AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE DEPARTMENT OF HOMELAND SECURITY: PROMOTING RISK-BASED PRIORITIZATION AND MANAGEMENT

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 13, 2005

Serial No. 109–7

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

22–396 PDF WASHINGTON : 2005

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

CHRISTOPHER COX, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania, *Vice Chairman*
CHRISTOPHER SHAYS, Connecticut
PETER T. KING, New York
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

CONTENTS

Page

STATEMENTS

The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Committee on Homeland Security
Oral Statement 1
Prepared Statement 3
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security 4
The Honorable Donna Christensen, a Delegate in Congress From the U.S. Virgin Islands 40
The Honorable Peter A. DeFazio, a Representative in Congress From the State of Oregon 29
The Honorable Charles W. Dent, a Representative in Congress From the State of Pennsylvania 25
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washington 23
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina 43
The Honorable Jane Harman, a Representative in Congress From the State of California 25
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas, ... 48
The Honorable John Linder, a Representative in Congress From the State of Georgia 34
The Honorable Zoe Lofgren, a Representative in Congress From the State of California 50
The Honorable Daniel E. Lungren, a Representative in Congress From the State of California 38
The Honorable Michael McCaul, a Representative in Congress From the State of Texas 44
The Honorable Kendrick B. Meek, a Representative in Congress From the State of Florida 46
The Honorable Eleanor Holmes Norton, a Delegate in Congress From the District of Columbia 32
The Honorable Bill Pascrell, Jr., a Representative in Congress From the States of New Jersey 37
The Honorable Dave G. Reichert, a Representative in Congress From the State of Washington 21
The Honorable Mike Rogers, a Representative in Congress From the State of Alabama 42
The Honorable Loretta Sanchez, a Representative in Congress From the State of California 18
The Honorable Christopher Shays, a Representative in Congress From the State of Connecticut 31
The Honorable Rob Simmons, a Representative in Congress From the State of Connecticut 17
The Honoralbe Curt Weldon, a Representative in Congress From the State of Pennsylvania 27
The Honorable Don Young, a Representative in Congress From the State of Alaska
Prepared Statement 5

Page

WITNESS

The Honorable Michael Chertoff, Secretary, Department of Homeland Security
Oral Statement 6
Prepared Statement 8

THE DEPARTMENT OF HOMELAND SECURITY: PROMOTING RISK-BASED PRIORITIZATION AND MANAGEMENT

Wednesday, April 13, 2005

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 1:37 p.m., in Room 2200, Rayburn House Office Building, Hon. Christopher Cox [chairman of the committee] presiding.

Present: Representatives Cox, Weldon, Shays, King, Linder, Lungren, Simmons, Rogers, Pearce, Harris, Reichert, McCaul, Dent, Thompson, Sanchez, Dicks, Harman, DeFazio, Lowey, Norton, Lofgren, Jackson–Lee, Pascrell, Christensen, Etheridge, Langevin, and Meek

Chairman COX. [Presiding.] Welcome. This hearing will come to order. Today, the committee will examine the Department of Homeland Security's use of the principle of risk to prioritize America's counterterrorism strategy.

We presently have business on the floor of the House of Representatives. We expect three votes to come up in short order. Because I want to honor the time of the Secretary and the time of all the members who are here and who will be here after we vote, we are going to begin the hearing on time. We will go through opening statements and at least get those accomplished before the bells ring, and then we will immediately resume the hearing after the conclusion of our work on the floor.

Our sole witness today is the Honorable Michael Chertoff, Secretary of the Department of Homeland Security.

Mr. Secretary, we welcome you. This is your first appearance before the Homeland Security Committee, and we look forward on both sides of the aisle to working with you.

Using risk management, which is the subject of your testimony today and the focus of our hearing, is important because we have, while significant resources are devoted to homeland security, limited resources. We also have an extraordinary breadth of targets with which to concern ourselves in the country and obviously a limit to our capacity to reach all of them.

Using risk management involves, first, intelligence. We have got to examine and rely upon the information that we put together on terrorist capabilities and intentions. We have got to conduct threat assessments to evaluate the likelihood that a given asset will be subject to a terrorist attack. We have got to conduct vulnerability

assessments to identify specific weaknesses in given assets that might be exploited by terrorists. And, we have got to assess as well the potential consequences such as economic impact and loss of life to determine the level of significance of an asset and how much protection that asset should receive in comparison to others.

This kind of risk assessment, both within a particular programmatic area and across Department of Homeland Security responsibilities is a vital management tool. It is one that is new to the United States since September 11. As a result of the newness of this challenge, it is not yet possible for the Secretary or this Congress to evaluate as well as we would like the degree to which we are appropriately aligning our resources to match our nation's greatest risks.

One example of the work that we have yet to do is the billions of dollars that Congress and the Department allocate each year to states and local governments to enhance the terrorism preparedness of first responders. Instead of applying specific risks and allocating funds to address them, the system that we presently use sometimes does nearly the opposite.

Congress and the Department allocate tens or even hundreds of millions of dollars to each state and to certain local governments across the country without the prerequisite analysis of risk, and these authorities then occasionally find themselves looking for ways to spend the money. The abuses such an approach invites have been well publicized, and if not corrected ultimately will undermine our legitimate efforts to prepare our first responders for acts of terrorism.

Unfortunately, the lack of risk-based rigor affects even those DHS grant programs that are not formula driven and that are, by intention, based on competition among applicants. For example, the DHS Inspector General recently found that $67 million in port security grants had been spent on projects of "marginal homeland security benefit" and that awards had been made to private sector projects that "appeared to be for purposes other than security against an act of terrorism."

The 9/11 Commission rightly recognized the inherent dangers from this type of spending, recommending that "Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. Federal homeland security assistance should not remain a program for general revenue sharing," that according to the 9/11 Commission.

We, on this committee, and the Select Committee that preceded it, have advocated that Federal efforts to prevent, prepare for, and respond to terrorist attacks within the United States should be based on risk. That is why we introduced the original version of the Faster and Smarter Funding for First Responders Act 18 months ago.

This bill, which has been reintroduced in the 109th Congress and which Ranking Member Thompson and I have coauthored with the support of every one of this committee's members, would expedite the delivery of Federal assistance to those first responders who face the greatest risk of terrorist attack.

This kind of risk-based approach has to be expanded beyond specific grant programs to encompass all of our Federal government's

activities. Strong leadership and clear congressional direction will be required to instill risk-based prioritization in the formulation of budgets, into policies and into programs throughout the Department and across the government, and especially to legacy agencies that prior to 9/11 did not have to think this way. We cannot have 20th century programs to respond to 21st century threats.

That is why, Mr. Secretary, I noted with great interest the speech last month that you gave in which you emphasized your intention to bring a risk-based philosophy to the management and operations of DHS, and that is why we invited you here today to talk about that very topic.

Not only is such an approach necessary to enhance our national security, it is also critical to our long-term economic security. Each year, 440 million visitors arrive in the United States by land, sea, and air; 7 million cargo containers cross through our ports; and 118 million vehicles, including 11 million trucks and 2.5 million rail cars, cross our borders.

A layered risk-based security system is the only one that will ensure that our borders and ports of entry remain open and secure to accommodate the free flow of legitimate goods and travelers. We have got to work to strengthen security in ways that simultaneously improve our security and promote economic growth.

The purpose of today's hearing is to start a dialogue with the new Secretary to understand how this committee, the Congress, and the Department can work together to instill risk-based prioritization and management throughout DHS programs and operations.

I want to thank the Secretary for his testimony today and look forward to continuing this crucial dialogue in the weeks and months ahead.

I will now recognize the Ranking Member, Mr. Thompson, for his opening statement.

PREPARED STATEMENT OF THE HONORABLE CHRISTOPHER COX, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

Today, this Committee will examine the Department of Homeland Security's use of the principal of risk to prioritize America's counterterrorism strategy. Our sole witness is the Honorable Michael Chertoff, Secretary of the Department of Homeland Security (DHS).

Mr. Secretary, we welcome you in your first appearance before the Homeland Security Committee, and we look forward to working with you as you seek to build on the progress of the past two years.

RISK MANAGEMENT BEGINS WITH INTELLIGENCE:

(1) *assessment* of what is likely to be subjected to a terrorist attack;

(2) a *vulnerability assessment* to identify specific weaknesses in a given asset that could be exploited by terrorists; and

(3) an *assessment of consequences,* such as economic impact and loss of life, to determine the level of significance of an asset and how much protection that asset should receive in comparison to other assets.

Such risk assessment—both within a particular programmatic area, and across DHS programmatic areas—is a vital management tool, and one that is, new to the U.S. since September 11th. As a result of the newness of this challenge, it is not yet possible for the Secretary or the Congress to evaluate whether we are appropriately aligning our resources to match our Nation's greatest risks.

One example of this failure is the billions of dollars DHS allocates each year to States and local governments to enhance the terrorism preparedness of first re-

sponders. Instead of identifying specific risks and allocating funds to address them, DHS—with the complicity, if not outright direction, of the Congress—does exactly the opposite. DHS allocates tens or even hundreds of millions of dollars to each State and to certain local governments across the country without any analysis of risk, and these authorities then look for ways to spend the money. The abuses such an approach invites have been well-publicized, and—if not corrected—ultimately will undermine our legitimate efforts to prepare our first responders for acts of terrorism.

Unfortunately, this lack of risk-based rigor affects even those DHS grant programs that are not formula-driven and that are, supposedly, based on competition among applicants. For example, the DHS Inspector General recently found that $67 million in Port Security Grants had been spent on projects of "marginal" homeland security benefit, and that awards had been made to private sector projects that "appeared to be for a purpose other than security against an act of terrorism."

The 9/11 Commission rightly recognized the inherent dangers from this type of spending pattern, recommending that "[h]omeland security assistance should be based strictly on an assessment of risks and vulnerabilities. . . .[F]ederal homeland security assistance should not remain a program for general revenue sharing."

I long have advocated that Federal efforts to prevent, prepare for, and respond to terrorist attacks within the United States should be based on risk. That is why I introduced the original version of the "Faster and Smarter Funding for First Responders Act" 18 months ago. This bill, which Ranking Member Thompson and I reintroduced yesterday with the support of this Committee's Members, would expedite the delivery of Federal assistance to those first responders who face the greatest risk of terrorist attack.

But such a risk-based approach should be expanded beyond specific grant programs, to encompass all of the Department's activities. Strong leadership and clear Congressional direction will be required to instill risk should be risk-based prioritization into the formulation of budgets, policies, and programs throughout DHS, and especially its legacy agencies. We cannot have 20th century programs responding to 21st century threats.

That is why, Mr. Secretary, I noted with great interest the speech last month in which you emphasized your intention to bring a risk-based philosophy to the management and operations of DHS. Not only is such an approach necessary to enhance our national security, it also is critical to our long-term economic security.

Each year, 440 million visitors arrive in the United States by land, sea, and air; 7 million cargo containers cross through our ports; and 118 million vehicles, 11 million trucks, and 2.5 million railcars cross through our borders. A layered, risk-based security system is the only system that will ensure that our borders and ports of entry remain open *and* secure to accommodate the free flow of legitimate goods and travelers. Indeed, we must work to strengthen security in ways that simultaneously improve our efficiency and promote economic growth.

The purpose of today's hearing is to start a dialogue with the new Secretary, to understand how this Committee, the Congress, and the Department can work together to instill risk-based prioritization and management throughout Department of Homeland Security programs and operations.

I want to thank the Secretary for his testimony today, and look forward to continuing this crucial dialogue in the weeks and months ahead.

I will now recognize the Ranking Member, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you, Mr. Chairman, and I am pleased to welcome Secretary Chertoff to this committee.

Judge Chertoff, you are well qualified for your position, and I look forward to your service. I hope we will see you more before this committee, and I know this is your maiden voyage on the Hill. I am sure you will remember it for a long time to come.

