security Presidential Directive-8 (HSPD–8) issued by President Bush,[3] which had been codified by Congress. The new directive reaffirmed past policies and direction, calling for the development of: (1) A National preparedness goal identifying the core capabilities necessary for preparedness, and (2) a National preparedness system guiding activities enabling the Nation to achieve the goal. National preparedness was defined as actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from the threats posing the greatest risk to the Nation's security.

Specifically related to the subcommittee's interest in addressing emerging threats, PPD–8 required that a new National preparedness goal address specific threats and vulnerabilities. This overtly reduced reliance on National planning scenarios issued several years earlier as yardsticks to measure preparedness capabilities. The goal was to define the core capabilities necessary to prepare for incidents posing the greatest risk to the Nation's security. This made concrete a new policy emphasis on maximum capacity for any major disaster or catastrophe.

---

[1] U.S. Department of Homeland Security (DHS). 2010. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.* [February 2010].

[2] Obama, Barack. 2010. *National Security Strategy.* [May 2010].

[3] Obama, Barack. 2011. *Presidential Policy Directive/PPD–8 National Preparedness.* [March 30, 2011].

The directive also mandated a new piece to the National preparedness system—planning frameworks for each of the five preparedness objectives—from prevention to recovery. It was envisioned that each planning framework would include a basic plan to address all-hazards. There would be roles and responsibilities at the Federal level, but annexes would address unique requirements for particular threats or scenarios. The directive also required a "campaign" to build and sustain preparedness. This would integrate community-based, non-profit, and private sector preparedness programs, research and development activities, and preparedness assistance.

The PPD–8 Implementation Documents

DHS has issued a flurry of documents in response to PPD–8's mandates. In May 2011, DHS issued the *Implementation Plan for Presidential Policy Directive 8: National Preparedness.*[4] Under the Implementation Plan, DHS was to perform a strategic, National-level risk assessment applicable to National, regional, and local levels. The assessment would help identify where core capabilities and associated performance objectives for the entire homeland security community should be placed, topped by the maximum preparedness capacity needed to respond to a catastrophic event.

Thus, developing "whole of community" core capabilities for catastrophes would not necessarily be restricted to specific threat and hazard scenarios described in earlier National planning scenarios. FEMA administrator Craig Fugate described the change as planning for a "meta-scenario" (or maximum of maximums) disaster. The basis for planning was a worst-case scenario involving multiple factors to plan for different hazards that challenges preparedness and overwhelms the response capabilities of every Governmental level.[5] As I understand it, the scenario, a no-notice event, contemplates the impact area of at least 7 million population and 25,000 square miles, and involving several States and FEMA regions. It results in 190,000 fatalities in its initial hours, with 265,000 citizens requiring emergency medical attention. There is severe damage to critical infrastructure and key resources, including transportation. The fiscal year 2011 Regional Catastrophic Grant Program guidance uses the meta-scenario to promote preparing for a catastrophe where extraordinary levels of mass casualties, damage, and disruption overwhelm traditional and well-established response and recovery plans and procedures.

In September 2011, DHS issued the *National Preparedness Goal First Edition.*[6] The new Goal included detailed tables with core capabilities for prevention through recovery (called mission areas) and their preliminary targets. For example, prevention capabilities included planning, public information and warning, operational coordination, forensics and attribution, intelligence and information sharing, interdiction and disruption, and screening, search, and detection. Each capability was described; to illustrate, interdiction and disruption is to delay, divert, intercept, halt apprehend, or secure threats and/or hazards.

The document made clear that these core capabilities presented an evolution from the voluminous target capabilities list developed in response to HSPD–8. The core capability targets would be the performance thresholds for each core capability and the basis to develop performance measures to evaluate progress in meeting the targets. The description of the core capabilities and their preliminary targets were significantly streamlined from the task and capability lists issued in response to HSPD–8 and subsequently tied to Federal homeland security funding. While still prescriptive, it appears the notion was that streamlining should create more room for members of the homeland security community to craft capabilities tailored to local and regional considerations, as well as the National interest.

The Goal stated that a strategic National risk assessment should confirm the need for an all-hazards, capability-based approach to preparedness planning. DHS' December 2011 unclassified *Strategic National Risk Assessment* grouped threats and hazards into National-level events to test the Nation's preparedness.[7] These included natural, technological/accidental, and adversarial/human-caused threat and hazard groups:

- *Natural.*—Animal disease outbreak; earthquake; flood; human pandemic outbreak; hurricane; space weather; tsunami; volcanic eruption; wildfire.

---

[4] DHS. 2011. *Implementation Plan for Presidential Policy Directive 8: National Preparedness.* [May 2011].

[5] Fugate, Craig. 2011. *Evolution of Emergency Management and Communication.* Statement before the U.S. Senate Committee on Appropriations, Subcommittee on Homeland Security. [June 8, 2011].

[6] DHS. 2011. *National Preparedness Goal First Edition.* [September 2011].

[7] DHS. 2011. *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach Toward a Secure and Resilient Nation.* [December 2011].

- *Technological or Accidental*.—Biological food contamination; chemical substance spill or release; dam failure; radiological substance release.
- *Adversarial or Human-Caused*.—Aircraft as a weapon; armed assault; biological terrorism attack (non-food); chemical/biological food contamination terrorism attack; chemical terrorism attack (non-food); cyber attack against data; cyber attack against physical infrastructure; explosives terrorism attack; nuclear terrorism attack; radiological terrorism attack.

The Goal did not address emerging or longer-term threats or drivers of threats such as climate change identified in the *Quadrennial Homeland Security Review Report.* This was purposeful. The unclassified *Strategic National Risk Assessment* said it evaluated the risk from known threats and hazards. Those events, it noted, had a distinct beginning and end and were clearly linked to homeland security missions. Thus, political, economic, and environmental, and societal trends possibly contributing to a risk environment but not National events for homeland security were excluded from the assessment. Nevertheless, the document said non-National-level threats, such as droughts and heat waves, could pose risks to jurisdictions and should be considered in preparedness planning.

In November 2011, DHS released a brief description of a new National Preparedness System.[8] Its components included: (1) Identifying and assessing risk, (2) estimating capability requirements, (3) building and sustaining capabilities, (4) planning to deliver capabilities, (5) validating capabilities, and (6) reviewing and updating. To identify and assess risk, the System document stated that the Strategic National Risk Assessment would analyze the greatest risks to the Nation. The Threat and Hazard Identification and Risk Assessment guidance under development at that time would provide a common, consistent approach to identify and assess risks and associated impacts.

Measuring progress toward achieving the National Preparedness Goal could be done through tools such as exercises, remedial action management programs, and assessments. The National Exercise Program was deemed the principal mechanism to measure readiness, supplemented by exercises done by individual organizations. Training and performance during actual events would test and validate achievement of desired capabilities. On-going sharing of lessons learned and monitoring would also occur through a remedial action management program and a comprehensive assessment system of the whole community. A National Preparedness Report is due in November 2012.

Major Themes in National Preparedness Expectations

Up to this point, I have briefly described the current National preparedness policy, strategy, and guidance. It has highlighted a number of major themes:

- Homeland security placed within National security.
- All-hazards as the centerpiece for preparedness for threats, including terrorism.
- Preparedness defined with the full coverage of objectives: Prevention, protection, mitigation, response, and recovery, with response and recovery no longer the centerpieces of preparedness.
- The whole homeland security community in addition to the Federal Government with the responsibility to protect National interests and way of life.
- Maximum capacity for a catastrophic event (a meta-scenario) as the benchmark for preparedness.
- Known threats and hazards with a distinct beginning and end central to homeland security risk management and preparedness.
- Core capabilities and targets for a National effort update past prescriptive, detailed individual tasks and target capabilities.
- A homeland security management system to accomplish homeland security and crafted with specific components, performance expectations, and assessment and adjustment requirements.
- Assessment of preparedness progress primarily through exercises and actual events.

CHALLENGES IN STRATEGY AND IMPLEMENTATION

Now, I will turn to the challenges I see in the overall preparedness strategy and its implementation to counter emerging threats that the subcommittee should consider. The first: Should there be a fundamental change in the operational approach to meeting a National preparedness goal? The second: Is implementation of the "whole of community" for the "maximum of maximums" pragmatically achievable? The third: What other emerging threats should DHS set as priorities for action?

[8] DHS. 2011. *National Preparedness System* [November 2011].

Alternative to the Current Capabilities Development Approach

The current and earlier National Preparedness Goal and their supporting documents, as well as Federal legislation, have identified the need to build and sustain specific preparedness capabilities for the entire homeland security community. Federal, State, and local governments, non-Governmental organizations, private organizations, and the general public are that community. National preparedness comes from capabilities across this whole community.

DHS in large part adopted the capabilities approach from the Department of Defense where it was used by the defense community in many countries.[9] HSPD–8 required a National preparedness goal to define measurable readiness (preparedness) priorities and targets, but also with a caveat about the resource investments. PPD–8 called for actions to achieve a preparedness approach to optimize the use of available resources.

Developing capabilities may have been the optimal route at that time towards achieving preparedness, but whether other alternatives that were better investments were considered was not made explicit—if, in fact, they were even considered. In the interim, as the subcommittee knows, DHS has provided billions in preparedness grants intended to aid States, urban areas, Tribal governments, and non-profit organizations, supposedly to strengthen their capabilities to meet threats associated with potential terrorist attacks and other hazards. Over time, the Department has attempted to link dollars spent with the development of capabilities.[10]

Assessing preparedness based on National preparedness capabilities remains very elusive. Summing the difficulties, the U.S. Government Accountability Office (GAO)[11] found that evaluation efforts that collected data on National preparedness capabilities faced limitations such as data reliability and the lack of standardized data collection. According to GAO, FEMA had problems in completing a comprehensive assessment system and developing National preparedness capability requirements based on established metrics. GAO[12] continues to cite these operational and implementation weaknesses, even though the assessment of capabilities and evaluation of preparedness is a legislative requirement. In addition, the GAO[13] specifically found problems with at least one tool mentioned by the new National Preparedness Goal as central to measuring progress—the National Exercise Program. FEMA's implementation of the National program has consistently run into problems, such as ensuring if Federal and State governments had addressed deficiencies identified by the exercises. In March 2011, FEMA developed a new National Exercise Program Base Plan that extensively revised the program, with major changes in requirements and leadership.[14] The verdict is still out whether the past history of the Department of Homeland Security in failing to adequately measure progress will be reversed.

Thus still left unanswered is the most significant question: What preparedness did the billions of dollars buy? With Federal funding constraints and similar challenges for other levels of government and other members of the homeland security community for the foreseeable future, this is an opportune time to consider if other policy options might be more cost-effective, or, at a minimum, justify the current policy of capabilities development and sustainability.

The capabilities approach is not etched in stone. There is at least one policy option the subcommittee might consider to contrast with the capabilities approach. This option is already grounded in Congressional legislation and administration policies: Simply, it is the application of National and/or international management

---

[9] Caudle, Sharon L. 2005. *Homeland security capabilities-based planning: Lessons from the defense community. Homeland Security Affairs I,* no. 2 [Fall 2005].

[10] See, for example, the report Local, State, Tribal, and Federal Preparedness Task Force. 2010. *Perspective on Preparedness: Taking stock since 9/11,* Report to Congress [September 2010].

[11] Jenkins, William O. 2010. *FEMA Has Made Limited Progress in Efforts to Develop and Implement a System to Assess National Preparedness Capabilities.* Letter to Subcommittee on Homeland Security Committee on Appropriations [October 29, 2010].

[12] U.S. Government Accountability Office. 2011. *Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11.* GAO–11–881 [September 2011].

[13] U.S. Government Accountability Office. 2009. *National Preparedness: FEMA Has Made Progress, but Needs to Complete and Integrate Planning, Exercise, and Assessment Efforts.* GAO–09–369 [April 2009].

[14] U.S. Federal Emergency Management Agency. 2011. *National Exercise Program* [March 18, 2011].

system preparedness standards applicable to all organizations, which I have advocated in the past.[15]

There are two National voluntary programs where management system preparedness standards, not elusive core capabilities, are used as the benchmark for preparedness requirements. Legislation implementing many of the 9/11 Commission's recommendations (Section 524 of the August 2007 Pub. L. 110–53) called for DHS to create a voluntary private sector preparedness program with standards, including accreditation and certification processes. In June 2010, DHS produced the Private Sector Preparedness Accreditation and Certification Program (PS–Prep). Three management system standards were approved for adoption in the program: ASIS SPC.1–2009 *Organizational Resilience: Security Preparedness, and Continuity Management System;* British Standard 25999–2:2007 Business Continuity Management; and National Fire Protection Association 1600: 2007/2010 *Standard on Disaster/Emergency Management and Business Continuity Programs.* At the end of September 2010, DHS announced a certification program tailored to the needs of small business.

The other National effort using management system standards is the current Emergency Management Accreditation Program (EMAP), a voluntary review process for State and local emergency management programs. EMAP certifies Government programs against standards directly based on NFPA 1600. State and local entities can use Federal homeland security grant funding to pay for EMAP activities. Interestingly, at one time, FEMA used the EMAP standards to administer its National Emergency Baseline Capability Assurance Program. If there truly is to be a "whole of community" effort, it would seem to be a necessary condition to have a compatible approach for all the entities involved.

Still to be resolved would be whether adoption of the management system preparedness standards should be mandated, perhaps tied to Federal funding or regulations, and how certification or accreditation against the standards would be conducted. Normally, management system standards such as those under the PS–Prep program or EMAP are voluntary, although compliance with such standards may be seen as part of a legal standard of care across an industry.

Government agencies such as DHS could implicitly mandate standards by using them as guidelines for complying with regulatory requirements. Or the agencies may forego a mandatory regulation if they view voluntary compliance as meeting policy goals. This seems to be the Legislative and Executive branch approach taken with the PS–Prep voluntary standards for the private sector. There are established provisions that can be invoked for mandatory adoption as part of National regulatory frameworks or legislation. The National Technology Transfer and Advancement Act of 1995 and resulting Office of Management and Budget (OMB) Circular A–119 (revised in 1998) mandated Federal agencies use management system standards developed by either domestic or international standards bodies instead of Federal Government-unique standards (e.g., the National Preparedness Goal) in their regulatory or procurement activities.

Implementing Whole of Community for the Maximum of Maximums

A second challenge is realistically implementing a "whole of community" effort in anticipation of a "maximum of maximums" effort, at least within 72 hours of a catastrophic incident. In June 2011 testimony, FEMA Administrator Fugate[16] stated that emergency management historically planned for scenarios to which Government could respond and recover from. Instead, he testified that modern disaster planning should be for a "meta-scenario" (or "maximum of maximums" event) destined to overwhelm all levels of Government. Such worst-case planning would require the efforts of a "whole community" approach intended to leverage the expertise and resources of Governmental and non-Governmental stakeholders—the entire emergency management community from the Federal Government to individuals, families, and communities.

The definition of "whole of community" is the same as "all-of-Nation" in the new National Preparedness Goal: "a focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of Federal, state, and local governmental partners to foster better coordination and working relationships."

As the subcommittee knows, the emphasis on shared responsibility and coordination is not new. President George W. Bush's June 2002 proposal to create DHS ex-

[15] Caudle, Sharon L. 2011. "National Preparedness Requirements: Harnessing Management System Standards," Homeland Security Affairs, 7(14) [June 2011].

[16] Fugate, Craig. 2011. Evolution of Emergency Management and Communication. Written statement before the U.S. Senate Committee on Homeland Security [June 8, 2011].

pressed hope that the agency would make State, local, and private sector coordination one of its "key components."[17] The first *National Strategy for Homeland Security* viewed homeland security as a concerted National effort. The approach was based on shared responsibility and partnership involving the Congress, State and local governments, the private sector, and the American people in a concerted National effort to prevent attacks.[18]

Is the "whole of community" approach rooted in a mega-disaster scenario realistic or, more particularly, cost-effective? One visualizes all homeland security actors anticipating a catastrophe such as Hurricane Katrina, a nuclear event, or a worldwide pandemic, that will overwhelm all local and regional partners for a good length of time. It is not clear to me how the Federal Government will actually strategically and operationally determine "whole of community" preparedness for a mega-disaster going forward.

PPD–8 calls for planning frameworks with basic plans for all hazards—presumably a maximum of maximum effort, plus specific threat or scenario annexes. The Implementation details to date do not provide the information on how members of the "whole community" should interact to achieve these capability targets and what scarce resources practically can be invested. It is expected that those details will await the finalization of the National Preparedness System and the publication of all National Planning Frameworks, also required by PPD–8. The National Preparedness System will "guide domestic efforts of all levels of government, the private and nonprofit sectors and the public."[19]

In sum, the focus on "whole of community" may well be noteworthy, but its implementation calls for complexity of coordinated action, assessment, and funding that may be overwhelming and marked by imprecision. A return to "whole of Government" may be more realistic, simply because of the ties to Federal funding. Despite the uncertainty of Government funding, it is reasonable to assume that preparedness will retain its importance, although not perhaps to the hoped levels of National capabilities for a meta-scenario.

Emerging Threat Priorities

A third major challenge I see that the subcommittee might consider in the DHS strategy is addressing threats that are longer-term in their emergence as a direct threat to National security. Among other things, the September 2010 Local, State, Tribal, and Federal Preparedness Task Force[20] report to Congress called for: (1) Improving the ability to strategically forecast emerging preparedness requirements and associated policies and/or capabilities, and (2) develop a strategic policy planning process that prepares for future challenges by performing long-range assessments. The Task Force said that the complexity of the envisioned homeland security and emergency management enterprise, especially in terms of non-Governmental roles, means that desired preparedness outcomes often may take years to achieve. In their view, a range of dynamic issues—such as the environment, demographics, economics, and health trends—are likely to play increasingly important roles. Preparedness policies, therefore, should be anticipatory, not reactionary, enabling anticipatory investments in key areas.

As I mentioned earlier, the hazards listed in the *National Preparedness Goal* reference well-known, specific event hazards and attacks determined by the current *Strategic National Risk Assessment.* However, the current *National Security Strategy and Quadrennial Homeland Security Review Report* explicitly define a strategic threat environment and global trends that appear to have National preparedness implications, although they are not described as imminent. These include the gradual emergencies and disasters that result from dependence upon fossil fuels, global climate change, fragile and failing states, and global illicit trafficking and related transnational crime, and economic and financial instability.

In a 2009 article on National security strategies,[21] I discussed drivers of changes in security on a National and global scale, such as pandemics, population changes, and economic stress. These drivers translate into threats to security, whether individually or collectively, which countries have incorporated into their strategies. In other countries, the security environment includes these longer-term threats. In general, their National security strategies (including those covering homeland security or domestic security) incorporate them into the strategies and follow-on policy

---

[17] The White House. *The Department of Homeland Security.* June 2002. p. 3.
[18] Office of Homeland Security. *National Strategy for Homeland Security.* July 2002, p. 2.
[19] PPD–8. p. 2.
[20] Local, State, Tribal and Federal Preparedness Task Force. 2010.
[21] Caudle, Sharon. 2009. "National Security Strategies: Security from What, for Whom, and by What Means," *Journal of Homeland Security and Emergency Management,* 6(1), article 22.

and operational requirements and guidance. For example, climate change or environmental change pose dangers that may occur on a National or global scale, such as more frequent heat waves, droughts, flooding, reduced crop yields, and wildfires.[22] The Goal and supporting documents target building and sustaining capabilities narrowly for the near-term threat of a meta-scenario. It is not clear how these capabilities will prepare the country for the challenges of the longer-term threats.

There have been a multitude of studies on these drivers or changes with recommendations for immediate action. The Organisation for Economic Co-Operation and Development (OECD) presented an analysis of "global shocks"—cascading risks that become active threats as they spread across global systems.[23] These included pandemics, financial crises, critical infrastructure disruption, and cyber risks, geomagnetic storms, and social unrest. As the OECD study pointed out, surveillance is central to risk assessment and management. In addition, security agencies, working with regulatory agencies, should use, adapt, and implement risk-assessment tools to design more resilient National and international systems. Emergency management of future global shocks, OECD said, called for policy options such as: (1) Surveillance and early warning systems, (2) strategic reserves and stockpiles of critical resources, (3) addressing where countermeasures to systemic threats have been weak, and (4) monitoring of future developments that could pose potential risks. OECD cited challenges such as insufficient skills and knowledge to manage global shocks and obstacles to international cooperation and coordination.

DHS certainly understands the need for action anticipating these global shocks. FEMA's Strategic Foresight Initiative, initiated in 2010, emphasizes the importance of understanding and addressing the drivers of future change.[24] FEMA urges the emergency management community to establish a foresight capability—identifying key future issues, trends, and other factors with an eye to executing an agenda for action over the next 20 years. Not surprisingly, FEMA identifies well-known drivers—universal access to and use of information, technological innovation and dependency, shifting U.S. demographics, climate change, global interdependencies and globalization, Government budget constraints, critical infrastructure deterioration, and the evolving terrorist threat. The FEMA study says that through the foresight process, over the next few decades very rapid change and complexity will define the emergency management environment. FEMA says that even slow-moving and predictable trends such as demographic changes could be radically changed because of drivers such as climate change or pandemics.

FEMA sees a number of emergency management capabilities as needed as part of strategic foresight that could be included in preparedness efforts (pp. 13–20). For example, these include addressing dynamic and unprecedented shifts in local and regional population characteristics and migratory flows; anticipating emerging challenges and develop appropriate plans and contingencies; employing alternative surge models to meet the challenging confluences of social, technological, environmental, economic, and political factors and conditions; and remediating hidden vulnerabilities in critical supplies from water to energy to medical products to offset threats to the full scope of emergency management activities.

Throughout these three challenges, I urge the subcommittee to consider if the current DHS strategies overweigh the opportunity costs in continuing to pursue a comprehensive capabilities approach, insisting on the whole of community being prepared for a maximum of maximum event, and delaying action on confronting longer-term threats.

This concludes my statement. I appreciate the opportunity to appear before the subcommittee today and look forward to any questions you may have.

Mr. MCCAUL. Thank you, Dr. Caudle.

The Chair now recognizes himself for 5 minutes for questions.

Yes, Dr. Caudle, in our home State of Texas we have many homeland security operations on the ground. We have the largest stretch of the U.S.-Mexico border, so we have CBP down there, we have ICE—immigrations is obviously a huge issue in the State of Texas—and then FEMA. Between hurricanes and the wildfires that

---

[22] Hough, Peter. 2008. *Understanding Global Security.* 2nd ed. London: Routledge.

[23] OECD. 2011. *Future Global Shocks: Improving Risk Governance.* OECD Reviews of Risk Management Policies, OECD Publishing.

[24] FEMA. 2012. *Crisis Response and Disaster Resilience 2020: Forging Strategic Action in an Age of Uncertainty.* Office of Policy and Program Analysis [January 2012].

we saw out at Bastrop and all across the State of Texas FEMA plays a huge role.

As I mentioned in my opening statement, though, there are about probably five to 10 different, you know, documents of strategies out there that doesn't unify the DHS mission. So my initial question is: How does this lack of a comprehensive strategy impact these operations that I talked about on the ground and what can we do to fix that strategy so it works?

Ms. CAUDLE. I think overall is coming up, really, with, what is the goal on the border? You know, certainly, as you have mentioned, we are seeing issues around whether or not it is border security, closing the border, stopping illegal immigration or cargo or items that are coming across the border, but then we also have a policy of immigration enforcement in the interior that sometimes is counter to it.

I think overall, looking at what is the overall goal there in terms of the border security and making sure that whether it is ICE or the border security agents there, or the technology, as Mr. Schneider talked about, are all ones that are looking to that security aspect. Right now you do have different types of opinion about what the actual goals are there, and certainly the Texas Department of Public Safety has similar concerns when they talk about border.

Mr. MCCAUL. Well, thank you.

Mr. Schneider, you talked a great deal about the DOD model, Goldwater-Nichols, and how we could apply that model to the management and strategy of the Department of Homeland Security. I have been a big advocate for leveraging existing technologies within the DOD to use within DHS—for instance, sensor surveillance equipment that we use in Afghanistan, using that on the Southwest Border. We talked to the generals in Afghanistan on a recent CODEL—Mr. Duncan was with me—about that very issue.

Can you elaborate more on this DOD model that you think would be effective?

Mr. SCHNEIDER. Sure. Thank you.

Quick background: The Goldwater-Nichols Department of Defense Reorganization Act of 1986 made very sweeping changes to Department of Defense since it was established in 1947. It reworked the command structure of the United States military, and that has led to the origin of why you have combatant commanders, like CENTCOM, PACOM, SOUTHCOM, TRANSCOM, et cetera.

That fundamentally removed the responsibility from the service chiefs from fighting of the war to these combatant commanders that could put together adaptive packages—Army, Navy, Air Force, Special Ops, et cetera—in those regions responding to those unique threats. A fundamental change. Did not go over easy; very difficult, busted a bunch of rice bowls. But the fact of the matter is, if you take a look at how that has progressed since the 1990s, to 2000, to the way we operate today, I personally think it has been a huge success.

It was subsequently followed by the Defense Management Review in 1989, which fully implemented the Packard Commission Report, which led to Goldwater-Nichols. But basically it substantially improved the performance of the defense acquisition system

and managed acquisition resources across the Department. I think by any measure it has worked.

For example, the Air Force's Air Combat Command basically operates aircraft. It does not manage the development and production of the F–35. The COMSUBLANT operates nuclear submarines. It does not manage the acquisition of the junior class submarines.

So the two questions that I ask in my own mind when I look at this relative to the Department is this: Do we want the head of CBP, with 65—excuse me, roughly 65,000 people, 24/7 responsibilities, to keep the incorrect people and the bad stuff out of the borders at the same time that we hold him responsible for putting together very complicated C4 audios or persistent surveillance systems along the border? Is that the right model for the future?

In my mind, the answer to those two questions are absolutely not, and that is why I think it is time to take a hard look at what the operators do, what the warfighters do, operate, and basically provide good law enforcement, and have those people that are smart put together integrated systems using the maximum amount of technology available and satisfy those user requirements.

Mr. MCCAUL. That is a very interesting concept that I know that this committee will be taking a close look at. Have you had any discussions with the Department about using this model?

Mr. SCHNEIDER. When I was in the Department I was—I had the opportunity—and part of my blood is probably in on this floor somewhere—to have that type of discussion. I was frequently asked by Members of the committee that both were in the Homeland Security Committee and very knowledgeable at the Department of Defense whether or not it is time for Goldwater-Nichols.

My answer has always been, at some point in time it is the right thing to do. I thought 4 years ago it was not the right thing to do because it does create a lot of churn and frankly, the Department was still in its infancy. If you take a look at how long it took DOD to actually go implement it after it has been started by any measure I thought 4 or 5 years ago was not the right time. So I have always been consistent in saying that and talking about that.

I think at this point in time, roughly 3 or 4 years later since I was in the Department, it is probably a good time to start thinking about it.

Mr. MCCAUL. Have you had any discussions with the current administration about this?

Mr. SCHNEIDER. No. No. I really, for the most part, stay hands away from the Department.

[Laughter.]

Mr. SCHNEIDER. That is by choice.

Mr. MCCAUL. I see my time has expired. I know the Ranking Member is going to follow up on a line of questioning that I am very interested in, as well, and that is the recent cyber markup of the National Information Sharing Organization.

So with that, I recognize the Ranking Member.

Mr. KEATING. Great. Thank you, Mr. Chairman.

I do want to get into those questions, but I do want to follow up on just what you were saying, Mr. Schneider, too. You know, I have seen CENTCOM work in the counterterrorism and it was a wonderful thing to see, frankly, the way so many different areas of gov-

ernment and the—and defense worked together in one room, in one central command. I was so impressed and pleased.

The trouble I have, as great as that model is—and I have seen it happen and I have seen it work—we can't get the basic jurisdictions of homeland security settled first. So, you know, I agree with you in theory about that is a great approach, but do you honestly think in this time frame that we mentioned, since we haven't even set the jurisdictional problems that were still there from the 9/11 recommendations and still unfulfilled. In that framework how could we, at this time, ever overcome that without dealing with the jurisdictional issues that have to be dealt with first?

Mr. SCHNEIDER. Well, thank you. Thank you, Congressman.

I think the way to do that is to accept, basically, something less than 100 percent solution. So if you go at—I used to travel a tremendous amount of time on the weekends when I was the deputy secretary. If you go visit many of the major ports and key city areas—I don't care whether it is Detroit, San Diego, Charleston, Seattle, Miami, et cetera—what you see is, frankly, the individual organizations with, I will call it the alphabet soup labels, informally working together—working together. Not just within the DHS, but go to San Diego, they work with the Navy, they work with the San Diego Harbor Police, they work with local law enforcement.

The reason is basically is this: You have all these organizations, you have sea assets, you have got air assets, and things like that, so the smart people that are at a lot of these places informally figure out a way to basically—figure out how to maximize the effective use of all of those assets. So I think you could do it, quite frankly, in—at not, maybe, 100 percent, but at least within the context of making substantial progress. That is why I really believe that you could do it.

Mr. KEATING. Okay. I would love to see that happen in reality, but I would say we would be lucky to get 10 percent the way things are going.

But in any case, I have a question: We had a field hearing earlier this year in the Port of Houston, and, you know, there really struck me a great deal of how important that is to our security in so many respects and the economic impact these could have. Now, the President included the Nation's homeland security agenda within the National Security Strategy, and in that he included climate change as well as violent extremism, but also natural disasters.

Dr. Caudle, how has this, you know, revamped whole-of-government approach to homeland security strengthened the Nation's preparedness? Because I think we saw first-hand what could happen if there was a—not only a terrorist attack but a natural disaster in something like the Port of Houston or in Cape Cod.

Ms. CAUDLE. You know, certainly in theory the whole-of-government, the whole-of-nation, whole-of-community I think is fine as a theory. My problem with the language around that is how do you practically leverage, really, the resources and goals of all of the different communities all the way down to the individual level?

It is one of those things that I think it is a principle that we have seen consistently, in fact, since 9/11, if not before, about having everyone working together. The practical implications of the new Na-

tional preparedness goal that the President issued that really is a continuation, if not an enhancement of what President Bush issued in his Presidential Directive. I ask for what does this really look like in terms of preparedness on the ground because you still have, as you mentioned, jurisdictional issues, you still have issues with resources, you still have people that are concerned with existing capabilities, equipment, hazmat suits, and the like.

How do they sustain that and where is the money going to come—anyway, and then the other thing is this whole issue of whether or not the Federal Government can put together this preparedness approach that really does not have an existing framework and hasn't had, really, a strong existing framework for management for the past decade.

Mr. KEATING. Yes. I think, you know, just quickly, and a common theme I have seen is the idea that we are retrofitting our security issues with budgets.

You know, what I am afraid of is the next disaster that comes we will just start spending and reacting to it and no one will be objecting then, but I really think that in the larger sense that this is very interesting here, and I appreciate both your efforts to try and do what I call retrofitting the budget we have. I really think, you know, the explanation has to be more expansive than, say, "Here is what we are facing," and I think the American public will agree that that is a great investment of our tax resources.

I have run out of time. If you get to fit into it, you know, Mr. Schneider, we did have a hearing and a markup recently on this committee where we moved forward with a public-private approach to cybersecurity. I don't know if you have a—can comment now or later, but that is something that we have basic agreement on in this committee.

Mr. SCHNEIDER. If I may, briefly, cybersecurity is very, very difficult, and I realize, frankly, from the perspective of the committee there are so many different committees with different jurisdictions of cyber, and you have to rational—you know, my answer here would be this: I would also agree to—or proceed to accept the half a loaf or a quarter of the loaf rather than solve the world hunger problem.

The reason is this: You have to rationalize so many different things. If we talk about cybersecurity in the utilities, what about the FERC? If you talk about cybersecurity and the companies on the exchange what about the regulation of the SEC?

What about the privacy issues? If somebody basically secures a network, how are they identified in case there is a problem in this massive exfiltration and economic loss? You have the economic trade issues and things like that.

So I would urge you to do this, quite frankly: I know how hard this thing is, and I think if you can make some incremental progress area by area this year, accept that as success and then move on.

Mr. KEATING. Thank you, Mr. Schneider. I am over my time.

Mr. MCCAUL. Thank you for your testimony.

The Chair now recognizes the gentleman from Missouri, Mr. Long.

Mr. LONG. I have only got 14 seconds left.

[Laughter.]

Mr. LONG. Thank you, Mr. Chairman.

Thank you all for your testimony here today. Just because I am an auctioneer they always want me to talk fast.

But, Mr. Schneider, to follow up a little bit on that, how can we better handle cybersecurity? You are talking about all these different committees and all these different cybersecurity jurisdictions, and we all know that it is a huge problem and I think that Leon Panetta is the one that said that our next Pearl Harbor is going to be a cyber attack. You see attacks every day and they are just going to get more egregious so we really, really need to get ahead of the curve on this if we can.

I know in my hometown of Springfield, Missouri we had some folks that—I think it was $440,000, they owned a little tiny title company, a land title company, and there was $440,000 removed from their bank account over the weekend, and I can't remember now what country it—Afghanistan, I think it ended up in, but what is your suggestion? What is your recommendation for getting ahead of the curve on this? Everybody gives it a lot of lip service but I never really hear anybody drilling down on it.

Mr. SCHNEIDER. Thank you for the question. I appreciate that.

I think you have to do two things. No. 1, you have to recognize—and this is my own personal opinion, and I spent most of my life in DOD, is that when DOD talks about cybersecurity they are really talking about, in many cases, a potential for cyber warfare, and what is the escalation curve——

Mr. LONG. You spent most of your life in what?

Mr. SCHNEIDER. In Department of Defense.

Mr. LONG. Okay. I thought you said DOT——

Mr. SCHNEIDER. No, no, no, no. No, I was——

Mr. LONG. I don't like acronyms. I am still trying to figure out what D.C. stands for, so—spell it out for me.

[Laughter.]

Mr. LONG. I thought you said DOT. I am sorry——

Mr. SCHNEIDER. No, I am sorry. I wasn't clear. So Department of Defense.

When they talk about cybersecurity a lot of what they are talking about has to do with cyber warfare, escalation, attribution, and what do you do. When DHS, much to their credit, though they have the spearhead responsibilities, a lot of what they talk about is, frankly, securing dot-gov. Dot-gov is that domain that basically is the Government's network. The problem is you have the DHS piece and then you have all these other departments.

What I think we need to be doing is to focusing on not the big defense companies, because they have millions of dollars to spend on network security. I am talking about the small, the mid-sized companies. I am talking about the State and local.

I think we need to figure out a way so that the Government can assist in the development of these cyber secure operation centers that can be done locally, regionally, in many ways like physical security except it is cybersecurity. Come up with a commoditized scheme by which a lot of these State and local, small, mid-sized companies in these jurisdictions can have affordable cybersecurity for their networks.

That takes a fundamental shift in focus from the big DOD, DHS, dot-gov, dot-mil systems to the rest of the country. I believe that, if properly incentivized, the industry, which—with its expertise in this area, could make a financial market to invest in this area and expand. That is just one thing I would do.

The other things you could do is just self-education. There is a lot of bad information that is out there about what you have to do, and if one could sponsor a series of forums—educational events and seminars and things like that would have widespread regional and local distribution, that would go a long way for basically informing the general public of the seriousness of the problem.

Mr. LONG. Say that again, that last part again. If you had regional what?

Mr. SCHNEIDER. Cybersecurity operational centers and educational forums. I think it would help raise the educational level of awareness of the public of the severity of this problem.

I honestly believe that until you personally get hacked and pay a price, like happened to me about 2 weeks ago, it becomes real, okay? So what you have to do is raise the awareness of the general public, not just the high-profile players like DHS and DOD and the dot-gov, dot-mil folks, but the rest of the population.

Mr. LONG. But if we have got too many people trying to watch the pot how do we correct that? I mean, if we have——

Mr. SCHNEIDER. You have always got to have—you are always going to have the people. There are so many different jurisdictions of this and there are so many potential impacts, and to be honest with you, you have a reluctance, as happened yesterday, I heard on the radio, of companies that have serious problems—cyber attacks—from divulging that. The reason is they don't want to affect their stock price; they don't want to see a run on their investors, and things like that.

So there has to be some sort of a truth in discussion ground rules that are set up for this. This is a massive problem that is not going to be solved in a year, and that is why I really think the right thing to do is agree on a consensus on a couple small pieces that make a difference, approve them, and then start working on the next set.

Mr. LONG. Okay. Thank you. I am past my time.

I yield back.

Mr. MCCAUL. Thank you.

Just to follow up, the sharing of information, that is something we try to put forth in this bill—and I know Intelligence Committee has one as well—to protect that information so that these companies can share that with the Government without it being divulged. You are right, they have a duty to their stockholders.

I think on the education and awareness piece, I know NSA has said that probably 70 percent of this could be through education and awareness computer hygiene—proper, you know, computer hygiene, so—with that, I now recognize—Chair recognizes the gentleman from Illinois, Mr. Davis.

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

Let me thank the witnesses for being here.

Mr. Schneider, in your testimony you propose that the Department should shift its business model for scanning equipment out-

side of the Government and focusing on outsourcing to commercial vendors. As you also rightly note, this is a model that is frowned upon by the Office of Management and Budget due to the cost.

Would it not be wiser to keep those funds in house or inside and use them to build on science and technology within the Department, and perhaps we get a little bit more mileage out of that?

Mr. SCHNEIDER. Thanks. Thanks for the question.

This is one of those situations I feel that unless you had the job I had, it is not very obvious to the outside world. When you take a look at the budget, this is the budget of reality, and Congress has been kind enough to increase, over the years, the amount of operational law enforcement people.

If you take a look at the Department, the amount of dollars required for salaries, throw in a couple of billion for the Disaster Relief Fund, throw in a couple of billion for the grants, that is about 70 percent of the dollars that are appropriated. That doesn't leave much money. A big chunk of what that remaining money is is IT.

So when you are faced with massive scanning equipment that is out-of-date and you need to refurbish it or you need to update it you are talking about big bills. From my standpoint, when I was there and especially today, the Department will never get that amount of money to do this. These are very expensive machines.

We are very fortunate that medical technology—imaging techniques and things like that—drive innovation. I am hopeful that with the advent of dental technology and the like it will increase the capability of the machines, but the simple fact is when you are there you just don't have the money, and my take is you will not have the money in the future, to actually go out and buy these machines and then worry about refresh, update, et cetera, and maintenance.

So my recommendation would be change the business model. Not basically outsource it, but get a long-term lease with—just like the IT providers do today, you have service level agreements, reliability, refresh requirements, and things like that, and pay as you go. It is a financing matter, in my mind, and it accepts budget reality that you will never get the big chunk of money you will need.

Frankly, I had great difficulty with the folks at OMB in this matter, and this gets back to—this gets to the issue of whether it is a capital lease or an operating lease, and I have been away from it too long to remember the differences, but the one that they don't like is what they consider this type of a scheme. I, personally, at the time, thought that they were wrong.

So you are not outsourcing, you are basically leasing. You can call that an outsource, but it is no different than your car.

So I just am heavily biased by the budget reality that I lived under, and more importantly, the more stringent budget reality today. I think this really needs to be looked at.

Mr. DAVIS. Well, thank you very much. It seems to me that we do a great deal of experimenting, I mean, almost every time. I mean, the airport that I use most frequently and there seems to be a different approach.

But thank you very much, and let me thank you.

Dr. Caudle, let me ask you, is it safe to say that the National Security Strategy released by President Obama was drastically different from the strategy that was released by President Bush?

Ms. CAUDLE. In terms of tall—I mean, calling it drastic, I think in both strategies there is recognition of the strategic threat environment that the Nation faces. The difference that I saw in what President Obama put out was this emphasis on placing homeland security within National security. You could see it coming and I think it—to my mind it certainly made a lot of sense to do that because homeland security, as you know, doesn't stop at the borders, is a cliché that we normally will say, and so extending the borders out in terms of National security and what we do overseas internationally, what we do with our defense establishments, as well, has implications for homeland security. So that is what I saw as a—the major feature.

There also was an emphasis on some other areas in engaging partners that was a stronger emphasis, but by and large, at least from my area of expertise, that encompassing homeland security—and what it said to me, as well, was that it was likely we will not have a National strategy for homeland security. The Quadrennial Homeland Security Review report that tended to replace the 2007 National Strategy for Homeland Security—I think now we will only see that National Security Strategy, so taking it as the document for, really, what are the goals that are laid out there, but then how do you operationalize, you know, as I am sure others will talk about.

Many of these National strategies are almost statements of principle. What the SEVA committee is focusing on is: What is this boots on the ground? What are the realities? What is the management scope that you really need to start paying attention to? What is the oversight? Where is the money going? Where is the personnel going?

So that is where—the strategies are fine, the new emphasis on homeland security, but how do we drive it down now for the preparedness, for the security that the Nation is asking for?

Mr. DAVIS. Thank you very much. It is a little build on what we are already doing, I would assume. Thank you very much.

Thank you, Chairman. I yield back.

Mr. MCCAUL. Chair now recognizes the gentleman from South Carolina, Mr. Duncan.

Mr. DUNCAN. Thank you, Mr. Chairman. Thanks for the timeliness of this hearing, especially coming in the wake of a hearing yesterday in Foreign Affairs where we talked about the Iranian threat within the hemisphere and globally.

I want to thank you for mentioning the trip to Afghanistan because since we were there in November I have given a lot of thought to our border security here in this country, and it is, you know, no secret that I believe that one of the roles of the United States Government is to defend the sovereignty of this country, and I look simply at our porous Southern Border and wonder what we can do, what we should be doing, what we can do more of, and where we are making mistakes.

So as we talk about the effective implementation of a strategy I wonder what is the actual strategy of the Department of Homeland

Security with regard to the border, because I read report after report that says we should put our emphasis here or should put our emphasis here. Mr. Chairman, I think about that Pakistani-Afghan border where there is a natural port of entry on Main Highway 1 that we saw, but then the berm that was created and the, I think, 60 cuts in that berm that allowed illicit activity to come across.

When we think about Afghanistan we think about IEDs and Taliban fighters and enemy combatants coming across, but what we were told is what is trying to circumvent that natural border crossing was money, drugs, and weapons. It really wasn't the Taliban or enemy combatants or IEDs, that most of those were attempting to come through that natural port of entry.