Unfortunately, since 9/11, we have had a lot of things with the Department that have gone wrong, and you will have an awesome responsibility to help us move the Department forward. But I want to talk to you a little bit about the past failures to handle risk analysis by the Department.

This hearing is focused on using risk analysis to prioritize and manage the Department's efforts, but in the one area where the Department has experience, it is risk analysis, the development of

a database of the nation's critical infrastructure, the Department has failed miserably.

As my Republican colleague representative, Ernest Istook, told USA Today in December, the asset database list is a joke. If the Department has been unable to handle risk analysis in the past, then what confidence can we have that it will be able to do it in the future. And I am sure your leadership will help us in that respect.

If the Department really wants to prioritize and manage based on risk, then should we have some uniform definition of risk? For example, I live in Mississippi. Most of my district is along the river, and I have a nuclear power plant. Are we planning for risk based on that analysis or are we using the same standard?

Other issues, Mr. Secretary, we talked about missed deadlines. You are aware that over 100 congressionally mandated deadlines have already been missed by the Department. We have to do better. There is no question about it. Now that we have pretty much the jurisdiction as a committee, we are looking for your leadership to meet those deadlines, and we will talk about those a little later.

There are some other issues associated with the Department. The whole issue of minority participation from the staffing level is absolutely important, from the issue of Hispanic and other minority-serving institutions participating in programs in the Department is absolutely essential. At this point, under the Centers of Excellence Program, for example, there are no minority or Hispanic-serving institutions participating. We have to do better. From the standpoint of small, disadvantaged and minority business opportunities within the Department, I challenge you to make the Department responsible and adhere to those edicts.

Again, Mr. Secretary, we welcome you here. I look forward to your testimony, and welcome aboard.

Chairman COX. I thank the gentleman. Let me remind all members that you are entitled to submit written opening remarks for the record, and due to our time constraints, I would ask the Ranking Member whether members should go to the floor in response to the bells or whether we want to risk getting the Secretary halfway through his opening statement?

Do you think we should go to temporary recess while we vote on the floor? There are seven minutes remaining in this vote. That will give members time to make it, and we will return immediately and commence with your opening statement.

Mr. CHERTOFF. Thank you.

Chairman COX. Thank you, Mr. Secretary.

We are in temporary recess.

[Recess.]

PREPARED STATEMENT OF THE HONORABLE DON YOUNG, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ALASKA

Mr. Chairman, thank you for holding today's hearing on "Risk-Based" funding and management. This is an important yet often misunderstood subject. It sounds so simple, but it is extremely difficult in practice.

The basic argument goes something like this: "The Department of Homeland Security (DHS) has limited resources so it must focus its efforts and funding on those areas of greatest risk." That sounds good right? Well, only if DHS is really certain which areas are at greatest risk, and if DHS is the best agency for addressing that risk. Otherwise, we just put all of our eggs into the wrong basket.

Now I would be the first to say that DHS cannot do everything. If it tries to do all things, then it will end up doing nothing well. Perhaps the most important ability DHS needs is to understand its own limitations. DHS can then focus on what it can do well, delegate other areas to agencies with more expertise, and develop new capabilities to address risks for which we are currently unprepared.

We also need to appreciate a few simple facts. First, terrorism is incredibly difficult to predict. We have a lot of really bright and talented people working on this, but the reality is that threat and risk assessments are extremely uncertain. We simply do not know where or when terrorists will attempt to strike next. Second, security requirements have the potential to place a tremendous burden on our economy and citizens. We must be very careful not to regulate our economy into a recession or undermine our freedom. If we do that then the Bad Guys have won.

When it comes to terrorism preparedness and first responder funding, all States need to have baseline capabilities and a guaranteed minimum level of funding for at least three reasons. First, every State could be a target so they at least need to have minimum response capabilities. Second, during a catastrophic attack units from all across the country will be called upon to help respond or backfill jurisdictions that respond to the attack. And finally, DHS is responsible for assisting States respond to all disasters, not just terrorist attacks.

Thank you again Mr. Chairman for calling this important hearing. Also, I would like to thank you for working so closely with me on your first responder bill. I believe we have a better bill because of our efforts, and that it will help ensure our Nation is ready for the next attack or major disaster. Thank you.

Chairman COX. The Committee on Homeland Security will again come to order.

Secretary Chertoff, again, welcome. Thank you for indulging us during our floor votes.

Your complete written testimony will be included in the record, and you are now recognized for such time as you may consume to provide an oral summary of that testimony.

STATEMENT OF THE HONORABLE MICHAEL CHERTOFF, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. CHERTOFF. Thank you, Mr. Chairman. As you pointed out, this is my first outing before this committee. I look forward to a long and productive relationship.

Mr. Chairman, Ranking Member Thompson, I think what I am going to do is simply summarize the main points of my statement in the interest of time.

The Department of Homeland Security was created a little bit over 2 years ago, and it was created to do more than simply erect a big tent under which a lot of different organizations would be collected.

It was created to put together a dynamic organization that would identify a set of missions in furtherance of homeland security, that would execute those missions in an integrated and comprehensive manner and that would take a reasonable and sensible philosophy to dealing with the matter of homeland security. And, 2 years into the Department, coming on as the new Secretary, I have the opportunity to engage in what we call a second-stage review of where we are headed, where we have come and what course corrections, if any, we need to make.

And we undertake this process of the second-stage review with a very keen appreciation for the fine work done by my predecessor, Governor Ridge, and his deputies, Gordon England and Jim Loy. They put this together in the first instance. They launched the first stage, and that has gotten us on the mission, but we have to again ask ourselves what adjustments we need to make.

And I think broadly speaking they fall into three categories. First of all, we need to make sure that all of our activities are not focused on the process of the component that is performing the function but on the mission that we are trying to achieve.

We need to be outcome oriented, and the best example I can give to people about what I mean by this is, if I have a problem in my house, my appliances are not working, and I call the electrician, I call the plumber, I call the contractor, and they work for a day and then they come to me and they say, "Well, we have all done exactly what we are supposed to do. We followed all of our protocols, but the stuff still does not work."

I do not consider that a job well done. I consider a job well done to be when the appliances work. And that is called being outcome or mission oriented. We want the thing to work the way it is supposed to work, and we do not care about how many of the processes are checked off along the way.

So the second-stage review is designed to take a look at our missions, evaluate how far we have come, how far we need to go and then talk about how we accomplish the rest of our objectives without regard to the existing structures but with regard to what it is we need to get accomplished.

And the second piece of what I want to briefly mention is how we organize ourselves to carry out missions, and this obviously is going to be a function of our study of the mission and where we are and where we need to be. But I can tell you at this point, again, in general terms, it seems to me there are three aspects in which we need to be operating as a coordinated, comprehensive department.

First of all, intelligence. Intelligence is the driver of everything we do, and we need to operate under a common picture of the threats we are facing. There are two dimensions to that. First of all, we are collectors of intelligence, meaning that we have a lot of different organizations that interact with the outside world and collect information. We need to make sure that we are capturing all that, we are pulling it together and we are fusing it at the top of our organization. And so some of what we are going to be looking at in this review is how to make that happen and to improve our collection, capturing, and fusion of intelligence.

The second piece of intelligence is operating within a larger intelligence community, as contributors, as disseminators, and as customers. Obviously, we have a new DNI coming on. That is going to create an opportunity for us to work with the community as a whole to make sure that we are contributing the way we should be contributing, that we have the access that we need to have to do our job and that we are in a position to disseminate what needs to be getting to our Federal, state and local partners.

We need to also have a comprehensive approach to policy. Again, we have policy in a lot of different components, there are very smart people there, but we need to have a vision that looks beyond the components through the Department. And so elevating and standing up a policy organization that is capable of strategic planning and dealing with policy issues is a second matter we are paying close attention to.

And, finally, the issue of operations. We have proud organizations that are part of the Department of Homeland Security that have very strong senses of their own missions, but the purpose of the Department was to create an organization that could operate jointly, and therefore we need to make sure we have an operational element, an operations coordinator that is able to coordinate across the board so that when we take an item of intelligence and we try to translate that into action, we do it in terms of prevention, we do it in terms of protection, we do it in terms of response.

And standing up a comprehensive and robust operations function is the third piece of what we have to do in this effort to look at the way we are structured and operating.

Finally, let me touch on philosophy. As the chairman mentioned, he was gracious enough to mention early on in his remarks, a few weeks ago I spoke at George Washington University and talked about risk management as the template for how we do our work, and that means that in our handling of grants, in our deployment of resources, in our policy making we have to be driven by a disciplined, analytical approach that looks to the issue of measuring consequence, measuring vulnerability, and measuring threat.

And, obviously, there are a lot of subtleties involved in applying this general template to the kinds of individual issues that we face. But if we are at least clear about what our overall philosophy is, I think that is going to go a long way to making sure that we have a coherent and sensible and reasonable set of priorities about how to deal with homeland security.

As the chairman has observed, we cannot protect everybody in every place, at every time. We have to prioritize, and I think we are launching a process through this review of making ourselves better at doing that.

That being said, I look forward very much to working with the members of this committee in the weeks and months to come, and I am delighted to be here and to answer your questions.

[The statement of Mr. Chertoff follows:]

PREPARED STATEMENT OF THE HONORABLE MICHAEL CHERTOFF

INTRODUCTION

Mr. Chairman, Representative Thompson, and Members of the Committee: Thank you for the opportunity to address you today, and for your ongoing support of the Department of Homeland Security's efforts to keep America secure and free.

I am honored and pleased to appear before the Homeland Security Committee. This is my first appearance before the Committee, and I look forward to a productive exchange as the Department begins to reassess and readjust priorities and policies in accordance with the changing threat of terrorism over three and a half years after the September 11, 2001 attacks.

For more than two years now, the Department of Homeland Security has led a national effort to protect our country and our citizens from all manner of threats. It has been an honor to join the dedicated men and women who carry out this task daily. Ours is a difficult mission—to prevent another deadly and catastrophic terrorist attack such as the one we experienced on September 11, and if an attack occurs, to respond quickly and prevent further damage.

The 180,000-plus people of the Department carry out this mission with unflinching resolve and a driving determination that such an attack should never occur on American soil again. Realizing that we can make no guarantees, we pursue our mission with a sense of urgency and daily diligence, so that this nation can respond and recover quickly, should an incident or attack occur.

Since its establishment just over two years ago, DHS has made great strides in its efforts to unify the defense of our homeland. We have continued to integrate 22 distinct agencies and bureaus, each with its own employees, mission and culture.

But our security requires even greater coordination and effort throughout the Department, across all levels of government, and throughout our nation to create synergy and new capabilities. It requires an unwillingness to accept complacency as part of anything we do; rather, we know we must apply all effort to tear down stovepipes and coordinate key intelligence, policy, and operational issues across DHS and the government.

SECOND STAGE REVIEW

I have therefore initiated a comprehensive review of the organization, operations and policies of the Department as a whole. This comprehensive review will examine what we are doing and what we need to do without regard to component structures and programmatic categories.

We want to understand better what's working and what isn't. We will be evaluating every element of our working mission and making sure that the Department is best organized to meet the threats—both current and future—that face our nation.

Old categories, old jurisdictions, old turf will not define our objectives or the measure of our achievements because bureaucratic structures and categories exist to serve our mission, not to drive it.

Deputy Secretary Michael Jackson has been charged with overseeing this process. The goal of the review is to help me make informed decisions as I lead the Department. Deputy Secretary Jackson has selected a team of Department officials to look at a number of critical cross-cutting issues and determine how departmental resources and programs can be most effectively applied to achieve our security goals. I have asked them to get back to me by Memorial Day with the bulk of their recommendations. I intend to study and act on their recommendations.

What will the review cover? Take an issue such as maritime cargo security, which cuts across several departmental components. Customs and Border Protection, Coast Guard, Science and Technology, Information Analysis and Infrastructure Protection, and the Transportation Security Administration each address aspects of this overall mission. Each might perform its element well, but we must go further to ensure that each is performing seamlessly and in coordination with the others, that we eliminate any duplication of effort, and that we reap the full strength of our wide spectrum of capabilities.