So thinking about that and thinking about the September 2011 GAO report that cited DOD officials who are concerned that there is no comprehensive Southwest Border security strategy and the National Guard's role has been ad hoc, and then I look at this Texas Border Coalition's January 2012 recent report that talks about—we have put a lot of our emphasis on border crossings outside of the natural ports of entry. It has really brought my focus back to the border crossings and the ports of entry.

Reading this I learned that there are 52 border crossings in the Southwest, eight of which are rail, 43 are roadways, there are 24 bridges, two dams, 17 roads, and one ferry. So when you go to approach a problem you look at what are the easiest things to do, you address those first, then you broaden your scope until you solve the problem.

This year I have had the opportunity to go to Israel and look at the West Bank border crossings, what Israelis have done with fencing and ports of entry, and interdiction back in their country and the timeliness of it. So the question I have for you guys is why, based on this Texas Border Coalition's report saying our problem, most of the drugs and illicit activity that are coming across are not circumventing those ports of entry and coming across that no man's land, so to speak, on our border; a lot of it is coming through that natural port of entry where we have got the personnel.

You all have mentioned the number of—the increase in Department of Homeland Security Custom and Border Patrol personnel just in the last decade, and my gosh, from $400 million to $3.6 billion we have spent a lot of money on focusing on the Southwest Border, but are we not being effective if we are not focusing on the easiest thing, and that is where we are funneling that traffic through a natural port of entry where we already have systems in place? So what should we be doing there? How can we start there and then expand it to the fencing, the areas of surveillance and other things in the no man's land, so to speak, where we don't have a port of entry?

So my question to you, Mr. Schneider, is what should we do on the ports of entry? How can we make sure we do the easy things first?

Mr. SCHNEIDER. Congressman, first, I am a little dated because I have been out of office for 3 years, but I can tell you that based on what I experienced when I was in the Department that the more we basically put up fencing, the more we used air assets, it focused people on the ports of entry. That is why what we saw, in

many cases, at some of the ports, the—I will call it the frustration by the bad people to actually force their way, brute force, bad incidents right through the ports of entry.

So I know what we did at the time was to really beef that up relative to the security, beef that up relative to at the ports, the entry procedures that they have to do to basically get approval to cross, and frankly, rely heavily on intelligence and awareness and things like that. That is true of the personnel crossings and that is true of especially the border crossings with heavy automobile traffics, from the large ones, like at San Ysidro, to some of the small ones——

Mr. DUNCAN. Let me ask you this, because we are about out of time, but do you feel like they are just overwhelmed based on the amount of traffic that comes through those port of entries?

Mr. SCHNEIDER. Traffics are huge, and they are going to get huger. I know there is a modernization plan to expand that.

I think a lot has to do with intel. I don't know what is classified and unclassified; I am removed. But I can tell you, when you start talking about interfaces with DEA and ATF and things like that, and who passes what, and different analysis techniques and things like that, when I was there we were using that and using that effectively. I can only assume that just based on a lot of how that technology has evolved over the years and greater workings with some of these other organizations on intel that the performance in responding to that threat has gotten greater. But again, I am a little dated.

Mr. MCCAUL. Thank the gentleman.

I have been informed we have votes coming up in just a couple of minutes. I think this worked out perfectly.

So the Chair now recognizes the Ranking Member of the Cybersecurity Subcommittee, Ms. Clarke, from New York.

Ms. CLARKE of New York. Thank you very much, Mr. McCaul.

Thank you to our panelists for your testimony today. I just wanted to note that with respect to the GAO report, General McCaffrey also stated that as part of the strategy we need to include comprehensive immigration reform, and that is always a major part of a missing link when we are talking about our border security.

But my question goes to you, Mr. Schneider, and it is with regards to the references that you have made in your testimony specifically around Goldwater-Nichols. I know that you are a proponent of DHS adopting Goldwater-Nichols.

Some of us disagree with the assertion that Goldwater-Nichols' framework is applicable at DHS, because as you rightly stated, it has still not reached its maturity. By your own testimony, DOD was established in 1947 but Goldwater-Nichols, although authorized in 1986, did not take effect until 1989—so 42 years after DOD was stood up.

So given this time frame, do you think that DHS is still not ready, especially—don't you think that it is not ready, especially in light of its other challenges, for Goldwater-Nichols?

Mr. SCHNEIDER. No. I think it is ready, and the reason is if you take a look at the long historical basis for a lot of the services—Army, Navy, Air Force, Marine Corps, et cetera—I think it was a tougher nut to crack, to put it mildly. I fought the world change,

quite frankly, when in the late 1980s I was watching TV and I think it was Haiti I saw on the helicopters flying off the decks of the United States Navy aircraft carrier. So fundamentally things worked better, packaging the right amount of people from the different specialties, et cetera. That is why Special Ops gets a lot of credit to these days, and that is why I think these combatant commanders do a good job.

I am not sure that there is any right time, and I am not sure how long it is, but the fact of the matter is, the longer you wait on something like this the less possibility you are going to have of reaching some earlier amount of effectiveness than if you waited. So I think it is different, quite frankly. Law enforcement is different than the military, and I learned that from being in the Department.

Ms. CLARKE of New York. Dr. Caudle, for the first time ever President Obama including the Nation's homeland security agenda within the National Security Strategy. Furthermore, he included in his strategy climate change, violent extremism, and National disasters. How has this revamped the whole-of-government approach to homeland security and strengthened the Nation's preparedness?

Ms. CAUDLE. You know, certainly at present we don't see the follow-on of those emerging threats in the current National preparedness system that DHS has put up. The new National preparedness goal, the capabilities, and so on, specifically talked about only near-term threats, a beginning and end. So these emerging threats, they are saying, are something that will be under consideration with the next Strategic National Risk Assessment Review.

Certainly it is important. FEMA is working on their Strategic Foresight Initiative, which has identified that as an issue that should be addressed.

So we will have to wait and see how it is actually incorporated. There is some discussion in the National preparedness goal documents about mitigation, but they tend to be still for only a near-term, beginning-and-end-type disaster. So hopefully we will be seeing that emerge hopefully over the next several years.

Ms. CLARKE of New York. Let me ask—and this is to you, Dr. Caudle—the previous administration's National Security Strategy and National Strategy for Homeland Security excluded response to natural disasters from its definition of homeland security. How has the inclusion of this term in new strategies strengthened our response system, and as efforts are taken to further reconcile definitions of homeland security should there be an effort to make sure natural disasters continue to be included in the definition?

Ms. CAUDLE. Well, certainly. The new homeland security definition, although it is not in legislation, really speaks to the all-hazards approach, from terrorism, natural disasters, accidents, and the like, so you really have encompassed in homeland security all of the threats and hazards or drivers of those threats and hazards that are important.

The inclusion or non-inclusion almost became moot after Hurricane Katrina because the country realized that natural disaster—the Deepwater Horizon oil spill also was another indicator of these are the types of threat and hazards that are not just terrorism that the country should be paying attention to.

Ms. CLARKE of New York. Thank you, Mr. Chairman. I yield back.

Mr. MCCAUL. I thank you.

Let me just—I would like to enter into the record, if there is no objection, the Texas Border Coalition report. It basically says without strategy America's border security blunders facilitate and empower Mexican drug cartels. It says America's border security effort lacks strategic direction and operates on an ad hoc basis. So without objection, I would like to enter this report into the record, as well.

[The information follows:]

STATEMENT OF THE TEXAS BORDER COALITION

JANUARY 12, 2012

WITHOUT STRATEGY: AMERICA'S BORDER SECURITY BLUNDERS FACILITATE AND EMPOWER MEXICO'S DRUG CARTELS

The United States Government spent about $90 billion over the past decade to secure the U.S.-Mexico border.[1] The results are mixed, with apprehension rates up to 90 percent for undocumented persons seeking to cross the frontier between designated U.S.-Mexico border crossings, yet the Mexican drug cartels continue to enjoy commercial success smuggling more drugs than ever into the country through the legal border crossings.[2]

"America's border security effort lacks strategic direction and operates on an ad hoc basis."

A significant part of the $90 billion Government expense has been the deployment of U.S. military forces, including the National Guard, to supplement Border Patrol and Customs and Border Protection forces on the Mexican border. A recent Government Accountability Office briefing on the costs and benefits of the Department of Defense role in securing the Southwest land border reported that DOD officials "are concerned that there is no comprehensive southwest border security strategy" and the National Guard's role has been "ad hoc."[3]

As the United States spent $90 billion seeking to secure the Southwest Border, the Mexican cartels have continued to smuggle cocaine, heroin, and methamphetamine through the legal border crossings in California and South Texas, and marijuana between border crossings in remote areas of Arizona.[4] They generally smuggle smaller loads of cocaine, heroin, and methamphetamine in non-commercial vehicles (cars, SUVs, and pickup trucks) to blend in with cross-border traffic.[5]

As the Mexican drug cartels flourish in the face of $90 billion spent to secure the border through which they conduct their trade, the United States continues to focus on border security tactics grounded in operation that began in the 1990s when an anti-immigration backlash fueled crackdowns code-named "Operation Gatekeeper" and "Operation Hold-the-Line." Debates in Congress focus on building more fences and walls and whether to snuff environmental protections for public lands on the Southwest and Northern Borders.

"The legal border crossings on the U.S. southwestern border have become America's weakest border security link."

As reported by the Department of Defense and the Government Accountability Office, America's border security effort lacks strategic direction and operates on an ad hoc basis. Without a strategy, America will continue to lose the border security war to the better financed, equipped, more mobile and agile drug cartels. Our National success depends on defining and executing a strategy to defeat the cartels attacking our Nation.

---

[1] "$90 billion spent on border security, with mixed results," *Boston Globe,* June 26, 2011, Martha Mendoza, Associated Press.

[2] Ibid.

[3] Observations on the Costs and Benefits of an Increased Department of Defense Role in Helping to Secure the Southwest Land Border, GAO–11–856R September 12, 2011.

[4] U.S. Department of Justice National Drug Intelligence Center "National Drug Threat Assessment 2011" August 2011.

[5] Office of National Drug Control Policy, the White House, "National Southwest Border Counternarcotics Strategy", June 2009.

The legal border crossings on the U.S. Southwestern Border have become America's weakest border security link. Since the cartels choose to smuggle most of their products through the border crossings, a sensible strategy would be to attack their trade where it occurs and anticipate where their smuggling operations might move in response. Yet, the Department of Homeland Security has chosen to ignore these developments and refused to develop a strategy to confront them.

Budget forecasts by Department of Homeland Security officials suggest no new funding for border security infrastructure at the official border crossings for many years and personnel accounts will essentially remain static during that time.[6] While new equipment may become available, some cannot be utilized because the electrical facilities at the border crossings are outdated and inadequate to support the expensive new tools.

Congress and the administration confront a choice when considering strategic directions for securing the U.S-Mexican border. At a minimum, the Texas Border Coalition recommends that Congress and the President have a strategy rather than addressing this challenge ad hoc.

"Spending additional billions of dollars on more fencing-walls or exempting the Border Patrol from the rule of law should be lower priorities until the border crossings can be made functional in securing our borders."

The strategic paths forward offer a choice between closing the gaps between the border crossings, where criminals face a 90 percent likelihood of apprehension, or addressing the inadequate infrastructure, technology, and law enforcement personnel at the Southwest Border crossings where criminals are less challenged by an apprehension rate of merely 28 percent.

The Texas Border Coalition suggests that the only reasonable path forward is to refocus our border security priorities where our Nation is most vulnerable: At the legal border crossings. Spending additional billions of dollars on more Border Patrol agents, fencing-walls, or exempting the Border Patrol from the rule of law should be lower priorities compared to making the official border crossings functional in securing our borders.

To choose the other path and continue to fight the border security war where it has been won (between the border crossings) and to continue to surrender the war where we are losing (at the border crossings) is to threaten our National and border security and resign our Nation to defeat.

This document is focused on the security aspects of border strategy, especially as they related to Mexican drug cartels. There are additional benefits to improving the security at America's border crossings, including facilitation of legitimate trade and travel with Mexico, providing a major benefit to the American economy and jobs.

U.S. manufacturers and consumers depend on ready access to Mexican markets and goods. U.S. exporters serve the Mexican market and profit from foreign sales. Border region businesses in Arizona, California, New Mexico, and Texas tie their livelihoods to trade and create jobs for American workers. Mexico is America's third-largest trading partner behind only Canada and China.

U.S.-Mexico trade totals $400 billion, a nearly five-fold increase since the enactment of the North American Free Trade Agreement (NAFTA), with most goods crossing via commercial truck. More than 13,000 trucks bring over $630 million worth of goods into the United States from Mexico every day. U.S. exports to Mexico total $163 billion.[7]

As a matter of general strategy, America cannot solve our budgetary problems solely by cutting expenses. We must increase our revenues. Making our border crossings more efficient in conducting legal trade with both Canada and Mexico will increase our National revenues and give us the resources to fight the other problems we face in our borders.

BORDER SECURITY BACKGROUND

The U.S. Government divides its effort to enforce the land border with Mexico into two parts: One at the border crossings and the other between them. Along the nearly 2,000-mile border with Mexico, 42 official border crossings—located on bridges in Texas and on highways in California, Arizona, and New Mexico—connect the two nations, under the command of U.S. Customs and Border Protection (CBP). The CBP has multiple responsibilities, including facilitation of legal travel across the borders as well as defending against terrorist intrusions. Within CBP, the U.S. Bor-

---

[6] "Meeting Land Port of Entry Modernization Needs in Constrained Budgetary Environment," presentation by Mikhail Pavlov to the Joint Working Committee, October 2011.

[7] U.S. Department of Commerce, Bureau of the Census, Foreign Trade Division annual report, 2010, Washington, DC.

der Patrol has responsibility for policing the vast areas that separate the border crossings. CBP Officers handle traffic through the official border crossings.

"The probability of an illegal crosser being apprehended by law enforcement between the border crossings is about 90 percent; the probability of an illegal crosser being apprehended attempting to enter the U.S. at the border crossings is about 30 percent."

Since 1993, the United States has engaged in a long-term effort to increase enforcement on the Southwest land border with Mexico. It has invested heavily in manpower, technology, transportation, and infrastructure to arrange a multi-layered defense against illegal activities, but that investment has lacked balance.

The investment in deterrence has been greatest between the border crossings; in contrast, the investment at the border crossings themselves has been relatively small. This imbalance has produced a substantial differential of risk to those who seek to penetrate the border to cause harm to U.S. security. While there is admitted weakness in some of the data, the probability of an illegal crosser being apprehended by law enforcement between the border crossings is about 90 percent; the probability of an illegal crosser being apprehended attempting to enter the United States at the border crossings is less than 30 percent.

This imbalanced deterrence contributes to America's vulnerability to the Mexican drug cartels, terrorists, and traffic in people and contraband at the designated border crossings.

BETWEEN THE BORDER CROSSINGS

Since 1993, the number of agents deployed to secure the borders between the border crossings has more than sextupled from 4,000 to a projected total of 24,285 in 2012.[8] The Border Patrol budget has increased nine-fold over the same period from $400 million to $3.6 billion.[9]

"In 2010, the value of cross-border travel at the U.S. border crossings and exports with Mexico and Canada totaled more than $791 billion."

The vastly expanded effort between the border crossings accelerated in the aftermath of the September 11, 2001 attacks and the 2003 incorporation of the Border Patrol into the new Department of Homeland Security. Prior to September 11, 2001, the Border Patrol's priority was to prevent the illegal entry of people and contraband into the United States between the border crossings. After the September 11 attacks, fighting terrorism was established as one of the agency's prime responsibilities.

In addition, Congress funded construction of 670 miles of border fence, now completed at a cost to taxpayers of over $2.4 billion,[10] and an electronic detection system that has been canceled and restarted at a cost exceeding $1 billion.[11]

AT THE BORDER CROSSINGS

Despite expanded responsibility and an exponential increase in legitimate trade and tourism across the Southwestern Border as a result of the North American Free Trade Agreement's ratification in 1993, the enforcement budget for Customs inspection personnel has seen a paltry boost when compared to the sharp increase in funding for the Border Patrol. Funding for inspectors increased from $1.6 billion in 1993 to $2.9 billion in 2012.[12] Of that 80 percent increase over 19 years, nearly three-quarters was consumed by rising inflation.

The United States has 163 official border crossings. The General Services Administration (GSA) owns 96.5 and leases 22.5. The National Park Service owns one. CBP owns the remaining 43, of which 39 are located on the Northern Border. The CBP border crossings are relatively low-volume entry points, such as those on the Canadian border that handle fewer the 100 vehicles a day, while the GSA border

---

[8] Congressional Budget Justification, Fiscal 2012, U.S. Department of Homeland Security, Washington, DC, February 2009.

[9] Ibid.

[10] GAO–09–896 Secure Border Initiative: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed, Washington, DC, September 2009.

[11] Ibid.

[12] Congressional Budget Justification, Fiscal 2012, U.S. Department of Homeland Security, Washington, DC, February 2009.

crossings tend to be larger and have higher traffic volumes, such as at Laredo, Texas, which sees several hundred every minute.[13]

On the U.S.-Mexico border, there are 52 border crossings in all, of which 8 are rail lines, 43 are roadways (24 bridges, 2 dams, and 17 roads), and 1 is a ferry. For record-keeping purposes, the Government divides the crossings into 26 crossing groups, with data from a set of neighboring crossings aggregated under the name of a master port.[14]

"The emphasis on Border Patrol enforcement between the border crossings has shifted factors of risk associated with illegal crossings."

United States and Mexico facilitate 240 million legal crossings a year, nearly 30,000 per hour. The United States' two largest export markets are Canada and Mexico. In 2010, the value of cross-border travel at the U.S. border crossings and exports with Mexico and Canada totaled more than $791 billion.[15] Three out of four of all legal entries into the United States occur at an official border crossing.[16]

ROLES NOT INTERCHANGEABLE

The operational roles of the Border Patrol and CBP inspection officers are not interchangeable. Few recommend attempting to solve the imbalance between the two forces by reassigning Border Patrol agents to the border crossings. Besides weakening security between the border crossings, the training and outlook of the two forces does not qualify Border Patrol agents to substitute for CBP officers.

The primary activity of a Border Patrol agent is to Line Watch: To detect, prevent, and apprehend terrorists, undocumented aliens and smugglers. The Border Patrol does not recognize any legitimate activity in crossing the border between the border crossings.

"Apprehensions of persons seeking to enter the United States between the border crossings—where all entries are illegal—has fallen to levels not seen since 1970s, as the enhanced manpower, mobility, communications, technology, and infrastructure have been brought to bear on the traffic."

While CBP officers also defend against terrorist intrusion by identifying high-risk individuals who are attempting to enter into the United States at the border crossings and stopping criminal activities, they have additional responsibilities that are quite different from the function of Border Patrol agents. CBP officers are responsible for regulating and facilitating legitimate international trade and travel, collecting import duties, and enforcing hundreds of U.S. regulations, including trade, drug, and immigration laws. CBP officers must be able to distinguish between legitimate activities and those that violate our laws as they interact with the public in a polite and respectful manner.

MULTI-LAYERED STRATEGY

The multi-layered strategic deterrence built by the Border Patrol between the border crossings has increased the difficulty of illegal crossings, although controversy remains about the deterrence associated with individual layers or whether the effort actually deters migrants who are determined to the enter the United States to improve the economic state of their families.[17]

The emphasis on Border Patrol enforcement between the border crossings has shifted factors of risk associated with illegal crossings. Interviews with migrants show that the use of "coyotes"[18] for illegal crossings has increased markedly, which

---

[13] OIG–10–05, Review of the U.S. Customs and Border Protection Expenditure Plans for the American Recovery and Reinvestment Act of 2009, Depart of Homeland Security Office of the Inspector General, Washington, DC, October 22, 2009.

[14] Atlas of the Land Entry Ports on the U.S.-Mexico Border, Border Policy Research Institute, Western Washington University, Bellingham, Washington, Fall 2010.

[15] U.S. Department of Transportation Bureau of Transportation Statistics, Trans-Border Freight Data, *http://www.bts.gov/programs/international/transborder*.

[16] GAO–08–329T: Despite Progress, Weaknesses in Traveler Inspections Exist at Our Nation's Border Crossings: Statement of Richard M. Stana, Director, Homeland Security and Justice Issues, Washington, DC, January 3, 2008.

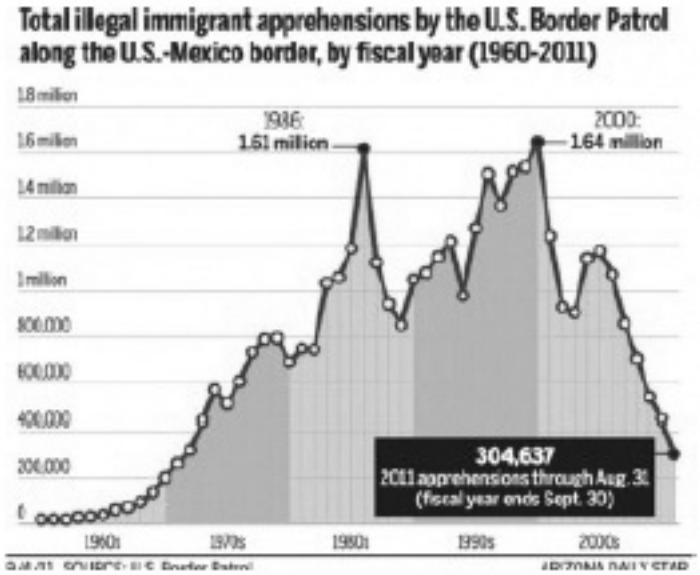
[17] Evaluating U.S. Immigration Control Policy: What Mexican Migrants Can Tell Us, Wayne Cornelius, Director, Center for Comparative Immigration Studies, University of California, San Diego, CA, April 14, 2009.

[18] A coyote or pollero is a professional criminal specializing in smuggling humans across the United States border from Mexico for a fee paid in advance.

boosts the probability of successful illegal entry. This demand has also increased the cost of services.[19]

WEAKNESS OF DATA

The lack of statistically reliable data related to the number of undocumented aliens residing in or entering the United States year-over-year hampers effective analysis related to border security. In addition, in spite of the data's inherent weakness, Department of Homeland Security agencies consider some volumes of related data to be "law enforcement sensitive" and restrict public and academic access to it.



For instance, estimating the flow of undocumented migrants is often an approximation based on apprehension data reported by DHS. The estimated probability of apprehension is often based on factors that include the number of Line Patrol hours of Border Patrol staff and the relative strengths and weaknesses of U.S. and Central American economies. More recently, this data has been supplemented by classified data compiled by DHS based on observation from unmanned aerial vehicles patrolling the border. While the comparison of apprehensions at and between the border crossings is not as precise as would be optimal, the estimates included in this report are based on the best available existing information, some of which has been publicly supplied by Customs and Border Protection Commissioner Alan Bersin.

BETWEEN THE BORDER CROSSINGS—90 PERCENT PROBABILITY OF APPREHENSION

Apprehensions of persons seeking to enter the United States between the border crossings—where all entries are illegal—has fallen to levels not seen since 1970s, as the enhanced manpower, mobility, communications, technology, and infrastructure have been brought to bear on the traffic.

In addition, increased apprehension rates in most Border Patrol sectors, up to 90 percent according to Customs and Border Protection Commissioner Alan Bersin, vastly impedes the trafficking of persons from Mexico to the United States between the border crossings.[20]

Two notes of caution: The data remains weak, and 90 percent apprehension rates do not mean only 10 percent of persons seeking illegal entry gain it. In fact, most

[19] Evaluating U.S. Immigration Control Policy: What Mexican Migrants Can Tell Us, Wayne Cornelius, Director, Center for Comparative Immigration Studies, University of California, San Diego, CA, April 14, 2009.

[20] Border commissioner touts greater enforcement, San Diego Union Tribune, January 5, 2011 by Elizabeth Aguilera, and The Border is Safe, Federal Officials Say, Texas Tribune, August 17, 2011 by Julian Aguilar.

of those who attempt to enter the United States illegally try more than one time, and eventually nearly all make it through.

Another point: The old belief that for every apprehension, three more gain entry (the getaway rate) is being proven untrue. Commissioner Bersin says that as a result of more reliable data provided by airborne surveillance vehicles deployed in the past several years by the Border Patrol, the Border Patrol detects far more illegal entries and catches a greater percentage of them.[21]

"Only 28 percent of 'major violators' attempting to enter the U.S. at the official border crossings are detected and apprehended."

Finally, as the Border Patrol improvements in manpower, mobility, communications, technology, and infrastructure have made illegal crossings more difficult and hazardous, the criminal cartels operating in Mexico have moved into the human smuggling market, forcing mom-and-pop smuggling operations out of business and increasing the cost of cross-border transport to would-be immigrants.

Without the infusion of many billions dollars more, the United States has achieved about as much control of illegal entries between the border crossings as possible without solving the core problem: Our immigration system must be modernized to accommodate immigration needs and provide adequate channels for people to legally enter the United States so they do not try to go around a broken system. We must have comprehensive immigration reform in order to achieve continued improvement in the effective control of our borders between the border crossings.

AT THE BORDER CROSSINGS—28 PERCENT PROBABILITY OF APPREHENSION

According to the most recent data released by the DHS, only 28 percent of "major violators" attempting to enter the United States at the official border crossings are detected and apprehended.[22] In addition, CBP reports only 50 to 74 percent success in improving the targeting, screening, and apprehension of high-risk international cargo and travelers to prevent terrorist attacks, while providing processes to facilitate the flow of safe and legitimate trade and travel.[23] The Department, under the claim that the statistics are "law enforcement sensitive," has not released more recent data.

STRATEGIC RESPONSE OF THE ENEMY

"Nearly all of the drugs smuggled into the U.S., and the guns and bulk cash smuggled into Mexico transits via official border crossings."

U.S. border security strategy should not operate in a vacuum. The smuggling of drugs and humans into the United States and the smuggling of money and firearms into Mexico fuel the criminal cartels operating from the Mexican side of the border. The cartels are mature organizations, possessing sophisticated communications, transportation, and intelligence systems. They are richly informed about the environment in which they conduct their criminal operations and highly skilled at evaluating risk and executing strategic and tactical operations based on risk judgments. One cartel, the Zeta organization, "looks very much like any global business organization that can quickly, flexibly, and effectively respond to virtually any opportunity, challenge, or changing situation."[24]

These criminal organizations are capable of discovering and exploiting weaknesses between the border crossings, but the Border Patrol has developed tactical mobility and agility to identify and respond to such threats. When presented with a choice between one path that presents a less than 30 percent risk of failure and another that presents an up to 90 percent risk of capture, the cartels naturally choose the less risky path. In the present environment, the cartels are choosing to conduct their trade across the bridges and highways, through the sanctioned border crossings and are rejecting the risk of crossing the Rio Grande and open desert between the border crossings.

---

[21] "Immigrant arrests nearing 40-year low" The Arizona Daily Star, September 4, 2011 by Brady McCombs.

[22] A major violation involves serious criminal activity, including possession of narcotics, smuggling of prohibited products, human smuggling, weapons possession, fraudulent U.S. documents, and other offenses serious enough to result in arrest.

[23] Department of Homeland Security Annual Performance Report for Fiscal Years 2008–2010, Department of Homeland Security Office of the Chief Financial Officer Program Analysis and Evaluation, Washington, DC, May 7, 2009.

[24] A "New" Dynamic in the Western Hemisphere Security Environment: The Mexican Zetas and Other Private Armies, Dr. Max G. Manwaring. U.S. Army War College Strategic Studies Institute, Carlisle, PA, September 25, 2009.

As reported by *Los Angeles Times* writer Richard Marosi, "One of the Sinaloa cartel's main pipelines runs through the antiquated U.S. port of entry at Calexico, a favorite of smugglers. The inspection station sits almost directly on the border, without the usual buffer zone of several hundred feet, so inspectors have difficulty examining cars in the approach lanes. Drug-sniffing dogs wilt in summer heat that can reach 115 degrees . . . Drugs were brought from Sinaloa state to Mexicali, Mexico, in bus tires. (The smuggler's) job was to move the goods across the border and deliver them to distributors in the Los Angeles area, about 200 miles away.

"The flow was unceasing, and he employed about 40 drivers, lookouts, and coordinators to keep pace."[25]

According to the U.S. Department of Justice National Drug Threat Assessment 2010, nearly 90 percent of cocaine, methamphetamine, marijuana, heroin, and MDMA smuggled into the United States enters through the border crossings. A joint project on U.S.-Mexico Security Cooperation coordinated by the Mexico Institute at the Woodrow Wilson Center and the Trans-Border Institute at the University of San Diego indicates that bulk cash to fuel the Mexican drug cartels' illicit and violent activities transits through the border crossings. And while data on the smuggling of firearms is incomplete, available information points to border crossings as the overwhelming point of entry into Mexico.

The conclusion is irrefutable that nearly all of the drugs smuggled into the United States, and the guns and bulk cash smuggled into Mexico, transits via the border crossings, a strategic choice made by the Mexican cartels because the likelihood of being detected or apprehended is three times more likely between the border crossings than at them.

STRATEGIC CHOICES FOR THE UNITED STATES

Those who mean our Nation harm have adjusted their strategies and tactics to reflect situational changes faster than DHS and Congress can adjust. Because of the U.S. Government's relative lack of nimbleness, DHS and Congress continue to pour billions of dollars of our National resources into defending the vast expanses of land between the border crossings, a path that the enemy has abandoned, while denying resources needed to defend the border crossings that the enemy has chosen to directly assault.

The choice for U.S. policymakers appears clear: Between (1) continue on the strategic path that wastes resources and produces fewer results by continuing to emphasize border protection between the border crossings and (2) changing our strategy to defend against an adroit, responsive enemy that is attacking us at the border crossings (while preparing for the enemy's next logical move, most likely aimed back to the water and the skies).

As Doris Meissner, former commissioner of the Immigration and Naturalization Service, put the choice: "The more [money] that you pour into the Border Patrol and into enforcement between land ports of entry (border crossings) . . . the more pressure there is for people to misuse the system that gets them through land ports. It's important to have a balance of resources between both."[26]

"The more [money] that you pour into the Border Patrol and into enforcement between border crossings, the more pressure there is for people to misuse the system that gets them through the legal border crossings."

The scenario envisioned by former Commissioner Meissner has already been in place for years: A field study conducted in the first quarter of 2009 by the Mexican Migration Field Research and Training Program, based at the University of California-San Diego, found that more than one out of four (28 percent) of unauthorized Mexican migrants interviewed for the study had entered the United States on their most recent trip to the border through a legal border crossing, either concealed in vehicles or using false or borrowed documents. The authors noted that "while crossing the border through a POE costs significantly more than crossing in remote areas (people-smugglers can charge $5,000 or more for POE crossings), that mode of entry is much more likely to yield success."[27]

Reports from the Government Accountability Office (GAO) have described the situation at the border crossings as inadequate to the task of protecting the Nation.

---

[25] "Inside the Cartel: Unraveling Mexico's Sinaloa drug cartel" The Los Angeles Times, July 24, 2011 by Richard Marosi.

[26] Border Security Falls Short In Audit, GAO Criticizes Staffing, Training By Spencer S. Hsu, Washington Post, November 6, 2007.

[27] Wayne A. Cornelius, David Fitzgerald, Pedro Lewin-Fischer, and Leah Muse-Orlinoff, Mexican Migration and the U.S. Economic Crisis: A Transnational Perspective (Boulder, CO: Lynne Rienner Publishers, 2009), pp. 61–62.

GAO found that managers at 19 of 21 border crossing offices cited examples of anti-terrorism activities not being carried out, new or expanded facilities that were not fully operational, and radiation monitors and other inspection technologies not being fully used because of staff shortages. At seven of the eight major border crossings GAO visited, officers and managers told of not having sufficient staff, which contributes to morale problems, fatigue, lack of backup support, and safety issues when officers inspect travelers—"increasing the potential that terrorists, inadmissible travelers, and illicit goods could enter the country."[28]

Although they refused to make the data publicly available for years because they classified it as law enforcement sensitive, DHS officials recently acknowledged publicly that for the border crossings to successfully complete their mission, the agency needs 6,000 additional personnel and $6 billion in funding for infrastructure and technology.[29]

"DHS officials recently acknowledged publicly that for the border crossings to successfully complete their mission, the agency needs 6,000 additional personnel and $6 billion in funding for infrastructure and technology."

In response, Congress has allocated zero dollars to border crossing infrastructure in fiscal 2011 and is likely to refuse to add funds in fiscal 2012. House and Senate appropriators have both approved adding 350 new CBP inspectors in fiscal 2012, but acknowledge that declining customs revenues will force a reduction of an equal number available to the agency, making the added personnel a net of zero. While technology is in the pipeline for delivery to the border crossings, a lack of adequate electric infrastructure often makes new equipment useless.

Instead of dealing with the strategic threat to the United States, Congress has chosen to focus legislation to deploy more Border Patrol, build additional walls and fences and exempt the Border Patrol from regulations that protect communities' air and water, safeguard our public lands and honor our cultural and historic heritage.

TEXAS BORDER COALITION RECOMMENDATIONS

The Texas Border Coalition suggests that mandating more Border Patrol, fencing and waiving environmental law reflects an ineffective, anachronistic strategy that has not kept pace with developments at the border or with the risk assessments made by the criminal cartels. TBC urges Congress and the Obama administration to restore balance to border security at and between the border crossings by engaging in an emergency program to provide the border crossings with $6 billion in funding for infrastructure and technology and to employ 6,000 new inspectors on America's front line over the next 4 years.

It is important that the new inspectors must be assigned to the front lines of the border crossings where they are needed, not to supervisory roles. According to GAO, prior personnel buildups at the border crossings have resulted in a 17 percent increase in CBP managers and only a 2 percent increase in the number of front-line CBP officers.[30] Anecdotally, there is evidence of this pattern over a period of many years. The Nation's security cannot afford to see an intended increase in front-line inspectors siphoned off to the management level of CBP.

"TBC urges Congress and the Obama Administration to restore balance to border security at and between the ports by engaging in an emergency program to provide the border crossings with $6 billion in funding for infrastructure and technology and to employ 6,000 new inspectors on America's front line over the next four years."

In addition, the TBC commends the leadership of many border Representatives in Congress for their attention to developing a real strategy for confronting the criminal cartels and security on the U.S.-Mexico border. We especially wish to salute Michigan Representative Candice Miller, Chair of the House Subcommittee on Border and Maritime Security, and Texas Representative Henry Cuellar, Ranking Democrat on the subcommittee, for advancing legislation requiring the Department of Homeland Security to develop strategy for securing borders within 5 years.

---

[28] GAO–08–329T: Despite Progress, Weaknesses in Traveler Inspections Exist at Our Nation's Border Crossings: Statement of Richard M. Stana, Director Homeland Security and Justice Issues, Washington, DC, January 3, 2008.

[29] "Meeting Land Port of Entry Modernization Needs in Constrained Budgetary Environment," presentation by Mikhail Pavlov to the Joint Working Committee, October 2011.

[30] GAO–06–751R, Information on Immigration Enforcement and Supervisory Promotions in the Department of Homeland Security's Immigration and Customs Enforcement and Customs and Border Protection, Washington, DC, June 13, 2006.

Finally, TBC agrees with CBP Commissioner Alan Bersin that public-private partnerships (PPPs) are vital to fund the projects necessary to handle the ever-increasing trade between the United States and Mexico. Since CBP officials have announced that any PPP relationship would require a new law, we propose legislation be enacted to authorize public-private partnerships for expenses at border crossings.

SUMMARY

In a world of asymmetrical threats to U.S. security, the United States cannot rely on outmoded tactics rooted in the past to defend the homeland today. It is vital that Congress and the Obama administration take immediate action to strengthen our Nation's weakest link in border security: American Southwestern Border crossings must be strengthened with a crash program of $6 billion to bring our infrastructure up to requirements and the hiring of 6,000 additional Customs inspectors.

Mr. MCCAUL. I want to thank the witnesses for attending this portion of the hearing, and, Dr. Caudle, for you flying all the way out from my home State of Texas; I really appreciate your testimony here today.

We have votes coming up so we are going to adjourn this panel. We should be back around 11:45 to begin the testimony of the second panel. Thank you.

[Recess.]

Mr. MCCAUL. The committee will come back to order. I know many of us have flights to catch so I would like to—the Ranking Member will be here shortly, but I think in the interest of time we are going to go ahead and proceed.

I would like to go ahead and introduce the witnesses and then hear their testimony. First we have Mr. Shawn Reese, who is an expert on homeland security policy at CRS. He has written numerous reports for Congress at the Federal, State, and local levels on homeland security policy issues.

He has testified before the House Government Reform and Oversight Committee and the House Homeland Security Committee on Federal counterterrorism training programs. Prior to coming to CRS Mr. Reese was an officer in the United States Army for 10 years.

Welcome, Mr. Reese.

Next we have Mr. David Maurer, who is the director in the U.S. GAO homeland security and justice team, where he leads GAO's work reviewing DHS and DOJ management issues. His recent work in these areas includes examining DHS management integration, the Quadrennial Homeland Security Review, Secret Service financial management, DOJ grant management, the Federal prison system, and an assessment of technologies for detecting explosives in the passenger rail environment.

Welcome, Mr. Maurer.

Last we have Alan Cohn. He is deputy assistant secretary for policy at the Department of Homeland Security. He was formerly a director of emergency preparedness and response policy in the DHS Office of Policy Development and counsel at Akin Gump Strauss Hauer & Feld, a very good Texas law firm.

He took part in the response to the 1993 World Trade Center bombing as an emergency medical technician in New York City and the response to the 9/11 attacks—and we thank you for your service in that regard—then the 2005 hurricane season as a member of FEMA's National Urban Search and Rescue Response System.

I want to thank you all for being here today, and the Chairman now recognizes Mr. Reese for his testimony.

STATEMENT OF SHAWN REESE, ANALYST, EMERGENCY MANAGEMENT AND HOMELAND SECURITY POLICY, CONGRESSIONAL RESEARCH SERVICE

Mr. REESE. Chairman McCaul, Ranking Member Keating, and Members of the subcommittee, on behalf of the Congressional Research Service I would like to thank you for this opportunity to appear before you to discuss the homeland security strategy. CRS was asked to discuss National policy on homeland security as communicated in National strategic documents.

My written statement addresses key findings, which include the absence of a consensus definition of homeland security and varied strategic missions that may result in a vague homeland security concept. I will briefly discuss the various homeland security definitions and missions identified in National strategic documents.

A consensus definition is necessary but not sufficient. A clear prioritization of strategic missions is what is needed.

Prior to 9/11 the United States addressed crises primarily through separate prisms of National defense, law enforcement, emergency management. Nine-eleven prompted a strategic process that included the debate over and the development of homeland security policy.

Today, this homeland security policy debate and development has resulted in a plethora of Federal entities with homeland security responsibilities. For example, there are 18 Federal departments with homeland security responsibilities excluding DHS, and OMB states that approximately 48 percent of Federal homeland security funding is appropriated to these Federal entities.

The concept of homeland security evolved over the last decade, and this evolution has been communicated in several strategic documents. As stated earlier, they include the National Strategy for Homeland Security, the DHS Strategic Plan of 2008, the 2010 National Security Strategy, the 2010 Quadrennial Homeland Security Review, the 2010 Bottom-Up Review, and the 2011 National Strategy for Counterterrorism.

While definitions and mission embodied in these strategic documents have commonalities, there are significant differences. Natural disasters are specifically identified as an integral part of homeland security in only four of the six documents, and only two of the documents—the Bottom-Up Review and the Strategic Plan—specifically include border and maritime security and immigration in their homeland security definition.

All of these mentioned issues are important and require significant funding. However, the lack of consensus about the inclusion of these areas of policy may have negative or unproductive consequences for National homeland security activities.

A consensus definition is necessary but not sufficient. A clear priority of strategic missions is what is needed.

So why is this important to Congress? As deficit reduction causes demand for reduced Federal spending Congress will likely pay more stringent attention to homeland security funding. With reduced funds comes the need for higher degrees of organization,

focus, and clarity about the purpose and objectives of homeland security.

Additionally, if homeland security policy priorities are unclear Congress' ability to provide effective oversight may be hampered. For example, how can policymakers determine whether to authorize and fund additional personnel for such areas as border security as opposed to aviation security?

What are the priorities of homeland security and how do such priorities help determine the right choice between additional border patrol agents or aviation security screeners? Limited resources heightens the importance of prioritization.

Additionally, Congress, due to its oversight function, evaluates the execution of current homeland security policies. For example, do the DHS homeland security grant programs provide a measurable impact on State and local security? What strategic missions are expected to be fulfilled through the expenditure of grant funds? Where do those missions fit relative to one another in terms of priority?

In closing, a vague homeland security concept may hamper Congressional authorization, appropriation, and oversight functions. It may also restrict the Executive Branch's ability to prioritize and implement policy initiatives. Failure to effectively prioritize and utilize homeland security investments today can affect the Nation's security and potential vulnerability tomorrow.

I will conclude my testimony here. If CRS may be of further assistance to you I and my colleagues are here to assist.

Once again, thank you for the privilege to appear before you today.

[The statement of Mr. Reese follows:]

PREPARED STATEMENT OF SHAWN REESE

FEBRUARY 3, 2012

INTRODUCTION

Chairman McCaul, Ranking Member Keating, and Members of the subcommittee, on behalf of the Congressional Research Service I would like to thank you for this opportunity to appear before you to discuss National homeland security strategy.

The subcommittee requested that CRS discuss National policy on homeland security as communicated in National strategic documents and the report CRS is developing on *Homeland Security Definitions, and Missions.*

Accordingly, my statement summarizes the salient portions of this CRS work, and addresses key findings which include the absence of a universal definition of homeland security and varied strategic missions. Ten years after the September 11, 2001, terrorist attacks, the U.S. Government does not have a universal view of "homeland security."