Of course, in executing the initial phase of putting the Department together and integrating the different components into a working structure, my predecessor and the men and women of Homeland Security did a tremendous job. They should be commended.

Now, as we enter into the second phase of the Department's life, we must also take a fresh, creative look at the Department itself—including its organization, its operations, and its policies. We are not yet fully integrated and our entities are still not always coordinated with each other. Now the challenge is to take the advantage of two years' experience and evaluate the Department to see if there are potential structural and operational changes that will improve and enhance our capabilities to protect and safeguard this nation.

CROSS-CUTTING FUNCTIONS AND INTEGRATION

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a common picture of the threats that we are facing. Second, we need to respond actively to these threats with the appropriate policies. Third, we need to execute our various component operations in a unified manner so that when we assess the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board.

My intent is to integrate each of these three areas-intelligence, policy, and operations—across the Department, so that each is directed from the most senior level of the Department.

Let me turn to intelligence. Intelligence plays a pivotal role in mapping our mission. When the Department was created, 22 separate and distinct entities were

woven together, a number of which had components focused on intelligence-gathering and analysis. One of my top priorities is to make sure that these various intelligence components function as a cohesive unit, and that our information and analysis is coordinated across the Department so that DHS, as a full member, can enhance its contribution to the Intelligence Community.

First, we must organize and combine all intelligence within DHS. To do this effectively, we must ensure that our own intelligence components are interoperable. The Department has already made progress in this area. For example, the Homeland Security Operations Center was stood up to help the Department develop a common operating picture and facilitate information sharing.

We must make sure that we are gathering all relevant information from the field, communicating with each other, and approaching analysis with a mission-oriented focus. We must ask, for example, whether those who evaluate the border from the Customs and Border Protection perspective are learning from analysts in the U.S. Coast Guard. They each look at border security, but from different vantage points. Only if they are working together can they fill in key gaps, paint a realistic picture, and evaluate all of the different pieces of information and intelligence that they are each gathering. We have to maximize the fact that all of these components now exist under the same umbrella.

Second, we must make sure that information is being disseminated both up and down the ranks of the Department. Strong and effective coordination does not just mean that our analysts at DHS headquarters are working together. We need to fuse and exploit all the information that we learn across the country, so that when a Border Patrol agent in Texas learns of a new alien smuggling method, that information is fed up to our intelligence analysts, incorporated where appropriate into our strategy to combat smuggling, and disseminated across the Department to others focused on the same problem. We must build a culture in which the disparate pieces of information are being transmitted to our analysts so that they, who have the benefit of the fuller picture, can properly analyze all of our information and inform our decision-making.

The converse must be true when our intelligence analysts learn of new vulnerabilities that terrorists are trying to exploit. That same agent in Texas needs to know, on a timely basis, of the threat and what he should be looking out for. We have a great many talented individuals at the Department. Some gather and analyze intelligence. Others learn critical information as they are in the field performing their jobs. The opportunities are endless. DHS needs to bring all of these nuggets of information together and disseminate them appropriately. We need to have the structure and the correct systems and technologies in place to take full advantage of them.

Third, our focus must extend beyond the Department itself. We must review and make use of intelligence coming from the Intelligence Community and we must play an active role in providing intelligence information to the Intelligence Community. As the WMD Commission made clear in its report two weeks ago, sharing information across the Federal Government is critical if we are to succeed. To that end, I am committed to making sure that our law enforcement and intelligence partners across the Federal Government have appropriate access to the Department's information and analysis, to the maximum extent possible under the law, while protecting the privacy rights and civil liberties of Americans. By the same token, we must sit as full partners at the table with full access to others in the Intelligence Community. We must work in concert with the Intelligence Community. I will work closely with the Director of National Intelligence, whose job it will be to make sure that the Intelligence Community is well-coordinated and mission-focused.

In addition, intelligence and information from other Federal agencies is critical to our efforts to secure the homeland. The development of the terrorism information sharing environment, as called for under the Intelligence Reform and Terrorism Prevention Act, will connect the resources (people, systems, databases, and information) of Federal, State, and local governments, and the private sector allowing users to share information and improve collaboration.

Finally, we must inform and communicate with our State, local, tribal entities, and private sector partners. As I observed just last week during TOPOFF, when it comes to securing the nation, we must ensure that these entities are well-equipped both to react to crisis and to prevent it. As part of this effort, we must improve our ability to operationalize intelligence. As information comes in, we need to make sure it is getting out to the right people and in a way that they can use to strengthen their efforts and contribute effectively to ours. Intelligence in a vacuum is meaningless. We need to explain how our outside partners can counter that threat and what we need them to do to watch out for it.

Now, let me address policy development. Development and coordination of policy are major responsibilities of this Department. The Department has the central mission of securing the homeland, but there are many different aspects of that mission with numerous contributors. Large elements of DHS include traditional operational functions in which we deploy personnel, equipment, planes, ships and vehicles. But other elements principally involve planning and rule making, and networking with State, local, and tribal entities, and private parties. All of these must serve and promote our homeland security imperatives.

Therefore, we need to further enhance our capability to think through broad and over-arching issues like border security, emergency preparedness, transportation security, and cargo security, with a Department-wide perspective, rather than just through the lenses of one particular component. We need to develop our policies by first looking at our missions and asking the comprehensive, result-oriented questions, rather than by looking to one particular entity that has the lead in driving an issue to conclusion.

Accordingly, I believe that we should pull together the vast expertise and the varying perspectives already at the Department as we work toward integrating our many cross-cutting functions. For this reason, one of the areas that we are closely studying in the Second Stage Review is the advisability of creating a department-wide, substantial policy office. This office will also be a very important focal point for coordinating DHS's policy work with other Federal, State, local, and tribal entities.

Finally, let me discuss operational coordination. Just as with intelligence and policy, we need to find new ways to increase our operational coordination. Diverse operational components were woven together when Congress stood up the Department, each with its own history and identity. As I have become acquainted with these various components, I have quickly learned that there is a great deal of talent within them. Each entity has its own unique focus, but often they address the same mission from differing perspectives. But we cannot function as a cohesive unit, unless each operational component works together in combination to promote common missions.

This means that our operations must be driven by mission-oriented plans. It can no longer be the case that different components tackle different problems each in its own way and then later look to see if the pieces fit together. Whether it is preventing a potential act of terrorism, emergency preparedness, border protection, or countering a particular threat, we must first define the mission and second deploy all the tools within the Department to effectively execute each operation.

The Department has already begun this process. To take but one example, on the Arizona border, we have a cross-cutting initiative to protect the border, integrating intelligence gathering, border enforcement, and monitoring. It encompasses the efforts of several of our agencies, including Customs and Border Protection, Immigration and Customs Enforcement, Science and Technology, the Coast Guard, and Information Analysis and Infrastructure Protection. Each plays an integral role. The operations themselves involve patrolling the border, generating information, and using it to take enforcement actions. The genius of the Department of Homeland Security is that we have the capability within one department to do all of these things. But we need to carry out joint operational activities and have a joint perspective on a routine basis, not only when we stand up a special project.

Operations are also the mechanisms by which we respond to crisis. We cannot wait for a crisis, however, to learn, for example, whether TSA has the capability to communicate effectively and coordinate with FEMA. Nor can we learn in crisis that both are conducting the same operations or sending different messages to the private sector. The Department has made significant progress in this area. For example, it developed the National Response Plan to more effectively map out how to handle crisis situations. Now is the time to organize around missions rather than old bureaucracies, work through all of these potential disconnects in our systems, and operate as one unified Department.

But integrating ourselves cohesively is not enough.

RISK-BASED APPROACH

I have been saying, and you will continue to hear me say, that we need to adopt a risk-based approach in both our operations and our philosophy. America is dynamic. Our strength as Americans is the sum of every generation that has ever been born in or immigrated to this great land. Our wealth and livelihoods are advanced by the inspired ideas and innovation of our own people. We prosper through the vast opportunities that exist to interact with the global economic community.

Risk management is fundamental to managing the threat, while retaining our quality of life and living in freedom. Risk management must guide our decision-making as we examine how we can best organize to prevent, respond and recover from an attack. We need to be realistic in our prioritization. We must assess the full spectrum of threats and vulnerabilities.

We all live with a certain amount of risk. That means that we tolerate that something bad can happen; we adjust our lives based on probability; and we take reasonable precautions.

So, too, we must manage risk at the homeland security level. That means developing plans and allocating resources in a way that balances security and freedom when calculating risks and implementing protections.

The most effective way, I believe, to apply this risk-based approach is by using the trio of threat, vulnerability, and consequence as a general model for assessing risk and deciding on the protective measures we undertake.

Here I inject a note of caution because the media and the public often focus principally on threats. Threats are important, but they should not be automatic instigators of action. A terrorist attack on the two-lane bridge down the street from my house is bad but has a relatively low consequence compared, to an attack on a major metropolitan multi-lane bridge. At the other end of the spectrum, even a remote threat to detonate a nuclear bomb is a high-level priority because of the catastrophic effect.

Each threat must be weighed, therefore, along with consequence and vulnerabilities.

As consequence increases, we respond according to the nature and credibility of the threat and any existing state of vulnerabilities.

Our strategy is, in essence, to manage risk in terms of these three variables—threat, vulnerability, consequence. We seek to prioritize according to these variables. . .to fashion a series of preventive and protective steps that increase security at multiple levels.

We must examine the mission and work of all elements of DHS through this template of consequence, vulnerability and threat. Have we fully defined our missions? How far have we gone in carrying them out? What more needs to be done?

The Department is already working with State, local, and private sector partners to further refine the Interim National Preparedness Goal to aid the targeting of resources to where the risk is greatest. There is much that we are doing. DHS agencies, for example, have provided unprecedented level of funding and resources since 9/11 to State, local and private sector partners to protect and prepare America's communities and individual citizens. We continue to improve the ways for first responders across the nation to be better equipped, better trained and more capable of communicating across the public safety community. But we must bring even greater focus and discipline to our preparedness mission. We need to take a very substantive look at how we align our preparedness activities and functions. We need to look at how best to configure our organizations, operations, programs and policies so that we can think strategically about preparedness.

What should drive our intelligence, policies, operations, and preparedness plans and the way we are organized is the strategic matrix of threat, vulnerability and consequence. And so, we'll be looking at everything through that prism and adjusting structure, operations and policies to execute this strategy.

CONCLUSION

Two years ago, Congress and the President took on the enormous undertaking of creating a new Department whose central mission would be to secure the homeland. Under Secretary Ridge's leadership, the entities that now comprise the Department of Homeland Security unified under this overarching goal. As I have become acquainted with the many talented people of the Department, I am impressed by all that they have accomplished thus far. But there is no time to pat ourselves on the back. We must now take it to the next level.

We must move in an expeditious and innovative manner to carry out our important mission. On September 11, 2001, we learned that the homeland is not immune from attack and that we must do everything within our means to keep our great nation safe. The Congress responded by constructing a Department dedicated to this mission. Together, our job is to make sure that the Department accomplishes that mission. As the Department initiates our second stage review, organizes around missions, eliminates duplications, and adopts a risk-based approach, we must identify our cross-cutting functions and ensure that we are thinking innovatively how to best exploit our intelligence capabilities, develop policy functions, execute our operational tasks, and implement our long-range preparedness planning.

I thank the Congress for its support, which has been critical in bringing us to this point. I am grateful to be here today to talk about the work we are doing to make America a safer home for us, for our children and generations to come. Thank you for inviting me to appear before you today. I look forward to answering your questions.

Chairman COX. Thank you very much.

And let me take this opportunity to tell you how personally pleased I am that President Bush asked you to do this job. I know that he has selected the right person for the most important task of management and organization in the Federal government at this time.

We have a high degree of confidence in your ability to do this, and the second-stage review that you are going through right now is, in my view, a very important first step to making sure that we benefit from all that we have learned since 9/11 and all that we have learned since Congress mandated the creation of what is now the second largest cabinet department in terms of authorized spending.

You and I have spoken in other venues, and as you mentioned, you delivered a speech expressly on this topic about how we might bring more disciplined approaches to risk management, to the choices that we make—policy makers here in Congress—and the decisions you make as the manager of that Department when it comes to setting priorities, to determining which threats we are going to protect against, and where we are going to place our money across America and around the world.

One of the things that has struck me for some time is that, because of the newness of this task, we are not yet accustomed to making tradeoffs of any kind, so that if someone points out that terrorists might do this, or that this many people would die if terrorists were to choose this site or this method of attack, there seems to be a reflexive response to go after that, the, if you will, "seize the pants" approach to risk management.

Congress, in my view, is much more guilty of this than is the Department, because we are in the job of earmarking things sometimes, and we just indulge our collective priorities in this way. We need to discipline ourselves in Congress, and we need to help you as we authorize and send you money to maintain discipline in the Department.

Forty thousand Americans, innocent Americans are going to die this year here at home, in the continental United States in car accidents. This is a risk that we knowingly take. It is a cost that we knowingly bear. The Federal government will spend this year about $600 million to mitigate that risk on highway safety programs, but it has taken us a century to internalize this risk management approach with the automobile.

We know that the best way to reduce that risk to zero would be to stop driving or stop being passengers in cars or stop using crosswalks. We do not do that because life has to proceed, and there are tradeoffs involved.

There are tradeoffs also involved, as we put our economy on the block, send a lot of its resources to preparations for terrorist attack, towards intelligence to warn us of terrorist attack, and so on. We have to find the right balance. We need to find which terrorist threats are the most consequential, which are the most likely, and

where are our greatest vulnerabilities, and in a much more systematic fashion put that all together.

As you conduct this second-stage review, what are the opportunities that you see for doing this within the Department? What are the big picture approaches that you are going to take to head in that direction? And then what, in terms of specific resources that you might need to accomplish this task, do you want assistance from Congress on in order to help move us in that direction?

Mr. CHERTOFF. Well, thank you, Mr. Chairman, for asking me that question, because I think it really goes to the heart of what we are trying to do here.

I think we have a couple of opportunities, broadly speaking. First of all, we are going to undertake the process of looking at our objectives in terms of these three issues: consequence, vulnerability, and threat.

For example, take the issue of cargo. Cargo security is the issue that falls within the responsibility of a number of components of the Department, but what I am interested in seeing is if we look across the board at how we deal with the issue of cargo security and efficient movement of cargo, which are two important goals, I want to look at it across the board, and I want to look at it without thinking about what the components have responsibility for. I want to see it in terms of the outcome of a secure but efficient cargo transmission system. Where are we doing a good job in promoting that, where are we not doing a good job and then plugging the gaps.

And we are going to apply that template across the board to things like how do we keep bad people out of the country, how do we better service people who want to come into the country and become productive members of America by getting citizenship? How do we deal with the issue of airline security in a way that properly focuses on the priority risks in a way that allows people to enjoy air travel without having it become so cumbersome and difficult that they actually choose other forms of transportation? So this is the approach we want to take across the board in terms of what we are doing.

In terms of how we actually analytically start to measure these things, one of the questions I have asked is how do other parts of the government, what kind of analytical tools do they use in measuring risk, what does the private sector use in measuring risk? People do this all the time. As you point out, each of us does this in our own life when we decide whether we want to get in a car and go to the movies, and we trade off the risk of getting into an accident against the benefit of the movie.

But, actually, government and private industry do this all the time too, and they have a variety of tools for doing so. So as we are developing and refining our analytical tools, I am asking people to be looking at other departments and get expertise from their experience. The EPA has certain analytical tools they use, DOD has certain tools and practices they use, and try to, again, use the benefit of all of this experience to help us sharpen our own ability.

And I think we are—one example of this is the preparedness goals which we issued, I think, in the last couple of weeks are an effort to start to really identify capabilities that responders need in

a variety of different scenarios so that we can then start to be quite specific about what kind of equipment should they be looking for, what kind of training should they be needing, and that would be the kind of tool one could use, again, bearing in mind potential consequences and vulnerabilities and threats so that when we advise people about what to do and we talk to government entities about the kinds of steps they ought to take, we can do it with a very specific and disciplined approach.

How can Congress help? I think it may emerge, and of course we are still waiting for the results the recommendations that I hear that there are some structural changes that would be efficient, that might help us comprehensively operate the Department more readily and at the same time might flatten some of the bureaucratic structures, so that we would have the benefit of both coordination and yet a more nimble ability to manage. And I think as we develop this review and get a better sense of what we need to do, we may be asking Congress for some assistance in that regard.

Chairman COX. Thank you. My time has expired.

The gentleman from Mississippi, Mr. Thompson, is recognized.

Mr. THOMPSON. Thank you, Mr. Chairman.

Appreciate your testimony, Mr. Secretary. You have indicated that you have undertaken this second-stage review in a number of things, but let me call a situation to your attention that causes concern for a lot of us.

You had three directors at TSA in 3 years. You have no head of the Border and Transportation Security Directorate. You are missing the entire leadership of the Infrastructure Analysis and Infrastructure Protection Directorate, you have no Cybersecurity Director and you are about to lose your Chief Information Officer, your Director of Citizenship and Information Services, and your head of ICE.

That is a significant challenge for you, and I would just like to hear how you propose to close that gap and give us some confidence that we can get some people who will stay on the job long enough to finish it.

Mr. CHERTOFF. Well, of course it is a concern to me to make sure we have a good leadership structure in the Department, and it is not unusual after people serve a number of years in office for people to move on. In some cases, we have had more rapid turnover than in other cases.

I can say, for example, with respect to infrastructure protection, I think the President announced last week his intention to appoint someone to that position who has been a very significant member of the Department, Bob Stephan, so that is a position that we are moving to fill. I now have a Deputy in place, there has been a General Counsel nominated, and with respect to a number of these other positions, we are moving rapidly, working to find the right person for the job.

I mean, there is an opportunity here as well to draw creative energy and fresh perspective to the job that we have not had. And so while it is, in some sense, a burden to fill the turnover, there is an opportunity we intend to exploit to get very good people into the Department to bring a lot of energy and creativity to the task we have to do.

Mr. THOMPSON. One other question, and I would hope that my comments earlier about diversity as you select the leadership in homeland security, that it is one of the considerations that you would look at. I think it is important that diversity is taken into consideration.

With respect to the infrastructure protection and national infrastructure risk analysis, we have information that there is an inordinate amount of contractors and detailees in the Department and not enough people who are actually employees of the Department of Homeland Security. If that is the case, how do you propose to consolidate this Department so that those individuals become employees of the Department of Homeland Security?

Mr. CHERTOFF. Well, as I sit here, I cannot tell you that I have a clear picture in my mind of where we have a lot of contractors. I know traditionally it is not uncommon, particularly in standing up a department and trying to get people with the skill set in, to have contractors. But I would like our Department to develop an internal structure for career development that would make, first of all, a very attractive place to work and to recruit and also build within the Department a spirit of opportunity for advancement and for education and for improvement that would, again inspire our workforce to do a good job.

I mean, one of the things that interests me in terms of building a single department is developing within the career path for people who work in the Department an advantage in cross pollination, moving out of their particular agency and perhaps working at a joint coordinating function or a department-level function, much the same reason the military does to some extent. They encourage their officers to spend some time in a joint planning or operations function as a career development element, and that has the benefit of giving people a little bit of a perspective of other parts of the Department.

So one of the things I am looking forward to doing is working with the employees to see if there are ways we can use the career advancement process to bind us together as a unitary organism.

Mr. THOMPSON. Last question, Mr. Secretary: We have had some security breaches with the staff at companies like ChoicePoint, Lexus Nexus. Have you directed your department to look at that as a potential risk for us to be concerned about?

Mr. CHERTOFF. Well, of course, as you may know, Secret Service obviously has an investigative responsibility and shares it with the FBI in this particular area. The area of identity theft is a very serious area that we are concerned about from a number of different standpoints. I mean, obviously, from a cybersecurity standpoint, we are concerned about hackers. That is one kind of threat.

My understanding, at least in the ChoicePoint, is it was not so much a hacker as it was their internal decision to sell some of their product to somebody who turned out to be different than who they expected. And whether that is something that is corrected investigatively or in some regulatory reform, I do not know that I am prepared to say at this point.

But I do agree that the issue of identity theft and identity use is not something we are very carefully focused on in terms of a whole range of issues that we consider in the Department, includ-

ing things like screening for identity, and that brings us to the issue of biometrics, which of course is one way to deal with this kind of problem.

Mr. THOMPSON. Thank you.

Chairman COX. The gentleman's time has expired.

I would advise members that under our committee rules, members will be recognized for questions in order of seniority present at the time of the fall of the gavel. For members who arrive later, they will be recognized in order of appearance.

The Chair now recognizes the gentleman from Connecticut, Mr. Simmons.

Mr. SIMMONS. Thank you, Mr. Chairman.

Thank you, Mr. Secretary, for your testimony. I was very pleased to see in your testimony that you laid out three priority areas—intelligence, policy and operations—and spent much of your testimony dealing with the area of intelligence.

It is my honor to be now serving as the chairman of the Intelligence Subcommittee with my colleague from California, and I believe that the fundamental obligation of the Department of Homeland Security is to protect our homeland, to protect our citizens and our people from attack and the greatest investment that we can make is in intelligence so that we can detect, deter, defend, disrupt or mitigate any such attacks and that while we must prepare, as we have in the TOPOFF exercise, for a failure of that system, that it is most important to put our money up-front and put it into intelligence.

In saying that, I am aware of the fact that the 9/11 Commission report and the recent Robb report have laid out serious failures of the U.S. intelligence community. I am aware of the fact that your organization is relying, in many respects, on information collected by that intelligence community, that that intelligence community has relied on secret systems of collection, which do not necessarily lend themselves to domestic activities here in the United States, because we value our civil liberties, we value our civil rights, our Fourth Amendment rights to privacy.

And so my question to you would be to what extent have you looked at open sources of intelligence to feed your information analysis system? To what extent do you believe the intelligence community is actually sharing information with you? And I can tell you as a former CIO, there is a culture against sharing, we all know that, that is the way it goes. To what extent are your requirements being given priority in the intelligence cycle, by the intelligence community? And, finally, do you feel that the Department of Homeland Security is sitting at the table? In other words, do you have a representative, for example, on the President's Foreign Intelligence Advisory Board or other similar boards at this point in time.

Mr. CHERTOFF. Congressman, I am delighted to answer those questions, and I think I have tried to keep track. If I miss one, come back and remind me.

Taking them in turn, I think you have put your finger on something very important when you talk about open source intelligence. My observation has been oftentimes people think of intelligence as by definition something that is only done with spies or super secret

satellites. And in fact intelligence is often the accumulation of individual facts which may be right out in the open.

One of the things I am doing internally at the Department, and we have talked to the intelligence people about, is recognizing the importance of the thousands of interactions that occur at the border, on airplanes, and through ICE every day that yield important information.

In fact, hypothetically, we find that people with a particular connection to a terrorist group that turn up on our watch lists are seeking to cross the border in a lot of different places at the same time. An individual officer might not necessarily see the significance of a single interaction, but if we can collect all that and we can bring it up, that is going to tell us something very important.

So we are going to work very hard, and this is one of my priorities, to strengthen internally our collection system to develop a system which I think is similar to what the Bureau is putting into effect of making sure we are getting good reporting in the field that we can then bring up and fuse together in order to maximize what we do internally through what is either open source of just kind of fairly routine intelligence collection.

Second, we need to be able to contribute that to the intelligence community because that is sitting at the table. I think generally my experience with organizations is your value as a partner is directly proportional to your contribution as a partner. So we need to complete this function so we can contribute.