Currently, different strategic documents and mission statements offer varying homeland security missions. The strategic documents framing the U.S. homeland security mission include National strategies produced by the White House and strategy statements developed by the Department of Homeland Security (DHS). The White House has produced documents such as the 2007 *National Strategy for Homeland Security,* the 2010 *National Security Strategy,* and the *National Strategy for Counterterrorism.* DHS has developed the *Strategic Plan—One Team, One Mission, Securing the Homeland;* the *Quadrennial Homeland Security Review;* and the *Bottom-Up Review.*

Varied homeland security definitions and missions may impede the development of a coherent homeland security strategy, and the effectiveness of Congressional oversight may be hampered. This written testimony discusses examples of the varying homeland security definitions and missions identified in the aforementioned White House and DHS documents, and analyzes the policy question of how varied

homeland security definitions and missions may affect the development National homeland security policy. This testimony, however, does not examine DHS' implementation of strategy.

ISSUANCE OF HOMELAND SECURITY STRATEGIC DOCUMENTS

The evolution of U.S. homeland security strategy produced a series of White House and DHS documents. President George W. Bush's administration's issuance of a National homeland strategy was foundational in this process. The 2002 National Strategy for Homeland Security was described as a grand strategy.[1] Five years later, the administration issued a second version and its purpose was " . . . to guide, organize, and unify our Nation's homeland security efforts."[2] Some critics, however, argued that while the 2002 version had merit, the 2007 version of the strategy " . . . obfuscates rather than clarifies the government's homeland security mission. "[3] Conversely, others state that the 2007 version was a comprehensive effort that attempted to define America's homeland security mission.[4]

Subsequent to these two versions of the National homeland security strategy, President Barack Obama's administration issued the 2010 *National Security Strategy* and the 2011 *National Strategy for Counterterrorism.* DHS issued the *Strategic Plan—One Team, One Mission, Securing Our Homeland;* the 2010 *Quadrennial Homeland Security Review;* and the *Bottom-Up Review.*

These documents, collectively, are an example of the numerous strategies that have been issued that address homeland security. These strategic documents provide varied homeland security definitions and missions. Additionally, some of the documents do not prioritize resources to address the varied homeland security missions.

HOMELAND SECURITY DEFINED

It has been argued that homeland security is a "uniquely" American concept, developed because of geography and an American belief in a distinct divide between events and issues inside and outside of U.S. borders. Homeland security development as a strategic concept was precipitated by the terrorist attacks of 9/11. Prior to those attacks, National policy was typically described as law enforcement, emergency response, and National defense. Discussions of the need to evolve the way National policy was conceptualized occurred with such entities as the Gilmore Commission[5] and the United States Commission on National Security (which referenced homeland security early in 2001).[6]

After the 9/11, policymakers realized a new approach was needed to address large-scale terrorist attacks. The establishment of a Department, a Presidential council, and a series of Presidential directives in the name of "homeland security" occurring after 9/11 further demonstrated that it was a distinct, although in these cases, undefined concept.[7] Later, the Federal, State, and local government responses to disasters such as Hurricane Katrina expanded the homeland security definition to include significant disasters, major public health emergencies, and other events that threaten the United States, the economy, and the rule of law, and Government operations.[8]

Homeland Security Definitions

The debate over the varied definitions persists as the Federal Government continues to issue and implement homeland security strategy. All of the strategic documents discussed in this written testimony define homeland security as security ef-

---

[1] Richard A. Falkenrath, "Homeland Security: The White House Plan Explained and Examined," Brookings Forum, Washington, DC, September 4, 2002, p. 4.

[2] Office of the President, Homeland Security Council, *The Homeland Security Strategy,* Washington, DC, October 2007, p. 1.

[3] James Jay Carafano, *New Homeland Security Misses the Mark,* Heritage Foundation, Washington, DC, October 10, 2007, *http://heritage.org/Research/HomelandDefense/wm1659.cfm.*

[4] Christopher Bellavita, "Changing Homeland Security: Ten Essential Homeland Security Books," Homeland Security Affairs, vol. 3, no. 1 (February 2007), pp. 3–4.

[5] For information on the Gilmore Commission, see *http://www.rand.org/nsrd/terrpanel.html.* The Gilmore Commission was established prior to 9/11, however, it released its fifth and final report in December 2003.

[6] For information on the U.S. Commission on National Security, see *http://www.fas.org/irp/threat/nssg.pdf.* The U.S. Commission on National Security was established in 1998 and issued its final report in February 2001.

[7] Harold C. Relyea, "Homeland security and information," *Government Information Quarterly,* vol. 19, 2002, p. 219.

[8] Nadav Morag, "Does Homeland Security Exist Outside the United States?," *Homeland Security Affairs,* vol. 7, September 2011, p. 1.

forts, however, each one defines these efforts in different terms. Examples of these documents include the 2007 and 2010 *National Security Strategy,* the *Strategic Plan—One Team, One Mission, Securing Our Homeland;* the 2010 *Quadrennial Homeland Security Review;* and the *Bottom-Up Review.*

Additionally, these documents provide further information on the homeland security concept. This information is not necessarily what homeland security is, but rather what it entails or how it is achieved. This conceptualization is both explicitly and implicitly implied, and includes the following:

- the homeland security enterprise encompasses a Federal, State, local, Tribal government and private sector approach that requires coordination;
- that homeland security can involve securing against and responding to both hazard-specific and all-hazards;
- that homeland security activities do not imply total protection or complete threat reduction;
- homeland security includes the need to ensure that the U.S. critical infrastructure, key assets, and economy are resilient; and
- that homeland security includes border, waterway, and marine security.

The following table provides examples of U.S. strategy documents and their homeland security definitions.

TABLE 1.—SUMMARY OF HOMELAND SECURITY DEFINITIONS

Document	Definition
2010 National Security Strategy.	A seamless coordination among Federal, State, and local governments to prevent, protect against and respond to threats and natural disasters.[1]
2007 National Strategy for Homeland Security.	A concerted National effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.[2]
2010 Quadrennial Homeland Security Review.	A concerted National effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and ways of life can thrive.[3]
2007 U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2008–2013.	A unified National effort to prevent and deter terrorist attacks, protect and respond to hazards, and to secure the National borders.[4]
2011 National Strategy For Counterterrorism.	Defensive efforts to counter terrorist threats.[5]
2010 Bottom-Up Review.	Preventing terrorism, responding to and recovering from natural disasters, customs enforcement and collection of customs revenue, administration of legal immigration services, safety and stewardship of the Nation's waterways and marine transportation system, as well as other legacy missions of the various components of DHS.[6]

[1] Office of the President, *National Security Strategy,* Washington, DC, May 2010, p. 2.
[2] Office of the President, Homeland Security Council, *The National Homeland Security Strategy,* Washington, DC, October 2007, p. 1.
[3] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review,* Washington, DC, February 2010, p. 13.
[4] U.S. Department of Homeland Security, *One Team, One Mission, Securing the Homeland: U.S. Homeland Security Strategic Plan, Fiscal Years 2008–2013,* Washington, DC, 2008, p. 3.
[5] Office of the President, *National Strategy For Counterterrorism,* Washington, DC, June 29, 2011, p. 11.
[6] U.S. Department of Homeland Security, *Bottom-Up Review,* Washington, DC, July 2010, p. 3.

Homeland Security Definition: Analysis

The common themes among the many homeland security definitions are that National homeland security efforts are unified, concerted, and coordinated across all levels of government. Thus, the importance of the Federalism approach to homeland security is highlighted. This approach is a combined effort of Federal, State, local, and Tribal governments, however, individual Federal, State, local, and Tribal government efforts are not identified in the documents. Another common theme across all of the documents in defining homeland security is preventing, responding to, and

recovering from terrorist attacks, which is consistent with evolving homeland security policy after the terrorist attacks of September 11, 2001.

The focus of the concept of homeland security communicated in the strategy documents differs in regard to two areas that may be considered substantive. Natural disasters are specifically identified as an integral part of homeland security in four of the six documents, but are not mentioned in the 2007 *National Strategy for Homeland Security and the 2011 National Strategy for Counterterrorism.*[9] Two documents—the Bottom-Up Review and the Strategic Plan—specifically include border and maritime security, and immigration in their homeland security definition. Homeland security issues such as natural disaster prevention, response, and recovery; border and maritime security, and immigration are important and require significant funding. Failure to have consensus on their importance and role in homeland security may result in the Nation's efforts being uncoordinated and counterproductive.

The competing or varied views in these documents may indicate that there is no succinct homeland security definition. It is, however, possible that such definition exists among relevant policymakers and just isn't communicated in the strategic documents. However, without such a definition, homeland security stakeholders and policymakers may not be able to coordinate and resource homeland security missions necessary to secure the Nation. These differing definitions may also be attempting to identify and counter every threat and risk with prioritization.

In addition to these strategic document examples, DHS Deputy Secretary Jane Lute recently stated that homeland security " . . . is operation, it's transactional, it's decentralized, it's bottom-driven," and influenced by law enforcement, emergency management, and the political environment. Conversely, DHS Deputy Secretary Lute stated that National security " . . . is strategic, it's centralized, it's top-driven," and influenced by the military and the intelligence community.[10] Some see these comments as reflection of a DHS attempt at establishing a homeland security definition that is more operational than strategic and an illustration of the complexity of a common understanding of homeland security.

HOMELAND SECURITY MISSIONS

Varied homeland security definitions may result in all levels of government identifying and executing varied missions. These efforts may be competing rather than integrated and result in ineffective or inefficient security. The examples of strategic documents in this written testimony provide numerous homeland security missions such as terrorism prevention, response, and recovery; critical infrastructure protection and resilience; Federal, State, and local emergency management and preparedness; and border security. As noted earlier, none of these documents specifically task a homeland security entity or stakeholder with these missions. The following table summarizes the varied missions identified in these strategic documents.

TABLE 2.—SUMMARY OF HOMELAND SECURITY MISSIONS AND GOALS

Document	Missions and Goals
2007 National Strategy for Homeland Security.	-Prevent and disrupt terrorist attacks. -Protect the American people, critical infrastructure and key resources. -Respond to and recover from incidents that do occur. -Strengthen the foundation to ensure long-term success.[1]
U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2008–2013.	-Protect the Nation from dangerous people. -Protect the Nation from dangerous goods. -Protect critical infrastructure. -Strengthen the Nation's preparedness and emergency response capabilities. -Strengthen and unify the Department's operations and management.[2]

[9] Obviously, the National Strategy For Counterterrorism would not mention any hazard or threat other than terrorism.

[10] Christopher Bellavita, "A new perspective on homeland security?" Homeland Security Watch, Dec. 20, 2011, *http://www.hlswatch.com/2011/12/20/a-new-perspective-on-homeland-security/*.

TABLE 2.—SUMMARY OF HOMELAND SECURITY MISSIONS AND GOALS—Continued

Document	Missions and Goals
Quadrennial Homeland Security Review.	-Prevent terrorism and enhance security. -Secure and manage our borders. -Enforce and administer our immigration laws. -Safeguard and secure cyberspace. -Ensure resilience to disasters.[3] -Provide essential support to National and economic security.[4]
Bottom-Up Review	-Prevent terrorism and enhance security. -Secure and manage borders. -Enforce and manage immigration laws. -Safeguard and secure cyberspace. -Ensure resilience to disasters. -Improve Departmental management and accountability.[5]
2010 National Security Strategy.	-Strengthen National capacity. -Ensure security and prosperity at home. -Secure cyberspace. -Ensure American economic prosperity.[6]
National Strategy for Counterterrorism.	-Protect the American people, homeland, and American interests. -Eliminate threats to the American people's, homeland's, and interests' physical safety. -Counter threats to global peace and security. -Promote and protect U.S. interests around the globe.[7]

[1] Office of the President, Homeland Security Council, *National Strategy for Homeland Security,* Washington, DC, October 2007, p. 1.

[2] U.S. Department of Homeland Security, *One Team, One Mission, Securing the Homeland: U.S. Homeland Security Strategic Plan, Fiscal Years 2008–2013,* Washington, DC, 2008, p. 6–25.

[3] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review,* Washington, DC, February 2010, p. 2.

[4] This mission of providing essential support to National and economic security was not part of the 2010 Quadrennial Homeland Security Review, but has been subsequently added as an additional mission. U.S. Government Accountability Office, *Quadrennial Homeland Security Review: Enhanced Stakeholder Consultation and Use of Risk Information Could Strengthen Future Reviews,* GAO–11–873, September 2011, p. 9.

[5] U.S. Department of Homeland Security, *Bottom-Up Review,* Washington, DC, July 2010, pp. i–ii.

[6] Office of the President, *National Security Strategy,* Washington, DC, May 2010, p. 14.

[7] Office of the President, *National Strategy for Counterterrorism,* Washington, DC, June 2011, p. 2.

Homeland Security Missions: Analysis

The missions in these documents identify a consensus that preventing, responding to, recovering from, and being resilient against terrorist attacks are essential in securing the Nation. Additionally, there is an agreement that the Nation's populace, critical infrastructure, and key resources need protection from both terrorism and disasters. This protection from both terrorism and disasters is seen as a key homeland security mission. Some, but not all, of the documents include missions related to border security, immigration, the economy, and general resilience.

Some of these documents have been criticized. Senator Susan Collins—current Ranking Member, Committee on Homeland Security and Governmental Affairs—expressed disappointment in the *Quadrennial Homeland Security Review* and *Bottom-Up Review* because it does not communicate priorities and stated that it does not compare favorably to the most recent *Quadrennial Defense Review.* [11] The *Quadrennial Defense Review* identifies National security and U.S. military priorities and these priorities through a process " . . . from objectives to capabilities and activi-

[11] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Charting a Path Forward: The Homeland Security Department's Quadrennial Review and Bottom-Up Review,* 111th Cong., 2nd sess., July 21, 2010.

ties to resources." [12] Furthermore, the *Quadrennial Homeland Security Review* missions are different from the *2007 National Strategy for Homeland Security*[13] missions, and neither identifies priorities, or resources, for DHS, or other Federal agencies. Since the *National Strategy for Homeland Security* and the *Quadrennial Homeland Security Review* missions are differing and varied, and because the *Quadrennial Homeland Security Review* does not specifically identify a strategic process to achieve the missions, one may assume that this document is solely operational guidance. Additionally, critics found the *Bottom-Up Review* lacking in detail and failing to meet its intended purpose.[14]

Overall, strategic documents intended to provide guidance do not identify the same missions for any homeland security entity or stakeholder. One example, however, of homeland security entities and stakeholders being tasked with specific missions is the *National Response Framework.* The *National Response Framework* is not a strategy document but is a "guide to how the Nation conducts all-hazards response. It is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the nation, liking all levels of government, nongovernmental organizations, and the private sector."[15] Some policy makers may view the *National Response Framework* as effective guidance regarding all-hazards response and may be a model to develop a similar guide to National homeland security missions. The National Response Framework, however, does not identify National homeland security missions.

There is no evidence in the existing homeland security strategic documents that supports the aligning and prioritization of the varied missions, nor do any of the documents convey how National, State, or local resources are to be allocated to achieve these missions. Arguably, without prioritized resource allocation to aligned missions, the Nation's homeland security activities and operations may be haphazard and inconsistent. Another consequence of the absence of clear missions is that available funding then tends to govern the priorities. Thus the appropriations process may dictate National homeland security missions.

ANALYSIS OF CONSEQUENCES

Congress may wish to address the issues of homeland security strategy, definitions, and missions, in light of the potential for significant events to occur much like those of the terrorist attacks of September 11, 2001 or natural disasters such as Hurricane Katrina. These outstanding policy issues result from the varied definitions and missions identified in numerous National strategic documents. Additionally, these documents do not consistently address risk mitigation associated with the full range of homeland security threats. Finally, one piece arguably missing from these documents, and their guidance, is a discussion of the resources and fiscal costs associated with preparing for low-risk, but high-consequence threats.

Policymakers are faced with a complex and detailed list of risks, or threats to security, for which they then attempt to plan. However, managing those risks 99% of the time with even a single failure may lead to significant human and financial costs.[16] The actual end product of any homeland security strategic process that involves clarifying definitions and missions will invariably aid in this planning process though a number of risks may still not be adequately countered.

Homeland security is essentially about managing risks. The purpose of a strategic process is to develop missions to achieve that end. Before risk management can be accurate and adequate, policymakers must coordinate and communicate. That work begins by developing a foundation of common definitions of key terms and concepts. It is also necessary, in order to coordinate and communicate, to ensure stakeholders are aware of, trained for, and prepared to meet assigned missions. Finally, this analysis leads to the conclusion that missions are most effective when they are the product of a prioritization process based on National homeland security interests.

---

[12] U.S. Department of Defense, *Quadrennial Defense Review,* Washington, DC, February 2010, p. iii.

[13] The 2007 *National Strategy for Homeland Security* is the most recent National strategy specifically on homeland security.

[14] Katherine McIntire Peters, "DHS Bottom-Up Review is long on ambition, short on detail," *GovernmentExecutive.com,* July 2010.

[15] U.S. Department of Homeland Security, *National Response Framework,* Washington, DC, January 2008, p. i.

[16] Donald F. Kettl, *System Under Stress: Homeland Security and American Politics,* 2nd ed., Washington, DC, CQPress, 2007, p. 82.

It has been argued that homeland security, at its core, is about coordination because of the disparate stakeholders and risks.[17] Homeland security is not only about coordination of resources and actions to counter risks; it is also about the coordination of the strategic process policymakers use in determining the risks, the stakeholders and their missions, and the prioritization of those missions.

Without a general consensus on the physical and philosophical definition and missions of homeland security, achieved through a strategic process, there will continue to be the potential for disjointed and disparate approaches to securing the Nation. This general consensus on the homeland security concept starts with a consensus definition and an accepted list of prioritized missions that are constantly reevaluated to meet risks of the new paradigm that is homeland security in the 21st Century. These varied definitions and missions, however, may be the result of a strategic process that has developed an approach that adjusts Federal homeland security policy to emerging threats and risks.

Thank you.

Mr. MCCAUL. Thank you, Mr. Reese. I want to thank the outstanding work that CRS does for the Congress.

Next, Mr. Maurer is recognized for 5 minutes.

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

Mr. MAURER. Thank you, Mr. Chairman.

Good morning, Chairman McCaul, Ranking Member Keating, other Members and staff. I am pleased to be here today to discuss the findings from our prior work on strategic planning at the Department of Homeland Security.

To set the stage a bit, it is important to remember that DHS conducts a wide variety of operations every day—securing the border, protecting the President, providing grants to local governments, screening airline passengers, researching technologies. DHS does all of this and more.

It costs about $56 billion a year to do this. DHS is now the third-largest Department in the Federal Government and its sheer size and scope can complicate efforts to develop a common strategy to guide it all.

DHS needs to have a clear strategy because what it does is so important. DHS and its various components need to have a clear idea of what should be done, how daily operations align with broader priorities, what resources are necessary to achieve those goals, and how to assess progress along the way.

My statement for the record discusses our findings on DHS's efforts to develop this strategy as well as the Department's on-going work to build a single, unified Department that is greater than the sum of its whole. Right now I would like to briefly highlight three key points from our work.

First, DHS's strategic approach currently resides in three documents. The QHSR explains what DHS should be doing. DHS used the BUR to understand what it was actually doing and then developed a budget plan to align resources to keep priorities.

Our work found that DHS conducted significant outreach to various stakeholders and used their input when developing the QHSR. However, we recommended that DHS do a better job next time seeking input from non-Federal stakeholders and providing all stakeholders more time to comment.

[17] Ibid.

Second, DHS did not formally consider risk when studying strategic priorities. For example, the QHSR identifies five key missions for the entire Department but does not prioritize them as called for in the 9/11 Commission Act. The QHSR also discusses threats to homeland security but DHS did not conduct a National risk assessment.

In addition, DHS used the BUR to identify 14 key initiatives deemed a priority in the Department's fiscal year 2012 budget request. While DHS can be commended for identifying a discrete list of priorities, the Department did not consider risk information when making these key resource decisions. In our September 2011 report we recommended that DHS improve its consideration of risk during the next QHSR process and DHS agreed to do so.

Finally, effectively implementing a common strategy requires a unified Department. DHS has made significant progress knitting itself together, but 9 years after its creation DHS has not completed its transformation into an integrated department.

When DHS opened its doors in 2003 GAO designated it as a high-risk because building a new department out of 22 legacy agencies represented a significant challenge. Most significantly, the Department lacked an effective and unified management structure to support its critically important daily operations.

I am pleased to say that in recent years DHS leadership has placed considerable attention and effort addressing these issues, and as a result, DHS has made important progress recognizing and addressing its management challenges. GAO has worked closely with the Department in this regard.

In September 2010 we provided DHS 31 key actions and outcomes that are critical to addressing the challenges within and across the Department's management functions. Since then DHS has developed a series of plans to achieve these outcomes.

I believe these plans, if fully implemented, create an off-ramp from our high-risk designation, but the key for DHS is execution. DHS needs to implement its plans, align resources to support key outcomes, and most importantly, demonstrate sustained progress. A solid management foundation will help DHS carry out its vital missions and help ensure the Department can translate the words in its strategies into concrete actions.

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

[The statement of Mr. Maurer follows:]

PREPARED STATEMENT OF DAVID C. MAURER

FEBRUARY 3, 2012

GAO HIGHLIGHTS

Highlights of GAO–12–382T, a testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) requires that beginning in fiscal year 2009 and every 4 years thereafter the Department of Homeland Security (DHS) conduct a review that provides a comprehensive examination of the homeland security strategy of the United States. In February 2010, DHS issued its first Quadrennial Homeland Security Re-

view (QHSR) report, outlining a strategic framework for homeland security. In July 2010 DHS issued a report on the results of its Bottom-Up Review (BUR), a Department-wide assessment to implement the QHSR strategy by aligning DHS's programmatic activities, such as inspecting cargo at ports of entry, and its organizational structure with the missions and goals identified in the QHSR. This testimony addresses DHS's efforts to: (1) Strategically plan its homeland security missions through the QHSR; (2) set strategic priorities and measure performance; and (3) build a unified department. This testimony is based on GAO reports issued in December 2010, February 2011, and September 2011.

What GAO Recommends

GAO made recommendations in prior reports for DHS to, among other things, provide more time for consulting with stakeholders during the QHSR process, examine additional mechanisms for obtaining input from non-Federal stakeholders, and examine how risk information could be used in prioritizing future QHSR initiatives. DHS concurred and has actions planned or underway to address them.

Department of Homeland Security.—Additional Actions Needed to Strengthen Strategic Planning and Management Functions

WHAT GAO FOUND

DHS's primary strategic planning effort in recent years has been the QHSR. In September 2011, GAO reported on the extent to which DHS consulted with stakeholders in developing the QHSR. DHS solicited input from various stakeholder groups in conducting the first QHSR, but DHS officials, several stakeholders GAO contacted, and other reviewers of the QHSR noted concerns with time frames provided for stakeholder consultations and outreach to non-Federal stakeholders. Specifically, DHS consulted with stakeholders—Federal agencies; Department and component officials; State, local, and Tribal governments; the private sector; academics; and policy experts—through various mechanisms, such as the solicitation of papers to help frame the QHSR. DHS and these stakeholders identified benefits from these consultations, such as DHS receiving varied perspectives. However, stakeholders also identified challenges in the consultation process, such as concerns about the limited time frames for providing input into the QHSR or BUR and the need to examine additional mechanisms for including more non-Federal stakeholders in consultations. By providing more time for obtaining feedback and examining mechanisms to obtain non-Federal stakeholders' input, DHS could strengthen its management of stakeholder consultations and be better positioned to review and incorporate, as appropriate, stakeholders' input during future reviews.

DHS considered various factors in identifying high-priority BUR initiatives for implementation in fiscal year 2012 but did not include risk information as one of these factors, as called for in GAO's prior work and DHS's risk-management guidance. Through the BUR, DHS identified 43 initiatives aligned with the QHSR mission areas to serve as mechanisms for implementing those mission areas. According to DHS officials, DHS did not consider risk information in prioritizing initiatives because of differences among the initiatives that made it difficult to compare risks across them, among other things. In September 2011, GAO reported that consideration of risk information during future implementation efforts could help strengthen DHS's prioritization of mechanisms for implementing the QHSR. Further, GAO reported that DHS established performance measures for most of the QHSR objectives and had plans to develop additional measures. However, with regard to specific programs, GAO's work has shown that a number of programs and efforts lack outcome goals and measures, hindering the Department's ability to effectively assess results.

In 2003, GAO designated the transformation of DHS as high-risk because DHS had to transform 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 U.S. National and economic security. DHS has taken action to implement, transform, and strengthen its management functions, such as developing a strategy for addressing this high-risk area and putting in place common policies, procedures, and systems within individual management functions, such as human capital, that help to integrate its component agencies. However, DHS needs to demonstrate measurable, sustainable progress in implementing its strategy and corrective actions to address its management challenges.

Chairman McCaul, Ranking Member Keating, and Members of the subcommittee: I am pleased to be here today to discuss Department of Homeland Security (DHS) strategic planning. Various strategies and plans exist for guiding homeland security

efforts across the homeland security enterprise.[1] For example, the May 2010 National Security Strategy outlines key security priorities and the 2007 National Homeland Security Strategy defined the homeland security mission for the Federal Government. More specific to DHS, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) requires that beginning in fiscal year 2009 and every 4 years thereafter DHS conduct a review that provides a comprehensive examination of the homeland security strategy of the United States.[2] In February 2010, DHS issued its first Quadrennial Homeland Security Review (QHSR) report, outlining a strategic framework for homeland security to guide the activities of homeland security partners, including Federal, State, local, and Tribal government agencies; the private sector; and non-Governmental organizations.[3]

In addition to the QHSR, in July 2010 DHS issued a report on the results of its Bottom-Up Review (BUR), a Department-wide assessment to implement the QHSR strategy by aligning DHS's programmatic activities, such as apprehending fugitive aliens and inspecting cargo at ports of entry, and its organizational structure with the missions and goals identified in the QHSR.[4] The BUR report described DHS's current activities contributing to: (1) QHSR mission performance, (2) Departmental management, and (3) accountability. Subsequent to publishing the BUR report, DHS identified priority initiatives, such as strengthening aviation security and enhancing the Department's risk management capability, to strengthen DHS's mission performance, improve departmental management, and increase accountability.

DHS's on-going efforts to identify strategic goals and align key missions and resources with those goals are supported by another key Departmental goal: Building a unified department. In 2003, GAO designated implementing and transforming DHS as high-risk because DHS had to transform 22 agencies—several with major management challenges—into one department. Failure to effectively address DHS's management and mission risks could have serious consequences for U.S. National and economic security. Our prior work, undertaken before the creation of DHS, found that successful transformations of large organizations, even those faced with less-strenuous reorganizations than DHS, can take years to achieve. DHS is now the third-largest Federal department with more than 200,000 employees and $56 billion in budget authority, and its transformation is critical to achieving its homeland security missions.

My testimony today focuses on the findings from our prior work in three key areas:

- DHS's efforts to strategically plan its homeland security missions Department-wide through the QHSR,
- DHS's efforts to set strategic priorities and measure performance Department-wide, and:
- DHS's efforts to build and implement a unified department.

This statement is based on four past reports, issued in December 2010, February 2011, and September 2011, related to DHS's QHSR, GAO's high-risk series, and DHS mission implementation.[5] For these past reports, among other things, we interviewed DHS officials; analyzed DHS strategic documents; and reviewed our past reports, supplemented by DHS Office of Inspector General (IG) reports, issued since DHS began its operations in March 2003. We conducted this work in accordance with generally accepted Government auditing standards. More detailed information on the scope and methodology from our previous work can be found within each specific report.

---

[1] 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.

[2] Pub. L. No. 110–53, § 2401(a), 121 Stat. 266, 543–45 (2007) (codified at 6 U.S.C. § 347).

[3] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, DC: February 2010). Although the act requires the first QHSR to be conducted in 2009—see 6 U.S.C. § 347(c)—the QHSR report was issued in February 2010 and we refer to it in this statement as the 2010 QHSR.

[4] DHS, *Bottom-Up Review Report* (Washington, DC: July 2010).

[5] GAO, *Quadrennial Homeland Security Review: Enhanced Stakeholder Consultation and Use of Risk Information Could Strengthen Future Reviews,* GAO–11–873 (Washington, DC: Sept. 15, 2011); *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); *High-Risk Series: An Update,* GAO–11–278 (Washington, DC: February 2011); and *Quadrennial Homeland Security Review: 2010 Reports Addressed Many Required Elements, but Budget Planning Not Yet Completed,* GAO–11–153R (Washington, DC: Dec. 16, 2010).

DHS STRATEGICALLY PLANNED ITS HOMELAND SECURITY MISSIONS DEPARTMENT-WIDE THROUGH THE QHSR, BUT STAKEHOLDER CONSULTATIONS COULD BE ENHANCED

The QHSR identified five homeland security missions—(1) Preventing Terrorism and Enhancing Security, (2) Securing and Managing Our Borders, (3) Enforcing and Administering Our Immigration Laws, (4) Safeguarding and Securing Cyberspace, and (5) Ensuring Resilience to Disasters—and goals and objectives to be achieved within each mission. A sixth category of DHS activities—Providing Essential Support to National and Economic Security—was added in the fiscal year 2012 budget request but was not included in the 2010 QHSR report.

DHS's primary strategic planning effort in recent years has been the QHSR. DHS approached the 9/11 Commission Act requirement for a quadrennial homeland security review in three phases.

- In the first phase, DHS defined the Nation's homeland security interests, identified the critical homeland security missions, and developed a strategic approach to those missions by laying out the principal goals, objectives, and strategic outcomes for the mission areas. DHS reported on the results of this effort in the February 2010 QHSR report in which the Department identified 5 homeland security missions, 14 associated goals, and 43 objectives. The QHSR report also identified threats and challenges confronting U.S. homeland security, strategic objectives for strengthening the homeland security enterprise, and Federal agencies' roles and responsibilities for homeland security.
- In the second phase—the BUR—DHS identified its component agencies' activities, aligned those activities with the QHSR missions and goals, and made recommendations for improving the Department's organizational alignment and business processes. DHS reported on the results of this second phase in the July 2010 BUR report.
- In the third phase DHS developed its budget plan necessary to execute the QHSR missions. DHS presented this budget plan in the President's fiscal year 2012 budget request, issued February 14, 2011, and the accompanying Fiscal Year 2012–2016 Future Years Homeland Security Program (FYHSP), issued in May 2011.

In December 2010, we issued a report on the extent to which the QHSR addressed the 9/11 Commission Act's required reporting elements.[6] We reported that of the nine 9/11 Commission Act reporting elements for the QHSR, DHS addressed three and partially addressed six.[7] Elements DHS addressed included a description of homeland security threats and an explanation of underlying assumptions for the QHSR report. Elements addressed in part included a prioritized list of homeland security missions, an assessment of the alignment of DHS with the QHSR missions, and discussions of cooperation between the Federal Government and State, local, and Tribal governments.

In September 2011, we reported on the extent to which DHS consulted with stakeholders in developing the QHSR.[8] DHS solicited input from various stakeholder groups in conducting the first QHSR, but DHS officials, stakeholders GAO contacted, and other reviewers of the QHSR noted concerns with time frames provided for stakeholder consultations and outreach to non-Federal stakeholders. DHS consulted with stakeholders—Federal agencies; Department and component officials; State, local, and Tribal governments; the private sector; academics; and policy experts—through various mechanisms, such as the solicitation of papers to help frame the QHSR and a web-based discussion forum. DHS and these stakeholders identified benefits from these consultations, such as DHS receiving varied perspectives. However, stakeholders also identified challenges in the consultation process. For example:

- Sixteen of 63 stakeholders who provided comments to GAO noted concerns about the limited time frames for providing input into the QHSR or BUR.
- Nine other stakeholders commented that DHS consultations with non-Federal stakeholders, such as State, local, and private-sector entities, could be enhanced by including more of these stakeholders in QHSR consultations.
- Reports on the QHSR by the National Academy of Public Administration, which administered DHS's web-based discussion forum, and a DHS advisory committee comprised of non-Federal representatives noted that DHS could provide

[6] GAO–11–153R.

[7] We considered an element addressed if all portions of it were explicitly included in either the QHSR or BUR reports, addressed in part if one or more but not all portions of the element were included, and not addressed if neither the QHSR nor the BUR reports explicitly addressed any part of the element.

[8] GAO–11–873.

more time and strengthen non-Federal outreach during stakeholder consultations.

By providing more time for obtaining feedback and examining mechanisms to obtain non-Federal stakeholders' input, DHS could strengthen its management of stakeholder consultations and be better positioned to review and incorporate, as appropriate, stakeholders' input during future reviews. We recommended that DHS provide more time for consulting with stakeholders during the QHSR process and examine additional mechanisms for obtaining input from non-Federal stakeholders during the QHSR process, such as whether panels of State, local, and Tribal government officials or components' existing advisory or other groups could be useful. DHS concurred and reported that it will endeavor to incorporate increased opportunities for time and meaningful stakeholder engagement and will examine the use of panels of non-Federal stakeholders for the next QHSR.

DHS DID NOT PRIORITIZE QHSR MISSIONS OR USE RISK ASSESSMENTS TO HELP SET STRATEGIC PRIORITIES AND COULD IMPROVE DEPARTMENT-WIDE PERFORMANCE MEASURES

The 9/11 Commission Act called for DHS to prioritize homeland security missions in the QHSR.[9] As we reported in December 2010, DHS identified five homeland security missions in the QHSR, but did not fully address the 9/11 Commission Act reporting element because the Department did not prioritize the missions.[10] According to DHS officials, the five missions listed in the QHSR report have equal priority—no one mission is given greater priority than another. Moreover, they stated that in selecting the five missions from the many potential homeland security mission areas upon which DHS could focus its efforts, the five mission areas are DHS's highest-priority homeland security concerns.

Risk management has been widely supported by Congress and DHS as a management approach for homeland security, enhancing the Department's ability to make informed decisions and prioritize resource investments. In September 2011, we also reported that in the 2010 QHSR report, DHS identified threats confronting homeland security, such as high-consequence weapons of mass destruction and illicit trafficking, but did not conduct a National risk assessment for the QHSR.[11] DHS officials stated that at the time DHS conducted the QHSR, DHS did not have a well-developed methodology or the analytical resources to complete a National risk assessment that would include likelihood and consequence assessments—key elements of a National risk assessment. The QHSR terms of reference, which established the QHSR process, also stated that at the time the QHSR was launched, DHS lacked a process and a methodology for consistently and defensibly assessing risk at a National level and using the results of such an assessment to drive strategic prioritization and resource decisions. In recognition of a need to develop a National risk assessment, DHS created a study group as part of the QHSR process that developed a National risk assessment methodology. DHS officials plan to implement a National risk assessment in advance of the next QHSR, which DHS anticipates conducting in fiscal year 2013. Consistent with DHS's plans, we reported that a National risk assessment conducted in advance of the next QHSR could assist DHS in developing QHSR missions that target homeland security risks and could allow DHS to demonstrate how it is reducing risk across multiple hazards.

DHS Could Strengthen Its Use of Risk Information in Prioritizing Initiatives and Planning and Investment Decision-Making

DHS considered various factors in identifying high-priority BUR initiatives for implementation in fiscal year 2012 but did not include risk information as one of these factors as called for in our prior work and DHS's risk management guidance.[12] Through the BUR, DHS identified 43 initiatives aligned with the QHSR mission areas to help strengthen DHS's activities and serve as mechanisms for implementing those mission areas (see app. I for a complete list). According to DHS officials, the Department could not implement all of these initiatives in fiscal year 2012 because of, among other things, resource constraints and organizational or legislative changes that would need to be made to implement some of the initiatives.

---

[9] 6 U.S.C. § 347(c)(2)(C).

[10] GAO–11–153R.

[11] GAO–11–873.

[12] See GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure,* GAO–06–91 (Washington, DC: Dec. 15, 2005), and *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation,* GAO–09–492 (Washington, DC: Mar. 27, 2009). For DHS risk-management guidance, see DHS, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (April 2011).

In identifying which BUR initiatives to prioritize for implementation in fiscal year 2012, DHS leadership considered: (1) "Importance," that is, how soon the initiative needed to be implemented; (2) "maturity," that is, how soon the initiative could be implemented; and (3) "priority," that is, whether the initiative enhanced Secretarial or Presidential priorities. Risk information was not included as an element in any of these three criteria, according to DHS officials, because of differences among the initiatives that made it difficult to compare risks across them, among other things. However, DHS officials stated that there are benefits to considering risk information in resource allocation decisions. Consideration of risk information during future implementation efforts could help strengthen DHS's prioritization of mechanisms for implementing the QHSR, including assisting in determinations of which initiatives should be implemented in the short or longer term. In our September 2011 report, we recommended that DHS examine how risk information could be used in prioritizing future QHSR initiatives. DHS concurred and reported that DHS intends to conduct risk analysis specific to the QHSR in advance of the next review and will use the analysis as an input into decision-making related to implementing the QHSR.

Further, in September 2011, we reported on progress made by DHS in implementing its homeland security missions since 9/11.[13] As part of this work, we identified various themes that affected DHS's implementation efforts. One of these themes was DHS's efforts to strategically manage risk across the Department. We reported that DHS made important progress in assessing and analyzing risk across sectors. For example, in January 2009 DHS published its Integrated Risk Management Framework, which, among other things, calls for DHS to use risk assessments to inform decision-making. In May 2010, the Secretary issued a Policy Statement on Integrated Risk Management, calling for DHS and its partners to manage risks to the Nation.

We also reported that DHS had more work to do in using this information to inform planning and resource-allocation decisions. Our work shows that DHS has conducted risk assessments across a number of areas, but should strengthen the assessments and risk management process. For example:

- In June 2011, we reported that DHS and Health and Human Services could further strengthen coordination for chemical, biological, radiological, and nuclear (CBRN) risk assessments. Among other things, we recommended that DHS establish time frames and milestones to better ensure timely development and interagency agreement on written procedures for development of DHS's CBRN risk assessments. DHS concurred and stated that the Department had begun efforts to develop milestones and time frames for its strategic and implementation plans for interagency risk assessment development.[14]
- In November 2011, we reported that the U.S. Coast Guard used its Maritime Security Risk Assessment Model at the National level to focus resources on the highest-priority targets, leading to Coast Guard operating efficiencies, but use at the local level for operational and tactical risk-management efforts has been limited by a lack of staff time, the complexity of the risk tool, and competing mission demands.[15] Among other things, we recommended that the Coast Guard provide additional training for sector command staff and others involved in sector management and operations on how the model can be used as a risk-management tool to inform sector-level decision-making. The Coast Guard concurred and stated that it will explore other opportunities to provide risk training to sector command staff, including on-line and webinar training opportunities.
- In November 2011, we reported that the Federal Emergency Management Agency (FEMA) used risk assessments to inform funding-allocation decisions for its port security grant program.[16] However, we found that FEMA could further enhance its risk-analysis model and recommended incorporating the results of past security investments and refining other data inputs into the model. DHS concurred with the recommendation, but did not provide details on how it plans to implement it.

---

[13] GAO–11–881.

[14] GAO, *National Preparedness: DHS and HHS Can Further Strengthen Coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessments,* GAO–11–606 (Washington, DC: June 21, 2011).

[15] GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations,* GAO–12–14 (Washington, DC: Nov. 17, 2011).

[16] GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened,* GAO–12–47 (Washington, DC: Nov. 17, 2011).

- In October 2009, we reported that TSA's strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies was not risk-based.[17] Among other things, we recommended that DHS conduct a complete risk assessment related to TSA's passenger screening program and incorporate the results into the program's strategy. DHS concurred, and in July 2011 reported actions underway to address it, such as beginning to use a risk-management analysis process to analyze the effectiveness and efficiency of potential countermeasures and effect on the commercial aviation system.

DHS Has Established Performance Measures, but Has Not Yet Fully Developed Outcome-Based Measures for Many of Its Mission Functions

In September 2011, we reported that DHS established performance measures for most of the QHSR objectives and had plans to develop additional measures.[18] Specifically, DHS established new performance measures, or linked existing measures, to 13 of 14 QHSR goals, and to 3 of 4 goals for the sixth category of DHS activities—Providing Essential Support to National and Economic Security. DHS reported these measures in its fiscal years 2010–2012 Annual Performance Report. For goals without measures, DHS officials told us that the Department was developing performance measures and planned to publish them in future budget justifications to Congress.

In September 2011, we also reported that DHS had not yet fully developed outcome-based measures for assessing progress and performance for many of its mission functions.[19] We recognized that DHS faced inherent difficulties in developing performance goals and measures to address its unique mission and programs, such as in developing measures for the effectiveness of its efforts to prevent and deter terrorist attacks. While DHS had made progress in strengthening performance measurement, our work across the Department has shown that a number of programs lacked outcome goals and measures, which may have hindered the Department's ability to effectively assess results or fully assess whether the Department was using resources effectively and efficiently. For example, our work has shown that DHS did not have performance measures for assessing the effectiveness of key border security and immigration programs, to include:

- In September 2009, we reported that U.S. Customs and Border Protection (CBP) had invested $2.4 billion in tactical infrastructure (fencing, roads, and lighting) along the Southwest Border under the Secure Border Initiative—a multi-year, multi-billion dollar program aimed at securing U.S. borders and reducing illegal immigration.[20] However, DHS could not measure the effect of this investment in tactical infrastructure on border security. We recommended that DHS conduct an evaluation of the effect of tactical infrastructure on effective control of the border. DHS concurred with the recommendation and subsequently reported that the on-going analysis is expected to be completed in February 2012.
- In August 2009, we reported that CBP had established three performance measures to report the results of checkpoint operations, which provided some insight into checkpoint activity.[21] However, the measures did not indicate if checkpoints were operating efficiently and effectively, and data reporting and collection challenges hindered the use of results to inform Congress and the public on checkpoint performance. We recommended that CBP improve the measurement and reporting of checkpoint effectiveness. CBP agreed and, as of September 2011, reported plans to develop and better use data on checkpoint effectiveness.
- Further, we reported that U.S. Immigration and Customs Enforcement (ICE) and CBP did not have measures for assessing the performance of key immigration enforcement programs. For example, in April 2011, we reported that ICE did not have measures for its overstay enforcement efforts, and in May 2010 that CBP did not have measures for its alien smuggling investigative efforts, making it difficult for these agencies to determine progress made in these areas

---

[17] GAO. *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges.* GAO–10–128. (Washington, DC: Oct. 7, 2009).