But at the same time, as you point out, we need to be full partners at the table, because we have a need for intelligence and a use for intelligence that no other department of the government has, because we have to take it and apply it directly to homeland security functions: how we handle our border, how we adjust our internal investigations with respect to people who are coming in illegally, how we structure ourselves in terms of what we prioritize for protection purposes.

So we need to force from that large pool of information that the community has those items that are of interest to us. And I have spoken to others in the community about the importance of doing that. We obviously have—the President has nominated Ambassador Negroponte as DNI. I am very hopeful that the restructuring of the intelligence community and the addition of Ambassador Negroponte and General Hayden, if they are confirmed, will be a great opportunity for us to participate in the community at large.

Finally, with respect to the issue of requirements, I certainly have made an effort in my 2 months here to make it very clear that our requirements ought to be treated significantly in terms of gathering information, and so far, again, in the brief time I have been here, I have seen a positive response from the intelligence community. But it is certainly something that I will be paying a good deal of attention to and will be insistent upon because we need it to do our job.

Chairman COX. The gentleman's time is expired.

The gentlelady from California, Ms. Sanchez?

Ms. SANCHEZ. Thank you, Chairman Cox.

And thank you, Mr. Secretary, for being before us today, and good luck.

Mr. CHERTOFF. Thank you.

Ms. SANCHEZ. As you know, one of the challenges of securing critical infrastructure is that the majority of it is owned by private companies. And in addition to making incentives for them, I think that we probably have to set a minimum set of standards, or at least that is what I have heard from private companies, some sort of standard so that all the companies in a sector are doing the same thing or meeting the standards that we have.

And while numerous DHS agencies like the Coast Guard and TSA and Customs and Border Protection have regulatory authority, the Infrastructure Protection Division does not. Do you believe that it should have so that if we need industries to comply with standards that we set that they should have that? And if so, is that able to do regulatory work at this point?

Mr. CHERTOFF. Well, I think that obviously, as you point out, there are an array of things we can do to get private business to do what needs to be done for security and, again, balancing that with respect to the need to actually carry out their jobs. I mean, I think we always have to be mindful of the fact that we do not—I can guarantee perfect security at the port, for example, if I shut the port down. That would be self-defeating.

So I think the first thing is to make sure that the private sector understands that we have an identity of interest here. I mean, people who put a big investment in their business do not want to see it go up in smoke or do not want to see themselves losing customers because there is a problem.

So the first thing we have got to do is we have got to educate them to that. We have got to give them standards and best practices that will enable them to make their choices wisely about how in fact they do protect themselves. We have to use market-based incentives when we can, including working with the insurance community.

I can tell you from the Y2K experience we had a few years ago that we can get the private sector to be quite sensitive to the need to secure things if we work with the insurance community and we work with the marketplace to building incentives.

Now, there are going to be some instances where that is not going to be enough, and I know, for example, in the area of chemical plants, the President has indicated that if we could not get what we need in terms of security using these various kinds of market-based incentives and best practices, that we would look to the possibility of some kind of regulation in order to make sure we get to where we need to get.

So I think these are all tools we have to have available to us. The idea is to try to work with the interest of the private sector, which I think is identical to ours, where we can.

Ms. SANCHEZ. I understand that, Mr. Secretary. I am just telling you that when I have spoken to private sector companies, their big pitch is, "Look, we would like to, it is going to cost money, we need a set of standards, we need to know what you think should do in conjunction, obviously, planning with them." But, more importantly, they are concerned that their competitors will not be required to do the same thing that they would like to do but will cost money. So, again, the question is, can this agency take on the re-

sponsibility of being a regulatory agency if that is what we deem in the Congress, in conjunction with the administration?

Mr. CHERTOFF. Well, we certainly do have some regulatory authorities, and as I indicated in the area of the chemical plants, there are obviously some times when you need to regulate in order to prevent people from free riding, basically, and relying on others to enhance security and not doing it themselves. But, as I said, we want to be judicious about it.

I think there is a lot we can do. We clearly have to set good standards, and we have to let people know what works and what does not work, and that is part of what we are trying to do right now.

Ms. SANCHEZ. I had a second question because I sent you a letter with respect to the TIP grant and it looks to me like you are eliminating existing port, rail and transit security grants under the Urban Area Security Initiative and putting them all together.

On March 9, before the Senate Homeland Security and Government Affairs Committee, you testified that you thought in general every type of transportation presents its own issues, and I agree with that statement, and that is why I feel it is unwise, and I sent you a letter signed by some of the members of this committee, for the Department—I think it is unwise for the Department to force all of the transportation sectors to compete against one another for that funding.

I am also concerned that the program will not work without a completed national threat assessment, national infrastructure protection plan and national asset database to help us all decide how to prioritize funding. And of course the budget only has $600 million. It is nowhere close to meeting the needs.

Could you comment on that?

Mr. CHERTOFF. Sure. I mean, clearly—well, let me begin by saying, I think, in general, the idea of allowing a broader category of infrastructure to be measured makes sense in terms of risk management. It is true that they present peculiar issues and different issues, but at the end of the day there are certain commonalities that we have to be concerned about, going back to what we originally talked about: consequence, vulnerability and threat.

And in allocating money and in taking account of these three characteristics, you know it is going to differ depending on where you are in the country. In some parts of the country, rail service is a huge part of what moves people back and forth. In other parts of the country, it is less significant in terms of its impact on population. Likewise, the way air or bridges are configured and how they would be measured from an infrastructure protection standpoint might differ.

So the ability to look at all of them together I think makes sense if we are going to be risk-based. But you are also correct that we then have to be pretty specific about the kinds of characteristics we are going to look at. And I think we are moving down that path, although we are not there yet.

We have, I think, each year that we have been involved with grants gotten more refined about the kinds of things we look at that enter into our formula for grant making. We are developing better and more refined tools for analyzing consequences, what the

relative significance of consequences are, what the vulnerabilities are and what the threats are, so that these common principles, I think, as we get more information, we get more sophisticated analytical tools will in fact be the way in which we operate an infrastructure protection program in the most intelligent way possible.

Ms. SANCHEZ. Thank you, Mr. Chairman.

I guess I would just say it is difficult for me to know which is more risky, ports or rail, transit or buses, and I do not think anybody here can answer that. And we have been waiting a long time to get some more information on the infrastructure protection plan and its assessment through threat-based threats and vulnerability. And I think the chairman talked quite a bit about this. And I am hoping that you will spearhead that and get that done for us so we can do our job up here.

Mr. CHERTOFF. I will.

Chairman COX. The gentlelady's time has expired.

The gentleman from Washington, Mr. Reichert?

Mr. REICHERT. Thank you, Mr. Chairman.

Good to see you again, sir.

Mr. CHERTOFF. Good to see you.

Mr. REICHERT. Just a couple of quick things. First of all, I think we need to pause for just a second and as I was reading through the first page of your comments, "Ours is a difficult mission to prevent another deadly, catastrophic terrorist attack." Stop and think about that.

I mean, our world has changed tremendously. You have only been in this job 2 months. This is your mission: Protect the country, the United States of America. You have 180,000 employees to do that with. Not only is it your mission to protect this country from another attack, but then you also have a mission to assure that we can respond and recover quickly to the huge task ahead of you. I hope that we can help you in your task, as you mentioned earlier in some of your comments.

I agree intelligence really is where we need to focus our efforts and our attention. Intelligence is where we will be able to assess risk, gather intelligence, analyze intelligence, investigate those leads that intelligence offers us, and once we have assessed risk then we can allow and understand—we can allow our resources to be placed in those areas where those risks are identified.

We do that every day in the sheriff's office. As you know, I used to work for the sheriff's office in Seattle and you assess risks and have to analyze where to put your resources every day. One of the things that really is important, though, as you go through that whole exercise and process of gathering intelligence, analyzing intelligence and assessing risk, and then assigning resources, is accountability.

And my question is, as the money is allocated, for example, in the State of Washington $234 million have been allocated to the State of Washington, $60 million alone to Seattle–Tacoma area in the Northwest, only 27 percent of that money has been spent thus far. And as we know, as we watch "60 Minutes" and some other reports come out, some of those monies are not being spent in a wise way. What is your plan for holding not only your people internally accountable to do their job but how do we hold those other

agencies, those local agencies accountable to use the funding that has been allocated to them?

Mr. CHERTOFF. Well, I think this is obviously a very important issue for us. We issued in the last couple weeks interim national preparedness goals, which basically set forth 10 tasks and I think 38 capabilities, which cover the range of things we think that state and local governments need to be able to be prepared to do in the event of any number of scenarios that might occur. In fact, I think you got a lot of publicity because in building those capabilities we essentially imagined a bunch of scenarios that were pretty grim and then used those as ways of identifying the kinds of things you would need to be able to do if something like that happened.

Underneath that one document is a series of templates, and each of those capabilities that is really quite specific about what kinds of things one needs to be able to do, and they take account of the differences between the requirements of a city of New York, let's say, and a rural community.

For example, in a city we might say you need to be able to get hazardous material personnel to a place within a certain period of time. In a rural community, it might be a longer period of time. And because it is capabilities-based, it is designed to allow state and local governments to find different ways to achieve the capability as long as they get there.

Again, we are not completely through this process yet, but as we find this process, this is going to be a great tool for us, not only to give guidance but to give accountability.

If I can just take one minute to talk about our state and local partners. I want to be fair to them in this, because sometimes they do get an unfair rap. First of all, we have to distinguish between monies that are actually spent and money that is obligated. We all know as a common sense matter that when a grant is awarded what a state and local government is going to do is to go out and find the stuff they need that they are going to pay for. They do not obviously draw down on the money until they get the material. In fact, if they were to spend the money immediately before they got the product, we would be criticizing them for being wasteful and foolish.

So I think what is important to look at is what is obligated, and I think when I looked at it yesterday, I think approximately 96 percent of the funds that have been granted up through 2004 have been obligated, which I think is a very good number.

Second, even with respect to some of the stories about people in small communities buying HazMat trucks or things of that sort, obviously we are always going to find examples of waste or maybe misspent resources, but I also want to be fair. Sometimes what we have encouraged communities to do is to pool resources. We might say to a town, "Look, you buy something with the understanding that it is going to cover the whole region and it is going to be available to everybody."

And so when they do that, I think it is a little unfair when the press goes out and hunts them and says, "Well, here is a shining new HazMat truck in the town of X," without bothering to tell you that X covers really five counties, and that is what the deal is.

So we want to be disciplined with them. We think the preparedness documents are going to help them, but we also want to be fair to them.

Mr. REICHERT. Well, I am glad you touched on the regional issue. That was going to be my next question, and that is I think important.

Just one last comment. Having been a part of a large sheriff's office, the sheriff of the largest sheriff's office in the State of Washington and working with the COPS office and the grant process there, the COPS office Director, Carl Peed, has a great process in place for holding police departments and local agencies accountable. It might be worth taking a look at the process that they already have used for a number of years.

Mr. CHERTOFF. That is a good suggestion. I will do that.

Mr. REICHERT. Thank you.

Thank you, Mr. Chairman.

Chairman COX. The gentleman's time has expired.

The gentleman from Washington, Mr. Dicks?

Mr. DICKS. Thank you, Mr. Secretary. I want to welcome you and congratulate you on being confirmed by the Senate.

One of the issues I am concerned about is container security. A couple years ago there was a lockout of the long shoremen on the west coast of the United States, and within 5 days companies all over the country were yelling and screaming about not being able to get goods. And so I am worried that we have to take this container security issue seriously. I think in any risk analysis it has got to be up there near the top of our concerns.

Now, recently, 29 Chinese nationals were discovered at the Port of Los Angeles. These men lived inside a container filled with machinery parts for 2 weeks, and DHS officials had no idea that migrants were in the container until it arrived in the U.S. This is disturbing but not surprising given the millions of containers arriving in the United States without being screened or inspected.