[18] GAO–11–873.

[19] GAO–11–881.

[20] GAO, *Secure Border Initiative: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed,* GAO–09–1013T (Washington, DC: Sept. 17, 2009).

[21] GAO, *Border Patrol: Checkpoints Contribute to Border Patrol's Mission, but More Consistent Data Collection and Performance Measurement Could Improve Effectiveness,* GAO–09–824 (Washington, DC: Aug. 31, 2009).

and evaluate possible improvements.[22] We recommended that ICE and CBP develop performance measures for these two areas. They generally agreed and reported actions underway to develop these measures.

DHS HAS TAKEN ACTION TO IMPLEMENT, STRENGTHEN, AND INTEGRATE ITS MANAGEMENT FUNCTIONS, BUT NEEDS TO DEMONSTRATE SUSTAINABLE PROGRESS

In 2003, GAO designated the transformation of DHS as high-risk because DHS had to transform 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 U.S. National and economic security. This high-risk area includes challenges in strengthening DHS's management functions—financial management, human capital, information technology, and acquisition management—the impact of those challenges on DHS's mission implementation, and challenges in integrating management functions within and across the Department and its components. Addressing these challenges would better position DHS to align resources to its strategic priorities, assess progress in meeting mission goals, enhance linkages within and across components, and improve the overall effectiveness and efficiency of the Department.

On the basis of our prior work, in September 2010, we identified and provided to DHS 31 key actions and outcomes that are critical to addressing the challenges within the Department's management functions and in integrating those functions across the Department. These key actions and outcomes include, among others, validating required acquisition documents at major milestones in the acquisition review process; obtaining and then sustaining unqualified audit opinions for at least 2 consecutive years on the Department-wide financial statements while demonstrating measurable progress in reducing material weaknesses and significant deficiencies; and implementing its workforce strategy and linking workforce planning efforts to strategic and program-specific planning efforts to identify current and future human capital needs.[23]

In our February 2011 high-risk update, we reported that DHS had taken action to implement, transform, and strengthen its management functions, and had begun to demonstrate progress in addressing some of the actions and outcomes we identified within each management area.[24] For example, we reported that the Secretary and Deputy Secretary of Homeland Security, and other senior officials, have demonstrated commitment and top leadership support to address the Department's management challenges. DHS also put in place common policies, procedures, and systems within individual management functions, such as human capital, that help to integrate its component agencies. For example, DHS:

- revised its acquisition management oversight policies to include more detailed guidance to inform departmental acquisition decisionmaking.
- strengthened its enterprise architecture, or blueprint to guide information technology acquisitions, and improved its policies and procedures for investment management.
- developed corrective action plans for its financial management weaknesses, and, for the first time since its inception, DHS earned a qualified audit opinion on its fiscal year 2011 balance sheet;[25] and,
- issued its Workforce Strategy for Fiscal Years 2011–2016, which contains the Department's workforce goals, objectives, and performance measures for human capital management.

Further, in January 2011, DHS provided us with its *Integrated Strategy for High Risk Management,* which summarized the Department's preliminary plans for addressing the high-risk area. Specifically, the strategy contained details on the imple-

---

[22] GAO, *Overstay Enforcement: Additional Mechanisms for Collecting, Assessing, and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs,* GAO–11–411 (Washington, DC: Apr. 15, 2011) and *Alien Smuggling: DHS Needs to Better Leverage Investigative Resources to Measure Program Performance along the Southwest Border,* GAO–10–328 (Washington, DC: May 24, 2010).

[23] 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.

[24] GAO–11–278.

[25] For DHS, obtaining a qualified audit opinion is a first step toward achieving an unqualified audit opinion.

mentation and transformation of DHS, such as corrective actions to address challenges within each management area, and officials responsible for implementing those corrective actions. DHS provided us with updates to this strategy in June and December 2011. We provided DHS with written feedback on the January 2011 strategy and the June update, and have worked with the Department to monitor implementation efforts. We noted that both versions of the strategy were generally responsive to actions and outcomes we identified for the Department to address the high-risk area. For example, DHS included a management integration plan containing information on initiatives to integrate its management functions across the Department. Specifically, DHS plans to establish a framework for managing investments across its components and management functions to strengthen integration within and across those functions, as well as to ensure that mission needs drive investment decisions. This framework seeks to enhance DHS resource decision-making and oversight by creating new Department-level councils to identify priorities and capability gaps, revising how DHS components and lines of business manage acquisition programs, and developing a common framework for monitoring and assessing implementation of investment decisions. These actions, if implemented effectively, should help to further and more effectively integrate the Department and enhance DHS's ability to implement its strategies. However, we noted in response to the June update that specific resources to implement planned corrective actions were not consistently identified, making it difficult to assess the extent to which DHS has the capacity to implement these actions. Additionally, for both versions, we noted that the Department did not provide information on the underlying metrics or factors DHS used to rate its progress, making it difficult for us to assess DHS's overall characterizations of progress. We are currently assessing the December 2011 update and plan to provide DHS with feedback shortly.

Although DHS has made progress in strengthening and integrating its management functions, the Department continues to face significant challenges affecting the Department's transformation efforts and its ability to meet its missions. In particular, challenges within acquisition, information technology, financial, and human capital management have resulted in performance problems and mission delays. For example, DHS does not yet have enough skilled personnel to carry out activities in some key programmatic and management areas, such as for acquisition management. DHS also has not yet implemented an integrated financial management system, impeding its ability to have ready access to information to inform decision-making, and has been unable to obtain a clean audit opinion on the audit of its consolidated financial statements since its establishment.

Going forward, DHS needs to implement its *Integrated Strategy for High Risk Management,* and 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. Demonstrated, sustained progress in all of these areas will help DHS strengthen and integrate management functions within and across the Department and its components.

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

APPENDIX I: BOTTOM-UP REVIEW INITIATIVES

Initiatives selected by DHS for implementation in fiscal year 2012 listed in bold.

MISSION ONE: PREVENTING TERRORISM AND ENHANCING SECURITY

1. Strengthen counterterrorism coordination across DHS
2. Strengthen aviation security
3. Create an integrated Departmental information sharing architecture
4. Deliver infrastructure protection and resilience capabilities to the field
5. Set National performance standards for identification verification
6. Increase efforts to detect and counter nuclear and biological weapons and dangerous materials
7. Leverage the full range of capabilities to address biological and nuclear threats
8. Standardize and institutionalize the National Fusion Center Network
9. Promote safeguards for access to secure areas in critical facilities
10. Establish DHS as a center of excellence for canine training and deployment
11. Redesign the Federal Protective Service (FPS) to better match mission requirements

MISSION TWO: SECURING AND MANAGING OUR BORDERS

12. Expand joint operations and intelligence capabilities, including enhanced domain awareness
13. Prioritize immigration and customs investigations
14. Enhance the security and resilience of global trade and travel systems
15. Strengthen and expand DHS-related security assistance internationally (e.g., border integrity and customs enforcement security assistance) consistent with U.S. Government security, trade promotion, international travel, and foreign assistance objectives
16. Enhance North American security

MISSION THREE: ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

17. Comprehensive immigration reform
18. Improve DHS immigration services processes
19. Focus on fraud detection and National security vetting
20. Target egregious employers who knowingly exploit illegal workers
21. Dismantle human smuggling organizations
22. Improve the detention and removal process
23. Work with new Americans so that they fully transition to the rights and responsibilities of citizenship
24. Maintain a model detention system commensurate with risk

MISSION FOUR: SAFEGUARDING AND SECURING CYBERSPACE

25. Increase the focus and integration of DHS's operational cybersecurity and infrastructure resilience activities
26. Strengthen DHS ability to protect cyber networks
27. Increase DHS predictive and forensic capabilities for cyber intrusions and attacks
28. Promote cyber security public awareness

MISSION FIVE: ENSURING RESILIENCE TO DISASTERS

29. Enhance catastrophic disaster preparedness
30. Improve DHS's ability to lead in emergency management
31. Explore opportunities with the private sector to "design-in" greater resilience for critical infrastructure
32. Make individual and family preparedness and critical facility resilience inherent in community preparedness

IMPROVING DEPARTMENT MANAGEMENT

33. Seek restoration of the Secretary's reorganization authority for DHS headquarters
34. Realign component regional configurations into a single DHS regional structure
35. Improve cross-Departmental management, policy, and functional integration
36. Strengthen internal DHS counterintelligence capabilities
37. Enhance the Department's risk management capability
38. Strengthen coordination within DHS through cross-Departmental training and career paths
39. Enhance the DHS workforce
40. Balance the DHS workforce by ensuring strong Federal control of all DHS work and reducing reliance on contractors

INCREASING ACCOUNTABILITY

41. Increase Analytic Capability and Capacity
42. Improve Performance Measurement and Accountability
43. Strengthen Acquisition Oversight

Mr. MCCAUL. Thank you, Mr. Maurer.

The Chairman now recognizes Mr. Cohn for his testimony.

STATEMENT OF ALAN COHN, DEPUTY ASSISTANT SECRETARY, OFFICE OF POLICY, DEPARTMENT OF HOMELAND SECURITY

Mr. COHN. Thank you.

Chairman McCaul, Ranking Member Keating, distinguished Members of the subcommittee, thank you very much for the opportunity to appear before you today. You have my written testimony; I will provide a brief overview of that testimony in these opening remarks and I am happy to take your questions after that.

As was noted, I am the deputy assistant secretary in the Office of Policy. I head the Department's Strategic Planning Office. I am a career member of the Senior Executive Service and I have led the Department's Strategic Planning Office for the past 4 years, since January 2008.

As the subcommittee has requested, I have focused my written testimony and I will focus these opening remarks on the Department's strategy for homeland security. Let me start by stating clearly that the strategy that the Department of Homeland Security has pursued for the past 3 years to ensure a safe, secure, and resilient homeland is set forth in the Quadrennial Homeland Security Review report 2010.

The QHSR provided the Department the opportunity to work with its Federal interagency partners and stakeholders across the homeland security enterprise in setting a strategic framework for achieving a secure homeland. Subsequent planning activities, such as the Bottom-Up Review as well as the development of the Department's fiscal year 2012 budget proposal and accompanying documents, filled in other aspects of the Department's strategic approach; in particular that the Bottom-Up Review provided the opportunity for the Department to align its activities and its programs to the strategic framework of the Quadrennial Review, and that the fiscal year 2012 budget process and the regeneration of performance measures that were reported in our annual performance report from that year filled in the budget alignment and performance alignment elements of that strategy.

The Department's forthcoming fiscal year 2012 to 2016 strategic plan—our third DHS strategic plan—consolidates the QHSR strategic framework with DHS performance measures and BUR initiatives focused on maturing and strengthening DHS. However, as a basic matter of understanding, the Department's strategy for addressing emerging and enduring threats and challenges is and has been the approach set forth in the QHSR report, and that approach nests within the overall structure of the 2010 National Security Strategy.

The Department has also taken steps to develop and implement a comprehensive strategic management approach. The Office of Policy supports that approach through several mechanisms, including annual strategic investment guidance, support to capability development through portfolio management bodies such as the Screening Coordination Office, and review of major acquisition programs to ensure consistency and alignment of mission needs to Department strategy and policy beginning with the QHSR.

Finally, the Office of Policy is focused on enhancing the Department's ability to develop strategy and conduct strategic analysis through strengthened analytic techniques and methodologies, including remedying some of the shortfalls that were pointed out by the Government Accountability Office relating to the last QHSR.

Congress' recent authorization for the Secretary to transfer risk management and analysis functions to the Office of Policy will help the Department's risk modeling analysis and strategic planning functions and aid in ensuring that risk analysis is most effectively informed strategy development and strategic choice.

Thank you very much for your support of our efforts and our people and hopefully for your support of our future efforts to continue strengthening and maturing the Department. I am happy to take any questions that you have.

[The statement of Mr. Cohn follows:]

PREPARED STATEMENT OF ALAN COHN

FEBRUARY 3, 2012

INTRODUCTION

Chairman McCaul, Ranking Member Keating, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today to discuss how the Department of Homeland Security (DHS) is implementing a strategy to counter emerging threats. As the subcommittee has requested, we have focused primarily on how the QHSR has provided a strategic foundation for DHS, and DHS strategic management based on the QHSR.

I serve as Deputy Assistant Secretary and head of the Office of Strategic Plans in the DHS Office of Policy within DHS headquarters. One of the key responsibilities of the DHS Office of Policy is to ensure that the Secretary, Deputy Secretary, Assistant Secretary for Policy, and the senior headquarters and Component leadership of DHS are provided with objective, analytically rigorous decision support. In short, we help ensure that tough policy and strategy decisions are informed by a consideration of viable alternatives, with a clear sense of the associated risk and resource implications, and that those decisions, once made, carry through to subsequent decisions concerning investments and operations. For that reason, I am pleased to be able to highlight how we do that at DHS and how we intend to continue improving that process in the context of emerging threats.

The homeland security strategic environment is constantly evolving, and while we have made significant progress, threats from terrorism continue to persist. Today's threats are not limited to any one individual or group, are not defined or contained by international borders, and are not limited to any single ideology. Terrorist tactics can be as simple as a homemade bomb and as sophisticated as a biological threat or a coordinated cyber attack. In addition, broader strategic trends such as the dramatic spread of internet and mobile technologies around the world and the growing relevance of non-state actors on the world stage suggest new opportunities and challenges that must be accounted for in our current and longer-term homeland security strategic planning.

Another defining characteristic of our strategic environment is the tightening fiscal environment. It is increasingly important to define clear priorities, develop and assess viable alternatives, and make well-informed decisions involving difficult trade-offs. DHS has made substantial progress in this regard, particularly with respect to establishing an enduring strategic foundation for National homeland security efforts, refining our strategic and policy analysis capabilities and approaches, and improving strategic alignment through focused management tools and processes. Together, these improvements have positioned DHS to effectively address today's security environment while ensuring that we are sufficiently flexible, agile, and capable in the face of emerging threats and risks.

In my testimony, I will highlight our activities in each of these areas. Specifically, I will: (1) Describe how the Quadrennial Homeland Security Review Report (2010) (QHSR) has provided a strategic foundation and common framework to inform subsequent analysis and planning; (2) describe targeted efforts aimed at enhancing strategic alignment that ensure DHS is a strategy and policy-driven organization; and (3) outline key improvements in our analytic capabilities and approaches.

STRATEGIC FOUNDATION: THE QHSR AND BOTTOM-UP REVIEW

QHSR

The *Implementing the 9/11 Commission Recommendations Act of 2007* directed the Department to begin conducting quadrennial reviews in 2009, and every 4 years

thereafter. The QHSR and subsequent Bottom-Up Review (BUR) were critical first steps in the process of examining and addressing fundamental strategic issues that concern homeland security, and establishing an enduring strategic foundation.

As the first review of its kind for DHS, the QHSR clarified the conceptual underpinnings of homeland security, described the security environment and the Nation's homeland security interests, identified the critical homeland security enterprise missions, and outlined the principal goals and essential objectives necessary for success in those missions. I would like to highlight three elements of the QHSR that, in particular, provided the strategy and planning foundation that have positioned DHS to effectively address emerging strategic challenges.

First, the QHSR clarified the conceptual underpinnings of homeland security. In defining homeland security as the intersection of evolving threats and hazards with traditional Governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration, the QHSR emphasized the importance of eliminating traditional stovepipes to achieving success in homeland security. The QHSR also established the idea of the homeland security enterprise, which refers to the collective efforts and shared responsibilities of Federal, State, local, Tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. Each of these conceptual elements has infused all aspects of our strategy and planning.

Second, the QHSR took a comprehensive approach to threats by expanding the focus of homeland security to specifically address high-consequence weapons of mass destruction; global violent extremism; mass cyber attacks, intrusions, and disruptions; pandemics and natural disasters; and illegal trafficking and related transnational crime. Almost 3 years later, these challenges remain top priorities. At the same time, DHS is assessing major trends and drivers in the strategic environment in order to understand how these challenges may be evolving and to anticipate emerging threats and risks.

Third, the QHSR adopted a mission structure designed to endure across inevitable changes in the security environment. Our missions are to prevent terrorism and enhance security, secure and manage our borders, enforce our immigration laws, safeguard and secure cyberspace, enhance resilience to disasters, and provide critical support to economic and National security. Because tomorrow's security environment will not necessarily look like today's security environment, the missions provide a durable framework to effectively address whatever risks and threats may emerge over time.

This framework has informed all subsequent DHS strategy and planning efforts, whether they are DHS products or products that DHS supports with partners across the enterprise. For example, the recently-released *Blueprint for a Secure Cyber Future* defines the ends, ways, and means by which DHS and the homeland security enterprise will meet the goals and objectives set forth in Mission 4 of the QHSR, Safeguarding and Securing Cyberspace.

The BUR and Strategy Implementation

The QHSR and other strategic guidance within the Department are implemented through the programming and budgeting process, and the oversight of major acquisitions. As a first step in this process, the BUR was initiated in November 2009 as an immediate follow-on and complement to the QHSR. The BUR focused on three elements: (1) How to improve DHS's operational performance within the five homeland security missions; (2) how to improve Department management; and (3) how to increase DHS accountability for the public funds entrusted to us.

The Department's fiscal year 2012 budget request began the process of implementing the QHSR and specific BUR initiatives and enhancements, and the corresponding fiscal year 2012–2016 Future Years Homeland Security Plan set forth the budget plan required to provide sufficient resources to successfully execute the Department's responsibilities across the full range of homeland security missions as described in the QHSR. The Department's approach to managing its annual performance and its priority goals are guided by the QHSR and BUR, as reflected in the fiscal year 2010–2012 Annual Performance Report and Plan. In addition, the forthcoming *Fiscal Year 2012–2016 DHS Strategic Plan* is founded on the framework and methodological approach of the QHSR, reflects performance measures aligned against the mission areas of the QHSR, and emphasizes the initiatives concerning Department management and accountability set forth in the BUR.

Based on the strategic foundation set forth in the QHSR and BUR, DHS's Components complete their own strategies, strategic plans, and other strategic initiatives. These efforts may be legislatively-driven, or may be initiated within the Department in order to address a persistent or emerging threat or challenge. However, all strate-

gies and strategic plans should reflect the overall framework set forth in the QHSR and BUR. For example, the 2011–2014 FEMA Strategic Plan describes the cascade from the *National Security Strategy* through the *Quadrennial Homeland Security Review Report* to the FEMA Administrator's Intent Priorities. Similarly the 2010–2014 ICE Strategic Plan draws its four priorities from the QHSR mission structure. Likewise, efforts such as the Border Intelligence Fusion Section at the El Paso Intelligence Center, the supply chain security initiative, and the Balanced Workforce initiative can be traced back to initiatives identified or described in the BUR. DHS harmonized its account structure and reworked its suite of performance measures as part of the BUR process, which resulted in enhanced management effectiveness and accountability.

The Next QHSR

Under the schedule set forth in the Implementing the 9/11 Commission Recommendations Act of 2007, the Department will conduct its next quadrennial review in 2013. While the first QHSR set a durable framework of homeland security missions, the next quadrennial review can focus on a more extensive examination of the security environment and potential future trends and shocks, and provide a deeper review of a few key areas. The review can provide a more in-depth look at those key areas with respect to current strategic environment, future strategic environment, National homeland security risk, strategy options and alternatives, and capability and resource implications for changes in strategy. In this way, the next QHSR can begin to look much more like the Quadrennial Defense Review on which it is modeled. The review will also reflect a greater integration of risk analysis into all stages of the quadrennial review, as recommended by the Government Accountability Office in their review of the first QHSR. The Department has begun planning for the next QHSR and we look forward to working with Congress going forward on executing this second quadrennial review.

IMPLEMENTING THE QHSR: ENSURING POLICY AND STRATEGY INFORM RESOURCE ALLOCATION

The Under Secretary for Management is leading the development and implementation of a comprehensive, strategic management approach focused on maturing organizational effectiveness within DHS. The "front end" of this strategic management system is really the "back end" of the policy and strategy process. To that end, the Office of Policy supports the Under Secretary for Management's efforts, not only by ensuring clear statements of policy and strategy, but by translating strategic guidance into investment guidance in the annual Integrated Planning Guidance, supporting capability development and analysis, and ensuring that the Department's major acquisitions are grounded in mission needs derived from Department policy and strategy.

The Integrated Planning Guidance sets forth the Secretary's specific investment guidance for Components to use in developing their Resource Allocation Plans (RAP), consistent with the QHSR and other strategy documents. The Integrated Planning Guidance marks the transition from the planning to the programming phase of the Department's Planning, Programming, Budgeting, and Execution (PPBE) process. The Office of Policy also supports the Management Directorate's Office of Program Analysis & Evaluation, which administers the PPBE process, in conducting analysis of specific issues for the annual budget cycle, reviewing Component RAP submissions for consistency with the IPG, and raising issues as part of the Program Review Board process.

The Office of Policy also supports capability development through portfolio management bodies such as the Screening Coordination Office (SCO). Portfolio management bodies help identify areas where better coordination and a common set of goals can make DHS more efficient and effective. For example, SCO, an element of the Office of Policy, establishes standards for Departmental programs which deal with the screening of people, and helps the Department meet those standards. Working closely with DHS Components and the headquarters programming and budgeting staff, SCO has helped increase information flow and reduce duplication among screening programs. This not only reduces the overall cost of such programs, it enhances the ability of programs to share information and enhance our Nation's security. The Office of Policy also conducts strategic requirements planning in support of portfolio management efforts involving domain awareness and information sharing. Ultimately, portfolio management bodies become the engines to develop integrated, cross-Departmental requirements for homeland security functions such as screening, domain awareness, and information sharing.

Another place where policy and strategy intersect with Departmental strategic management is the major acquisition oversight process. The Office of Policy sup-

ports the Management Directorate in Phase 1 (Need) and Phase 2 (Analyze/Select) of the acquisition review process, by reviewing Mission Needs Statements and Operational Requirements Documents for consistency with Department policy and strategy. During these reviews, Policy focuses on the following key questions:

1. Is the program consistent with approved policy, guidance, and requirements (e.g. the Quadrennial Homeland Security Review; applicable laws and regulations)?
2. Is the program duplicative of other similar capabilities elsewhere in the Department?
3. Is there a coherent scope for the program, and clear mission-oriented objectives, consistent with the QHSR and other strategy documents?
4. Are the requirements set forth in the document best fashioned to advance mission and functional needs, as articulated in the QHSR and other strategy documents?

This "back end" involvement in the PPBE, portfolio management, and major acquisitions oversight processes is an essential element in the full cycle of policy and strategy development and implementation. DHS is committed to ensuring that articulated policy and strategy influences programming and budgeting, capability development, and major acquisition decisions.

ENHANCING STRATEGY AND STRATEGIC ANALYSIS

Given the complexity of homeland security challenges and our primary role in decision support, a consistent priority within the Office of Policy is the application of rigorous and cutting-edge analytic techniques and methodologies. The Office of Policy developed and has been piloting a methodology for developing strategy. Informed by best practices and insights from business, academia, the military, and Government, including a highly valuable Government Accountability Office report on developing counter-terrorism strategies, our methodology stresses the importance of prioritization and choice, the consideration of resource implications, and analytically-informed insights in any strategy discussion. An anticipatory posture is emphasized through a fulsome examination of both the current and future strategic environment. The methodology is built around four basic elements: (1) Setting the foundations for good strategy; (2) establishing appropriate context; (3) developing viable alternative solutions; (4) conducting analysis to support decision-making. Key steps across these four elements include:

- Obtaining leadership guidance regarding key priorities and expectations for the strategy;
- Developing a plan to execute the strategy that includes identifying and engaging stakeholders, roles, and important time lines;
- Identifying the current strategy, including the implicit strategy as expressed through the budget;
- Framing the problem and identifying strategic assumptions given a common understanding of the current and future strategic environment;
- Defining success through outcomes and strategic level measures;
- Generating viable alternative strategic approaches;
- Identifying the resource implications of each alternative approach; and
- Assessing the degree to which each alternative would achieve success and at what cost.

In addition, the Office of Policy has worked with the National Protection and Programs Directorate's Office of Risk Management and Analysis (RMA) as RMA has developed models for assessing strategic National risk and capability—and program-level risk reduction. The fiscal year 2012 DHS Appropriations Act authorized the Secretary to transfer the risk management and analysis functions performed by RMA to the Office of Policy in 2012. Such a transfer will enhance the Department's risk modeling, analysis, and strategic planning functions, and aid in ensuring that risk analysis most effectively informs strategy development and strategic choice.

Effective strategy provides a unifying device through which an organization's capabilities are integrated and employed efficiently, resources are allocated toward the highest priorities, and different organizational elements are collaborating in the pursuit of common objectives, all of which are essential for a highly distributed, operationally-focused enterprise like DHS. Our strategy methodology represents a critical step in producing effective strategy.

CONCLUSION

The best way to posture the Department to effectively address emerging threats is to ensure that tough policy and strategy decisions are informed by a consideration of viable alternatives, with a clear sense of the associated risk and resource implica-

tions, and that those decisions once made effectively influence subsequent programming and budgeting, capability development, and major acquisition decisions.

I look forward to addressing your questions.

Mr. MCCAUL. Thank you, Mr. Cohn.

You know, this is a critical mission of the United States Government. It is clearly within the Constitutional responsibility. I personally wish we could appropriate more dollars, but we live within a tough budgetary time and so I think we need to make best use out of the dollars that we have and make it more efficient, and I think that is part of what these hearings are going to be all about.

One thing, Mr. Maurer, you mentioned is that implementing this strategic plan that risk is not taken into account, I guess, as much as it should. Can you explain that a little bit more?

Mr. MAURER. Sure. In our September 2011 report that we issued on the QHSR we talked about risk in sort of two different ways. First, in developing the QHSR the Department started going down the road of developing a National risk assessment, sort of pulling up at the National level what are the risks to homeland security and trying to build that into the overall analysis.

They developed a methodology but they didn't have the full analytic framework in place in time to complete that for this current QHSR. So in our report we recommended that they do it for the next QHSR, and our understanding is that the DHS has actions in place to do that.

The second aspect of risk that we looked at was in the Department's decisions about which of these BUR initiatives to prioritize. These were key initiatives coming out of the Bottom-Up Review. What were the things that the DHS really wanted to focus on as a priority?

There were a number of things that went into that equation but there was not a formal risk assessment that was part of determining what things sort of floated to the top. Part of that reason was because some of these BUR initiatives weren't really apples-to-apples comparisons. They ranged from very large things like aviation security to more focused, narrow things, like developing—improving the capabilities of canines who can detect explosives.

So again, we recommended that DHS take this into account in next year—in the next iteration of the QHSR and they said that they would do so.

Mr. MCCAUL. Do you agree that that would make DHS a more efficient agency?

Mr. MAURER. Absolutely. We think risk is one of several inputs in these kinds of strategic decisions, but certainly that is what DHS is in the business of doing, protecting the homeland security, and risk needs to be part of that equation.

Mr. MCCAUL. Mr. Cohn, are you willing to, in the next, I guess this strategic plan will come out again this next year, is that correct?

Mr. COHN. So the strategic plan will be released with the President's fiscal year 2013 budget, so on or about February 13. But we agreed with the recommendations of the Government Accountability Office and are planning to incorporate both elements into the next QHSR, which we will conduct in calendar year 2013.

If I could just add to what Mr. Maurer said, in terms of the overall strategic National risk assessment, we recognized in the QHSR in the terms of reference that the Department did not have the methodology to conduct that, and one of the things we did in the first QHSR was charter a working group to determine how we would go about approaching that problem. That working group reported its results and part of that methodology was actually used to develop the strategic National risk assessment that informed our preparedness efforts that Dr. Caudle referenced.

For the next Quadrennial Review we are planning to do a full assessment of the homeland security environment to include the current strategic environment, future strategic environment, threat landscape, strategic National risk assessment for a full-scope look.

In addition, in terms of the BUR initiatives, the challenge that we had was the Department did not have a overall mechanism for doing as Mr. Maurer noted, an apples-to-apples comparison of dissimilar activities across missions and across organizations. Certainly most of our organizations use robust risk assessment processes in determining the thrust of their activities. The challenge has been for the Department in figuring out a holistic way to use risk at the capability, program, or activity level to look not only within organizations but across organizations, across missions and portfolios.

Mr. MCCAUL. Well, I look forward to seeing that and I am glad that you are taking Mr. Maurer's advice and his recommendations. You know, we heard testimony from Mr. Schneider, who has an interesting background both in the DOD and in DHS, has a lot of experience in management.

Mr. Cohn, you would probably be the best, and maybe perhaps Mr. Maurer, as well—what is your response to his idea of looking at kind of a DOD model that is a Goldwater-Nichols approach?

Mr. COHN. So it is interesting. I think that Deputy Secretary Schneider, both in his remarks and his written testimony, pointed out the time line that DOD worked on to reach the point of integration that it is at. Created in 1947, 9 years into the Department of Defense was 1956 and the Department of Defense struggled with a lot of the same issues that have been pointed out here.

In the early 1960s Secretary Robert McNamara implemented the planning, programming, and budgeting process in DOD, which was really an effort to get the Department to look holistically across its organizations at its Nationally-oriented programs from a mission perspective. It was not until 1986 with Goldwater-Nichols and 1989 with the Defense Management Review that you got to that heightened level of operational integration.

What the Department is really focused on right now is focusing on getting to that first step of being able to look at our investment processes from an integrated perspective across our Secretary and deputy secretary, the heads of our directorates, our components, looking at making sure we have cross-departmental perspectives and decisions on strategy and policy, on requirements, on programming and budgeting, and on acquisition oversight. That is a lot of the work that the management director is doing and that they are working in concert with the——

Mr. MCCAUL. I would like to follow up with that. I think it is an interesting idea. You know, whether it is workable, I think, you know—Mr. Keating and I can discuss that, but I—it is certainly an interesting idea to take a look at.

Mr. Maurer, do you have any thoughts on that?

Mr. MAURER. Yes. I think it is absolutely an interesting idea to look at, and I think that conceptually it makes sense to try to do whatever you can to try to break down some of the stovepipes across the various operational components of the DHS. The Department is doing some things to go down that road.

They have, for example, recently consolidated the process for developing an SES class. They used to have four separate processes; now it is just—whole Department. One of the BUR initiatives is looking at how the different components are having a regional presence and trying to consolidate that across the Department, as well.

I think there are definitely some lessons learned from Goldwater-Nichols that could be applied to DHS, and that would be something interesting to follow——

Mr. MCCAUL. I would like to follow up with Mr. Schneider.

Perhaps, Mr. Cohn, you and I can discuss it more.

One last question—I see my time is expired—but, Mr. Reese, you mentioned an interesting fact that I was not aware of, and how many agencies outside of DHS have a homeland security mission?

Mr. REESE. The Federal department there are a total of 19, just based on research that has been done, and that is including Department of Homeland Security. The CRS Homeland Security Department fiscal year 2012 appropriations has a table in the back that I will be happy to provide to staff that breaks down funding. DHS gets 51.7 percent of the funding and then the rest is broken down in those other agencies with Department of Defense being second, at approximately——

Mr. MCCAUL. I would like to see those agencies, because what you are telling me is Homeland Security Department, which has the primary mission of defending the Nation and the homeland, essentially gets 51 percent of the funding for the mission.

Mr. REESE. Yes, sir.

Mr. MCCAUL. That is a very interesting fact. I would like to follow up with you on that.

With that, I recognize the Ranking Member.

Mr. KEATING. Thank you, Mr. Chairman. That is a great segue to my question.

I think this discussion begins with, you know, the first analysis being the 9/11 Commission Report. Earlier this year our committee heard testimony from Lee Hamilton, from Tom Ridge, and they said that one of the primary results of their report is—still remains, even after these—this period of time, unmet, and that is breaking down the jurisdictional barriers that exist. I understand, you know, I am no novice to Government, how difficult that is, but I want to tell you, it is not only the inefficiencies that you are talking about and the inability to get management in place when it is so fragmented, but I want you to comment, if you could.

I think the first view of this is: What is the effect of this fragmentation on our security itself? I look at that as the primary question that remains—and whether we are talking about, you know,

the approaches that were mentioned by our prior speakers and how to deal with it, if someone that was in the trenches saying, "Well, we have to take these small, incremental approaches to work around all these"—how important is it—we know we are wasting money; we know we are not being efficient. But in terms of security—anyone—tell me how serious that fragmentation of bureaucracies remains, in terms of our National security.

Mr. MAURER. I think it is definitely—falls in the realm of, there is not really a clear answer to that. You just don't know, actually, what the results are because you can certainly get better efficiency, better effectiveness if things are better integrated and pulled together in a more cohesive way.

But to sort of answer your question, though, it is in the realm of the unknowables. I mean, we don't really know what is being lost by not taking advantage of some simple things, like if you have a consolidated management approach it would be easier for the Department leadership to understand the tradeoffs when they are making resource decisions within the Department of Homeland Security. If you had better performance measures you would have a better handle on what parts of the Department are working more effectively than others and make changes accordingly.

When you don't have that kind of consistent management framework it is really difficult to have an analysis to address the question that you raised, which is a very key question.

Mr. KEATING. I think it is the fundamental question. You know, I look at, you know, with the President did with, you know, incorporating emerging threats and natural disasters under that same umbrella, I applaud that approach because I think he is moving in that direction.

But we have to go further. I know there is legislation here in front of the Congress that has bipartisan support, yet nothing gets moved forward. To me, what we are left with, then, with declining revenues—and you have all addressed this—is the fact that we are looking at the monies we have and determining our security strategy around those parameters instead of looking at our security strategies and our needs and our threats and saying, "What is it going to take to fund safety?"

I mean, the holes are gaping. You know, our primary person in the panel this morning talked about his biggest threat being biological threats and that there was no priority to that at all.

Yet, that was the end of the discussion. We didn't get into that beyond that. We are looking at the cyber threats and we are trying to grapple with that on the public-private side, too, and think of approaches there.

But am I wrong? But doesn't it seem like the tail is wagging the dog here, that we are looking at our limited revenues and saying, "All right, how are we going to spread this around to all these different agencies and bureaucracies?" Lost in all this is, what are we doing to really put the premium on our security needs and risk assessment, and then putting the money forward?

I represent a coastal community. The Chairman, here, represents the region that includes Port of Houston, I mentioned before. Those kind of natural disaster threats as well as terrorist threats really have a fundamental economic and security threat to our country.

Do you have any advice to us other than just do our job and start reorganizing here? Do you have any plans? Can you come out with what we should look at as a blueprint for reorganizing, making sure we have—we are doing things the right way instead of—there is another term that comes to mind; I won't use it here.

But what are your thoughts on that?

Mr. COHN. You know, from the Department's perspective, we articulated a security environment that recognized the threats that Deputy Secretary Schneider laid out. We articulated five National missions that we need to engage in and we understand we need to engage with almost the entirety of the Federal interagency in accomplishing those goals as well as with a—with an enormous stakeholder community across all of those missions.

Obviously the fiscal environment is what it is. The Department has articulated a strategic approach that it follows and a priority of goals and objectives that we need to achieve, but the fiscal environment requires us and requires our Secretary to then carefully weigh what the relative priorities will be and to allocate resources in the best way possible to optimize to those goals and objectives.

Mr. MAURER. I think historically, in the early days of the Department when it was first being stood up, it was undergoing a period of significant growth. There was a recognition that there was a substantial threat, and so frankly, there was a lot of money thrown at the Department very quickly.

They are now starting to have to reposition themselves into a more austere fiscal environment which forces them to do exactly what you are talking about. They have to start—they have to flip the lens. They have to start thinking about, what are the predominant risks and the threats facing the Nation, and align the resources and priorities accordingly. That is going to take some time.

Now, the one thing that is encouraging, I have seen evidence of that in some of the plans that DHS has put forward to address the high-risk designation, so on paper those things are there to put those things in place. But we need to see execution on those plans and we need to see sustained progress in doing so.

Mr. KEATING. Thanks.

Mr. Chairman, I am over my time.

Mr. MCCAUL. That was a very good question.

Gentlelady from New York, Ms. Clarke, is recognized.

Ms. CLARKE of New York. Thank you very much, Mr. Chairman.

Thank you, Ranking Member, and to our panelists.

My first question is for Mr. Reese: Emerging threats represent a broad spectrum of possibilities. In your opinion, are the strategies we have in place and the efforts of DHS effective in confronting these threats?

Mr. REESE. Ma'am, first of all, working for CRS I don't have an opinion.

[Laughter.]

Mr. REESE. I would also say that the definitions identified in the documents—getting a succinct definition is sufficient. We can add what we want to the definition of homeland security; what is important is identifying the missions that evolve from that definition or our concept of homeland security, and then through risk assess-

ment and through threat evaluation then prioritize those missions. I believe that is the important step that has to be done here.

It was stated earlier that these are—these documents provide principles or guidance. The next step is actually prioritizing.

Ms. CLARKE of New York. So I guess the follow-up would be: Is there anything that you have observed that may be lacking? Are there any missing components? I mean, again, you are looking at so many different ways in which the homeland is threatened today.

You know, we have talked about a few areas, but there are so many more, whether it is radiological weaponry and things that may be already resident in many of our communities. You know, we have talked about the radiological transfers for medical facilities. Is there anything that you have observed that seems to be obvious but not so obvious?

Mr. REESE. Ma'am, everything that—especially when you look at the missions and the goals identified in the Bottom-Up Review and the Quadrennial Homeland Security Review, they do—and as I stated earlier, seem to be nested in the 2010 National Security Strategy. It seems that we understand what we need to be doing; it is just figuring out how do we prioritize and to achieve those goals.

So no, ma'am, I haven't observed anything that——

Ms. CLARKE of New York. Very well.

Mr. Maurer, you sort of, like peeked up a little bit. Would you want to comment here?

Mr. MAURER. Well, it is an interesting topic, of course. Yes, I think what is really missing are sort of the things that we have already talked about from the GAO perspective, which is the National risk assessment and a more informed risk-based foundation to these kinds of analyses, and the Department says it is taking actions to do that, and that is good.

Also talked about the need for having improvements in getting stakeholders more involved in the next process for developing these kinds of strategies, giving them more time to comment, as well as doing more effective outreach to non-Federal stakeholders. We recognize that that is a key challenge for the Department since there are so many. But State, local, Tribal, private sector play a big role and we have to make sure that they are a part of developing these strategies.

We would also like to see a little more detail in the implementation plan. But the key thing from a GAO perspective is we want to see execution on these plans and an—supported by an integrated management foundation.

Ms. CLARKE of New York. Very well.

Mr. Cohn, as a follow-up, it is well settled that the multiple agencies must cooperate with each other when it comes to homeland security and terrorism-related issues. The QHSR should have included a thorough discussion of the status of cooperation between Federal, State, local, and Tribal government in preventing terrorist attack and preparing for emergency responses to threats. This was not, however, included in the final product, and it appears to be outside of the scope of the BUR.

Does the Department plan to complete this statutorily required analysis? If so, when can we expect to have it delivered to Congress?

Mr. COHN. As I think the GAO found in their review, DHS did make an—did undertake to describe the interaction between the Department and its external stakeholders as well as other Federal agencies in fulfilling its mission to prevent terrorism as well as the other missions articulated in the Quadrennial Review. What we did not do was assess the status of cooperation by other Federal agencies with their partners as opposed to DHS.

That is a very difficult thing for an individual agency to do with its peer agencies. That is a topic of conversation and something we are looking to—to understand how we would fulfill that obligation as the requirement to conduct the next quadrennial review is coming up, and we will be looking and working to figure out how we complete that portion of the statutory requirement in the upcoming 2013 review.

Ms. CLARKE of New York. Oh boy. That doesn't sound too good. I say that, you know, in all honesty because that is almost at the core of your mission, which is to coordinate, right? So if you are not getting cooperation from other Federal agencies to meet that mandate, there is a challenge there that has to be met.

Mr. COHN. We absolutely recognize our obligation, and to coordinate with other agencies, and we do coordinate extensively with our Federal interagency partners and with our vast majority of stakeholders in the homeland security enterprise. The challenge comes in evaluating the actions of other Federal departments and agencies, and that is a similar challenge to the challenge, I think, of jurisdiction that the Congress is facing, of how different organizations, with their own authorities, might look to one another and assess one another's roles.

So it is a challenge that the Department recognizes in terms of that assessment. It is a difficult process and it is one that we will be working through.

Ms. CLARKE of New York. Mr. Maurer.

Mr. MAURER. I certainly understand that DHS faces in trying to assess the level of cooperation from other departments. It is an important issue, though, and it is certainly vital to the overall success of addressing homeland security threats.

I mean, we at GAO stand ready to perform that kind of service for the Congress if that is something we have been asked to do. We certainly have criteria analysis in place to look at overall interagency cooperation.

Ms. CLARKE of New York. Very well.

Mr. Chairman, before I yield back I just want to make a quick correction. I was informed by Mr. Keating that a comment I made earlier was not accurate, and it was about—with regard to General McCaffrey's comments on comprehensive—the need for comprehensive immigration reform. Those comments were actually made in the context of responding to the Texas report that you had submitted into the record. So I just wanted to clarify.

Mr. MCCAUL. I appreciate that clarification.

Ms. CLARKE of New York. Thank you, Mr. Chairman.

Mr. MCCAUL. Let me thank the witnesses for their valuable testimony. I think this has been a very productive discussion. You know, we are not here to play "gotcha" politics. We really want the homeland security to succeed. It is the right thing for the American people and for the mission.

I want to commend the witnesses. I also want to commend all of the employees in the Department of Homeland Security for their hard efforts. It is sometimes a thankless job and it is an easy target sometimes, an easy whipping boy. But the fact of the matter is they work long, hard hours. I know the Border Patrol agents down on the border have a very difficult job, the ICE agents, and really all across the spectrum at DHS. So I want to just take this opportunity—they may not hear it very often from Congress, but I want to say thank you to all of the employees in the Department for your hard work.

With that, this hearing now stands adjourned.

[Whereupon, at 12:27 p.m., the subcommittee was adjourned.]