This event occurred despite the fact that there is a 24-hour rule, a national targeting center to assess the risk of a container before it is shipped to the U.S. and the fact that we have Customs inspectors stations overseas as part of the CSI Program, including at the Port of Hong Kong where the container transited.

If 29 humans can be smuggled inside a container full of legitimate goods, can we be sure that our current strategy will prevent a dirty bomb or worse, a weapon of mass destruction from entering our country through one of our west coast ports or the Port of New York? And this is one area that—this and port security are areas of concern that I have in my region.

Mr. CHERTOFF. Well, actually, that story bothered me a lot when I read it too. And to make it worse, right before I was confirmed there was a similar story involving the Port of Los Angeles and so I asked a question about this. So needless to say, I was disturbed and it is something we are examining and also there are some elements of this that are classified that we can give a classified briefing on later.

Let me just make a couple points. My understanding is that the containers in question at the time that the migrants were discovered were still in the pre-inspection area of the port, meaning they

had not yet come to the part of the port where they would be inspected. So you should not assume that they would not have been inspected. They might well have been inspected before they came into the rest of the port and were then sent out in the other parts of the country. So that does not necessarily mean there is a failure of our screening process. It is kind of a geographic issue.

That does get to your second point, which is container security initiatives, can we do more of this overseas, and the answer is that is a great example of why we ought to pursue this initiative further. We do it in some ports, we do not do it in every port. Ideally, if we could do it in more ports, we could instead of finding the people in the pre-inspection area of whatever port we have in this country, we would find them in the port overseas.

Third, my instruction when I see something like this is, look, we have got to go and track back to the shipping company, the container company and find out what is the problem from their end. If it is a single failure of security and they can tighten it up, maybe we then address that.

Mr. DICKS. I think there is a role for technology here too. There has got to be some way, and we did this at the Port of Tacoma many years ago, where we would run these containers through a sensor on both sides and if there was something radiological or there was something of concern, it could detect it without having to inspect it.

The other thing I think we ought to do is what the military has been doing for quite a while now and that is having a sensor and a lock on these containers so that, one, we know where the containers are, and, two, we know what is in it and whether it has been tampered with.

Mr. CHERTOFF. Well, I think that is exactly right. We have been deploying radiological detectors in land ports and sea ports. That is a very important program. As we have indicated, I think today we have sent up an 872 notice indicating that we are going to stand up a domestic nuclear detection office which is going to be an interagency office, the function of which is going to be to move further on the technology for detecting radiological devices.

So absolutely correct. Again, I mean, part of our strategy has to be these non-invasive detection devices as well as other technological issues. We are going to look comprehensively at the issue of cargo. I think I mentioned that at the outset, but I wanted to tell you on this particular issue of the migrants, it annoyed me too. I have asked questions. I mean, in fairness, it was in the pre-inspection part of the port, but I think it is a cautionary tale to us about what we need to do here.

Mr. DICKS. Thank you, Mr. Chairman.

Chairman COX. The gentleman's time has expired.

Before I recognize Mr. Dent from Pennsylvania, the committee inquired of the Department about a week ago, and we are still waiting for an answer, whether in this human smuggling incident the shipping company was a C–TPAT member, and if so, whether it received a lower score and was not inspected for that reason. If you could get back to the committee, that would be very much appreciated.

Mr. CHERTOFF. We will.

Chairman COX. Mr. Dent?

Mr. DENT. Thanks, Mr. Chairman.

Good afternoon, Mr. Secretary. You were talking about threat vulnerability and consequence or criticality. How do you in the Department go about determining the relative importance of these critical infrastructures when you are looking at a nuclear plant versus a bridge or some kind of maybe telecommunications infrastructure? How do you go about that?

Mr. CHERTOFF. That is not the easiest thing in the world to do. We have used a variety of different analytical tools to look at the question of consequence. You obviously look at possible direct loss to human life. You look at economic consequences. What would blowing out a particular power grid do to the economy? You might look at other kinds of consequences that are indirect consequences in terms of illness or things of that sort.

To some degree, at some level, there is an element of kind of art rather than science in making the judgments, but I do think they are at least reasonable and I think analytically sound judgments that we make. And, again, because we are not just looking at consequences, we are also looking at vulnerability and threat, no one issue where there might be a disagreement is going to be necessarily dispositive. I mean, it is going to be a factor but there will be a number of factors. So that I think although someone could disagree at the margins, I think, in general, broadly speaking, it is a pretty sensible way of making a determination.

Mr. DENT. More specifically, if you have something that might be considered not very vulnerable but of high consequence, maybe like a nuclear plant, how do you make those determinations? I mean, when you have vulnerability is low but consequence is high, how do you balance those?

Mr. CHERTOFF. There are actually formulas that you can apply to that, and without getting into things again which I think are maybe somewhat classified, what I will say is I think it is intuitively obvious. Consequence is really a big driver in this in the sense that a cataclysmic consequence is one which you pay a lot of attention to even if there was comparatively low vulnerability. Whereas something, on the contrary, with very little consequence you do not care about. Like the footbridge down the road from my house I am not going to waste any time on even if it is very vulnerable. So consequence is a big part of that.

Mr. DENT. Thank you.

Chairman COX. The gentleman's time has expired.

The gentlelady from California, Ms. Harman?

Ms. HARMAN. Thank you, Mr. Chairman.

And welcome, Mr. Secretary. Count me as a big fan, because I think that this notion you have of getting your hands around the whole problem and attacking it with a strategy is exactly right. We will never succeed with the squeaky wheel theory of homeland security.

Let me make a couple points. First of all, we are all aware of substantial turnover at your department. In that regard, it pleases me to see Pam Turner behind you. She is excellent. I hope you are staying, Pam. Good. She has been excellent.

As you may know, I served on the Commission on Terrorism, which predicted in 2000 a major attack on U.S. soil. I actually hosted an event in my district in August of 2001 with the question, are we ready? And, clearly in September of 2001, we were not. And I would say we are still not ready. The key to getting ready is to have a strategy.

The goal of the Homeland Security Department was not to rearrange the deck chairs but to create one deck, one common, national integrated strategy, and I think, if I am hearing you right, that your focus on intelligence policy and operations is directed precisely to that; am I right?

Mr. CHERTOFF. That is correct, yes.

Ms. HARMAN. And I just applaud you for doing that. We cannot protect everything equally, and we should not, but this risk analysis applied to everything in some organized way will lead us to protect what we must, and, boy, must we protect many things like our ports better than we are.

I represent the communities around the Port of Los Angeles. I hope you will visit them soon. There have been two incidents, as you point out, where human beings have exited containers at the port. In one case, I know, the bill of lading said the contents of that container were clothing, and it missed all the screens and just an astute crane operator happened to notice people getting out of the container and called the police. And, fortunately, we had eyes and ears at the port and maybe or maybe not they would have been picked up. They were human smuggling rings, they were not terrorist cells, but there were more people in each container than attacked us on 9/11. So it is a very, very serious problem.

I want to ask you about two things. One of them is not intelligence. I think you have the right fix on intelligence, and if I can be helpful, please call on me. But there are two big problems that I do not think have been mentioned today, and I just hope they are on your screen. One is interoperable communications. Congressman Curt Weldon and I have for years been trying to require that Congress keep its promise to make some analog spectrum available for interoperable communications by the end of next year. That is a tough sell.

The broadcasting industry opposes us, but, boy, do we need that. Just in Los Angeles County alone, the largest county on the planet, all we can manage at the moment are bridging technologies, trucks that carry frequency integrators on them so that you can plug in at the site. That is just not near good enough, not for LA and not for the country. So please put that on your screen.

The other one is our broken threat warning system. I think the color-coded approach was a good try but I joked at one point and Tom Ridge did find it funny that he sounded more like an interior decorator talking about what we could do with yellow than he sounded like someone who earned the confidence of the country to talk to people and first responders about threats. So I hope you will figure this out.

That is a primary mission of yours, your Department. That is not resident in any other department, and I do not think the DNI is going to be the threat warner. So I would urge you, as might light turns to red, to get on top of that as quickly as possible.

Mr. CHERTOFF. Well, speaking of interior decorating, as you mentioned it, I was trying to figure out what the heck you could do with orange in interior decorating.

[Laughter.]

I think both those are serious issues. Both of them are things which we do have as part of our second-stage review, and I think we have to—particularly with respect to the warning system, there are a lot of things that are geared to that system. We have to figure out whether we have come to a point where we need to make some adjustments with it. We have now a little bit more experience about what is useful and what is not useful, and it is a good time to take a second look.

Ms. HARMAN. Thank you.

Thank you, Mr. Chairman.

Chairman COX. The gentlelady's time has expired.

The gentleman from Pennsylvania, Mr. Weldon?

Mr. WELDON. Thank you, Mr. Chairman.

Thank you, Mr. Secretary, for being here.

Mr. Secretary, if there is some pessimism coming out of this hearing today, you have to understand the mindset that comes from the members on the committee. I agree with you totally on the intelligence aspect of preparing for protection of our homeland, but it was the Congress back as far as the summer of 1999 that proposed creating a national collaborative center, we called it the NOAH, National Operations Analysis Hub, which would have brought together all 33 classified systems managed by 16 agencies.

In November of 1999, the FBI and the CIA said, "We do not need that." It took us until January of 2003 in the State of the Union speech for the President to announce the TTIC. The TTIC is exactly what the Congress proposed 4 years earlier.

The Congress has cried since 1995 to deal with what the gentlelady referred to and that is interoperable communications. That is when the Public Safety Wireless Advisory Committee came out and said, "We have to set aside 20 megahertz for public safety." This is 2005. We still have not done that. And all across the country when you meet with first responders, as you did last week, and we thank you for coming to the dinner, their number one problem is they cannot talk to each other.

When I went to the Trade Center in 1993 and talked to the fire commissioner, he said the same thing that the fire commissioner said in 2001, "We cannot talk to each other." So the frustration here is that the agencies just still are not getting it, and we talked to Secretary Ridge about this repeatedly.

The issue of technology transfer, I happen to serve as vice chairman of both this committee and the Armed Services Committee. It is frustrating to me to see us spend billions of dollars on technology that the first responder ought to have but for some reason we cannot get it to them. When I was at Loma Prieta Earthquake walking with the freeway with the fire chiefs of Oakland and San Francisco, they were looking for people in the freeway with dogs. I said, "Why aren't you using thermal imagers?" They said, "What are thermal imagers?" That was 12 years ago.

The Navy had produced that technology 5 or 10 years before that. We do not use the technology well, and if you could use and

perhaps establish an enhanced effort to integrate the technology transfer between DOD as opposed to reinventing that. We are spending a lot of money on UAVs. UAVs are going to become very important for homeland security as well as other transmission and other related technology.

In terms of private interface, I would hope that the agency has done or would do an assessment of all the stakeholders. I spoke this morning to ASIS. ASIS, as you know, has 33,000 members. It is the largest private sector representation of the private security leaders of our Fortune 1000 companies. They do not have a direct relationship yet to the agency. I asked them if they would. They said, "Absolutely."

And, Mr. Chairman, they have offered to establish a consulting role with this committee to provide the ongoing interface with the private sector.

And when you look at threats like—in my opinion, the number one threat to our security from the broad standpoint, which is not being addressed, is the threat of an EMP laydown, a terrorist country getting the capability of a low-yield nuclear weapon, launching it over our shore, detonating it, and then you basically fry all the electronic components and you dumb-down the entire country. We are not prepared for that.

In fact, up until 2 years ago when Congress mandated the establishment of the EMP Commission, the military did not want to hear about it. That is a homeland security threat that we have got to interface with the private sector on. So I hope you would see that as a priority for you.

And, finally, you referred to the people that are doing the first responding, and I appreciate your sensitivity to them, because, as you know, 85 percent of them on the fire and EMS side are volunteers, and many of them are not part of government. They are parts of 501(c)(3)s; they operate on their own. They have bought with their own money, through chicken dinners and tag days, to buy their equipment. We need to be sensitive to keep that base in place, because if the federal government ever tried to replace that, it would bankrupt the nation.

And simple things like the—and you just came from the Justice Department. The Justice Department ruling that says that a firefighter under 18 is really not a firefighter. The federal government has never defined what a firefighter is, but all of a sudden after 25 years of the Public Safety Officer Death Benefit Program, one person in DOJ decides that a 17-year-old firefighter is not a volunteer firefighter. Well, that is outrageous. The states determine criteria in line with their local departments.

And what that is having is a terrible effect across the country where the 32,000 fire departments have got to recruit new people. And so we have got to address those kinds of concerns to keep those people volunteering.

And I would ask you to be sensitive, as you were when you came to the dinner, and gave an outstanding speech, by the way, that was very positively received by all the firefighters in attendance, to make sure that we are nurturing that group of leaders that will in fact be there to protect the nation. Thank you.

Mr. CHERTOFF. Well, taking the last first, because on a personal level in the communities I lived in, most of them relied on volunteer firefighters, and I ate my share of chicken dinners and participated in that process, and I think they are the backbone of our response in many, if not most, communities, and we do owe them respect and also we need to attend to their needs and their capabilities.

I think all the points you make are important points. I know with respect to intelligence sharing, which has been a long time coming, the President is very committed to making sure that we are sharing and we are operating off the same page. There is no mistake about that. And he welcomed the most recent report by Judge Silberman and Senator Robb's commission and we have a new DNI coming out. So I think we really have—the table is set for completing this process of integration.

Likewise, I agree, I think that we need to work more closely with the Department of Defense on getting the benefit of some of those technologies, although I would put in a plug for the dogs. You know, when all is said and done, the dogs are actually very good at a lot of the stuff that they do, including the bomb detection and the USAR teams.

And, if I can just, again, be allowed a little moment of sentimentality, there were stories in 9/11 in the area of the crater of dogs that almost broke down because they could not find people that were in there that they were trying to find. So I do not want to diminish their utility as well.

Mr. WELDON. As a dog lover, I agree.

Chairman COX. The gentleman's time has expired.

The gentleman from Oregon, Mr. DeFazio?

Mr. DEFAZIO. Thank you, Mr. Chairman and Mr. Secretary.

I think that you have got a tough job in ascertaining on a risk-based system where to allocate resources, but I think we would all agree there is a continuing high interest with high-risk to aviation. So I would like to just focus on that for a couple of minutes.

Just want to kind of get your vision. As you know, Admiral Stone, the third Director of the TSA, is departing in June, and I see there are some ongoing problems at the agency, some of which I think he was cognizant of and at least as he represented in hearings, trying to deal with.

One is the overcentralization, bureaucratization of the agency, which deprives the local security directors of the flexibility they need to hire, fire, train, split shifts, do things like that, which creates certain frustrations with the airports and meeting the needs of passengers. So he was very aware of that, kept telling us he was going to deal with, it never quite got done, and I would like to hear what we hope to do there.

Secondly, he certainly was a good soldier and did not?well, let's put it this way: He was aware of, as is everybody, the fact that we are not investing enough in the technology, as we heard from the previous gentleman. We have airports lined up who want to go to inline systems, waiting for federal grants that are not available, which is in part a failure of the Congress but also the administration. We have not deployed technology that exists for what I consider to be the highest threat, which is bombs. I mean, the Russian

incident is pretty clear and maybe the last maybe wakeup call before something happens.

And I would just like to know what your vision is. And I particularly have a concern that Michael Jackson, with whom I have dealt with over the years with his previous iterations with the government, who went to the private sector and just before he came back he gave what has been described to me as a extraordinary speech to the Homeland Security Institute saying that there was no way to do aviation security except privatize, and I would like to know if you intend to push, because very few airports have applied to go back to privatized systems but they do want those problems that I described fixed with the federal system.

Mr. CHERTOFF. Well, we do have, as you know, some pilot programs with respect to privatizing, and that is certainly an option which the current system lays open for them. And maybe that in terms of our doing things we ought to do under the Safety Act, we have not been as efficient as we should be, and that is an issue we are going to look at.

I think that there is no question that a key part of the issue of dealing with aviation security is technology. The issue of explosives is obviously of great concern. Now, that is a little different than the 9/11 issue, which involved people turning aircraft into weapons, but it is of course in itself a serious issue. And there are technologies out there that we have to start taking a serious look at in terms of whether they can be deployed and how they would operate, and that includes backscatter, it includes puffing, and some of these things, you know, people have arguments about whether they are intrusive or not, and we have to think about how to deal with those arguments in ways that take account of legitimate concerns about privacy.

But you are quite right that ultimately our best tool and our advantage in this kind of asymmetrical warfare with terrorists is technology. And I think we need to make some decisions about getting new generations of technology out. There also may be in terms of financing this kind of new technology some tools we can use in terms of alternative ways of financing that would get it out there more rapidly than in the conventional method, and we have got to look at that as well.

Mr. DEFAZIO. I would be very interested to follow up on that because Mike and I had talked about that in the past but did not get much response from the administration in terms of some ways to fund these things up front and get them into the field.

Mr. CHERTOFF. We are thinking about those things, and we are exploring some of those as possibilities, and we will be interested in engaging on that subject.

Mr. DEFAZIO. And one other for all your portable memory units who are there behind you writing great notes, a number of firms have been certified under the Safety Act for aviation security. As I read the act, it is basically they carry a liability insurance and that is the limit of their liability. And I have been trying to find out what the liability limits have been set at, particularly for screening companies since we saw significant problems with screening companies pre–9/11. So if I could that get that information?

Mr. CHERTOFF. We will get that.

Mr. DEFAZIO. Thank you.

Thank you, Mr. Chairman.

Chairman COX. The gentleman's time has expired.

The gentleman from Connecticut, Mr. Shays?

Mr. SHAYS. Thank you, Mr. Secretary. I will join with the heartfelt congratulations and prayers as well. You have an awesome responsibility and a great opportunity.

I wanted to just say to my colleague on the other side of the aisle when she talked about being on the commission, there were three commissions, the Bremer Commission, Hart-Rudman Commission, Gilmore Commission. They all said we need an assessment of the terrorist threat—this is before 2001. We needed a strategy to combat that. We needed to assess a threat, a strategy to deal with the threat, and we needed to reorganize our government to implement the strategy. And all three basically concurred on that except the Hart-Rudman Commission went the furthest and said we needed a Department of Homeland Security and that is what we have.

We established the Department of Homeland Security, frankly, though, before we really established the strategy and really had an assessment of the threat. If I were to ask you now what is our strategy, what would it be?

Mr. CHERTOFF. I would say the first part of the strategy is not part of what we do in this Department but what the President has done in taking that word of the enemy. I have to say I continue to believe that the first layer of defense is a good offense, and that means as we eliminate camps, we eliminate labs that the enemy has, we kill or capture them, we put them in a position where they spend a lot of time worrying about their own safety rather than training and recruiting. That is the first piece of a major strategy.

A second piece of the strategy is working globally with our allies all over the world in making the world inhospitable to terrorists. And that is, again, a second piece.

And then of course there is a piece that begins at our own borders, which is complementary and part of the layering approach, and that involves having increased capabilities, both at our ports of entry and between our ports of entry to protect ourselves from bad people and bad stuff getting into the country, our capability inside the country to protect our transportation and our infrastructure, our special effort that we are undertaking now with respect to nuclear detection capability, which I think is an area where we need almost a mini Manhattan Project in terms of technology as well as deployment.

I think these are all parts of a comprehensive strategy, the idea being that we are going to do our best at every level to put them on the defensive, take them off the boards, prevent them from coming in, prevent them from shipping their stuff in, protecting our infrastructure and transportation if they do get in, and then if worst comes to worst, and we have to prepare for this too, being able to respond and mitigate the harm.

Mr. SHAYS. The last answers please me the most, because it seems to me that the Cold War is over, the world is a more dangerous place, that the Cold War strategy of contain, react, and mutually assured destruction went out the window, and that has to

be detect, prevent and it may have to be preemptive and it may have to frankly be unilateral. And it seems to me that that is what the mainframe work is, and then what you said about the strategy taking the word of the enemy, working globally with our allies and so on are parts of that.

I am concerned that we are not doing enough to detect and prevent, and I realize that is part of your responsibility. With the time I have left, how can we justify for a minute giving resources to deal with the reactive part of the dealing with the consequence of an attack? How can we for a second justify giving to a community resources that they do not need as much as, say, New York City or D.C. or even where the Hoover Dam is because, clearly, they need to have some. How can we justify that?

Mr. CHERTOFF. Well, I mean, I think we need to be—and I think I have said this before—we need to be driven by risk and that means that the resources have to go where they will do the most good to prevent, protect and respond based on consequence and vulnerability and threat. And that is where we have to put our resources.

We do not have money to waste, we do not have effort to waste. We have to be realistic about the fact that we have a menu of a large number of different things we have to protect. Some of them are—there are obviously people we have to protect directly, there is infrastructure, there are transportation nodes. There is no cookie cutter answer to this, but I completely agree with you that we cannot afford to waste money by just making everybody feel good like they got a little piece of something. It has got to be driven by essential priorities about what we have to worry about the most.

Mr. SHAYS. I just wanted to hear you say it again.

Thank you.

Chairman COX. The gentleman's time has expired.

The gentlelady from the District of Columbia, Ms. Holmes Norton.

Ms. NORTON. Thank you very much, Mr. Chairman.

And thank you very much for being with us and for your useful testimony. I appreciate the distinction you made between obligation and spending.

I would like to ask a question about your own definition of a risk-based approach. As I see it, the two top challenges you face are putting Humpty Dumpty together, not again but for the first time. It is very difficult. These are melding together agencies that nobody ever meant to be together. Were it not for 9/11, they would not be together. They still have domestic responsibilities that have nothing to do with you. That is real hard.

The second one has been of great concern to this committee, and that is developing and applying a risk-base analysis. I looked at page 10 of your testimony, and I was rather much attracted by the way you sent at the notion of "a trio of threat, vulnerability and consequence." I kind of like the notion of giving your example of a two-lane bridge down a street from your own house. Hate to see that dam but comparing it to an attack on a major multilane bridge, this is a touch approach, but what it seems to me does is give one an objective standard. Until we get an objective standard,

we are going to have great problems making jurisdiction as vast and diverse as those represented at this table.

Understand why A got more money than B and that this is not another of those population-based programs.

Let me try to apply the notion, the trio notion in your testimony to different rather disparate examples since I understand this that way.

One has to do with rail security. I have had a bill for rail security. Very, very concerned. You come from a part of the country where you ought to be even more concerned than I am, particularly after Madrid. I do not know what the latest figures are. It looks like 141 million in the 2005 budget. After 9/11, of course, we pumped money into aviation we better had. What I really am trying to get at is whether we are using any risk-based approach, either to budgeting or to other things.

Compared to air security, I mean it pales beside the number of people to get onto subways, buses, light rail every day of the week, and I have been flabbergasted by how far behind rail is. It does not hardly register here, I am not even talking just money. On the screen for approach as far as I have been able to tell, I would like to ask about your approach, threat, vulnerability and consequences applied, to that way of doing budgeting. That is number one.

Then let me take a specific example of whether that approach even works in the everyday world. We have got now two bills by the Chairs of two committees to bring aviation back to the nation's capital. Both chairman have gone at TSA. We even had a briefing, it was embarrassing, far from a risk-based analysis.

This was about a couple of years ago, Judge Chertoff. It was a kind of doomsday approach involving the monument and the Capitol. It did not have any analytical sense of risk versus cost and commerce and convenience and the rest of the kind of things you would expect a market society to do by instincts almost with more like a science fiction movie.

Here now you have what I regard as an override of the Department of Homeland Security, because TSA has taken no action. Both of these Chairs now are going to have committees. They both have introduced bills that no longer call for a plan. In the FAA bill, there was a section that said TSA had to present a plan. There having been no plan for 18 months, now they call for opening general aviation.

They do not have any risk-based analysis, they just know that something is wrong with the Department of Homeland Security if they make it even look like they do not know how to protect the nation's capital. Understand general aviation was up and running in New York City within days, helicopter service, all the rest of it, where the great debacle occurred.

I would just like you to take a stab at your own approach to risk-based analysis, threat vulnerability and consequence and apply it to the two examples that I have just presented.

Mr. CHERTOFF. Well, I think that they do apply, and let me take the second one first. We are working, as we speak, on this issue of general aviation, because I think actually it demonstrates two facets to this risk management concept. One is we have to really think hard about what the consequence would be if someone mis-

used a general aviation plane in Washington, how vulnerable we are at this point given what has been put in place and how real the threat is. But, you know, there is another piece to risk management which I think the chairman alluded to earlier which is there is also a cost benefit. Because I can completely eliminate risk by having no air travel and there will never be a risk of an aviation problem.

And that is clearly not the right answer. And I know that there was an understandable tendency on the part of some people right after 9/11 to take the attitude that protection overrides everything, but I think we understand now that this has got to be a long-term strategy, we have got to be structured for a long-term war against terror, and that means we cannot destroy our way of life in order to save it.

So whenever we make a risk analysis, we have to also make a cost-benefit analysis, and we have to say how much risk are we prepared to tolerate, or should we tolerate, in order to make sure we have a free flow of commerce, and that is an approach we are taking across the board.

So that I think in the area of general aviation, we are working hard now with general aviation to talk about what are precautions to put in place to have a plan so that we neither have nothing nor bar the door, everything goes like 9/11 never happened. Neither of those approaches make sense. What makes sense is an approach that opens up the possibility of general aviation but in a way that guarantees a reasonable amount of security bearing in mind consequence, vulnerability, and threat. So I think it very much does apply.

Likewise, with rail, we are obviously looking at the issue of rail, and we have to consider the consequences of a rail incident, bearing in mind that just a couple months ago in California there was a derailment. That was a bad thing, but it was not a catastrophic thing.

Ms. NORTON. And South Carolina?

Mr. CHERTOFF. And South Carolina too. And then we have to build things like a response capability, a security capability in terms of sensors on the tracks, things that might anticipate someone driving a car on the tracks. So, again, that is something we are working on. We are using exactly the approach I am talking about, and I think it is valid across the board and one which I think will give results that may not satisfy everybody but will at least be reasonable.

Ms. NORTON. Thank you, Mr. Chairman. I appreciate the responses. I am going to be looking—you are new at the Department—to see whether or not in these two areas I see this approach being carried out.

Thank you very much.

Chairman COX. The gentlelady's time has expired.

The gentleman from Georgia, Mr. Linder?

Mr. LINDER. Thank you, Mr. Chairman.

Mr. Secretary, welcome. Nice to have you here. I just had an honest question I ask people all the time: Do you ever think another airplane will fly into a building?

Mr. CHERTOFF. Do I think it will? I think it is certainly possible.

Mr. LINDER. Do you think the passengers would tolerate that?

Mr. CHERTOFF. You know, I think it would depend on a lot of circumstances. Are we talking about a large commercial airline, are we talking about a private airplane? I think the chances are much less now, but I cannot rule it out.

The one thing I can tell you is that as we take each step to secure the airlines from that kind of a possibility, we have reduced the chance measurably. I do not know that we are completely there yet, and I certainly would not suggest reversing direction and tempting fate.

Mr. LINDER. I just cannot imagine a flight full of passengers on a commercial airliner, allowing some people to take it over without going after them themselves, because they know what is going to happen. They know what it is all about, and they would rather risk dying in an effort to fight than going into a building. And we spend $5.5 billion looking for fingernail clippers. It seems that money could be spent more wisely worrying about, as you said, there is a difference between bad things and catastrophic things.

Mr. CHERTOFF. I am not sure that—I certainly think that toenail clippers are not the thing we are worried about, and I do agree what I think someone said earlier. I think we need to be concerned about explosives, but I do not think that I would draw the conclusion because I would rely on the passengers that we could stop searching people for knives or guns. I mean I think that we want to continue to keep those kinds of things off planes.

Mr. LINDER. It would be a bad thing if an airliner went down and 200 people died, but it would not be catastrophic. It would be catastrophic if we could find a way to use some of that money to worry about the intelligence for the bigger things like the nuclear bombs that are radioactive or biological threats.

And I worry about your department that you inherited. I appreciate your 60-day review, but I worry that you get so bogged down in a huge bureaucracy doing really some stupid things that you do not have the time to think about the big things.

Mr. CHERTOFF. Well, actually, I worry about that too, and I do not want to keep invoking the review, but I do want to tell you that almost every morning I get kind of a briefing as to what is going on from an intelligence standpoint, and I sit around with the very top people in the Department, and we talk about exactly the kinds of things you are talking about. We talk about whether we are spending too much time worrying about the kind of risk that is comparatively less of a consequence that while serious is not catastrophic and not enough time worrying about other things. And we really try to dig into this.

One of the reasons I do want to see us have a more powerful policy capability is precisely to be able to start to think about these things department-wide, to avoid the issue I think you are pointing at, which is every component focused on its world and its vision without someone standing back and looking at the whole menu. And that is really what we have to do, we have to look at the whole map.

Mr. LINDER. I view your challenge as becoming a very sophisticated intelligence organization so that when a threat arrives in some location, it may be in Reno or it may be in Hahira, Georgia,

that you can alarm those folks, let them know ahead of time the risk, and it is probably not going to be the same risk you might face in Phoenix. And I do not know how much percentage of your budget is spent on intelligence, do you have an idea on that?

Mr. CHERTOFF. I cannot tell you—I mean, partly I cannot tell you because there are pieces of intelligence that are placed within a lot of different—.

Mr. LINDER. Rob Simmons tells me it is 2.5 percent.

Mr. CHERTOFF. I am not in a position to dispute that. I know it is parceled out in a lot of different areas, frankly, and one of our challenges is to unify it and fuse it so we get the benefit of all of it.

Mr. LINDER. The biggest threat that I am worried about is biological. How much of a component in your intelligence community that you have is experts in bio threats?

Mr. CHERTOFF. Well, I mean, we deal with biological threats in a number of different ways. In terms of intelligence, of course, we get not only whatever intelligence we have within our department, but we get what the intelligence community generates.

But there is a separate piece of this which has to do with preparation and preparedness and response. We have in our Science and Technology Directorate scientists and medical people who have expertise. We largely also draw on the expertise of HHS and the Centers for Disease Control in terms of understanding the different kinds of biological agents there are. We have a Bio Watch Program in a large number of cities in which we have very sensitive sensing devices that do monitor for various kinds of biological agents.

And then we also—and I think this is an important piece of this entire approach—is we focus on having a clear set of plans for what to do in case of a biological incident. And that requires us to understand the way the agent works, to have access to the appropriate antidote and a plan for deploying that antidote and a sense of how to do it in a way that is most efficient in terms of getting it out and preventing the spread of the agent.

Mr. LINDER. Just one last question, Mr. Secretary: How did the plan work when the Pentagon withheld information for 5 days on their anthrax threat?

Mr. CHERTOFF. Well, you know, we have done, I guess what we call, an after-action report. I think the state and locals have too. We have talked to all the agencies involved. The Defense Department has changed its protocols. Thankfully, it was not really anthrax, but it was for me, actually, a very useful lesson in terms of seeing where we had a deficiency in our response capability and where we could correct it.

You know, I think where I want to go beyond that is I think we need to have on the shelf, and I think we are in the process of developing this, we have a lot of good product, an ability with respect to any one of the likely agents to understand how the agent works and have an ability to think about how to respond, because the response is different depending on the agent. It depends on how contagious it is, it depends on how long it persists in the environment.

So we jumped on studying this right away. We have embodied some immediate lessons that we have now changed, but I think we are building on that incident as a way of now going all around the

federal government and making sure that everybody has got their protocols and their plans in place for dealing with this kind of situation.

Mr. LINDER. Thank you, Mr. Secretary.

Chairman COX. The gentleman's time has expired.

Mr. Pascrell from New Jersey?

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Secretary, you have done a lot of good things in New Jersey concerning homeland security, and I would say that under Mr. Casperson I would put us as a model in terms of bringing all the entities together in New Jersey.

But that entity cannot do its job unless we share intelligence with that entity, and this is not happening—this is not happening.

I think the 9/11 Commission, Mr. Secretary, got it right, and I think you have it right. I will tell you why I think that. You have a philosophy which you bring to the job. I never even heard that word before in the last 2.5. years. It is not a scary word to me. You bring something to the table and not just reacting and responding. I think this is important, extremely important.

And while you say in your opening statement that you cannot guarantee, realizing that we can make no guarantees, we cannot guarantee but we can minimize our vulnerabilities. We need to be primarily dependent on intelligence, and you bring this up. Of course, that can mean a lot of things to a lot of people, and I want to get into that in a second.

So before port security, aviation security, train security, border security, all the way down the line, philosophy and strategy is very important to what we do. And so we have seen a lot of finger pointing over the last 2 years at the CIA and the FBI. Now, we know they have made mistakes but they have been driven, if you read the 9/11 report, if all of us have read it, you know that that is driven by philosophy and strategy. And if you are not—I am not saying you personally—if you are not willing to accept that, then nobody is ever held accountable. And that is the situation that we had.

That is why looking back over that 9/11 Commission report no one has been held accountable. Take a look. Unless I missed it in the news. So we can line up al the mistakes and we can point fingers at the FBI and the CIA but those entities run on the basis of where the President, be it Clinton, Bush or whomever, want to go. And let's not mistake anything about that.

So intelligence can mean a lot of things if it is supported by a strategy, if it is supported by a philosophy and we hone in on an enemy. Now, you say who is the enemy, take the war to the enemy. The end result of this is saving a lot of money, as you say, because we want to know where to spend that money. Say, take the war to the enemy. The problem is we do not know who the enemy is. We are fighting non-state terror. If it is a state, we know it is easier to get your hands around it. We are not fighting Islam; we are fighting extreme fundamentalist, Islamic, radical terrorists. That is who we are fighting.

We have not made that distinction in our policy or in our philosophy. And that is why some members of this body support increasing the profiling. And you know exactly what I am talking about in getting at the enemy.

Now, I believe we are at war. I believe that from the bottom of my heart and that we are at war with terrorists. But we need to preserve the freedoms, and you more than anything else know that and you have struck that balance in your entire life. I say that—I am not patronizing you because I say it because I mean it.

What is your reaction and response to the issue of profiling, keeping in mind Chapter 12 of the 9/11 report about who we should be reaching out to?

Mr. CHERTOFF. Well, let me say this: First of all, before I get to that issue, I just want to make it—I am certain to you about the fact that the President and everybody who works for him is committed to the idea of intelligence sharing, and I know that the President was committed to that before. Judge Silberman and Senator Robb presented the report, and I know that only reinforced it, and that has been a very clear mandate.

I agree with you, Congressman, that we have to be very careful about who we are fighting. We are fighting radical Jihadists. The vast majority of people who follow the religion of Islam are peaceful members of this community and this country, are every bit as good Americans as everybody else. And we make a grave mistake if we allow the actions of Jihadists to spill over into everybody who is practicing Islam—many more than we would do so if we were to identify the acts of Timothy McVeigh with people who are Christian or pick someone Jewish who does something wrong.

So we have to distinguish between—I am deadset against religious profiling for the following at least two reasons—many reasons. First of all, it is counterproductive. It is counterproductive, because we do need to reach out to—we will not do well if the world walks away with the impression that we are fighting a war against religion, because we will do very poorly in the world and we will do very poorly with the hearts and minds we need to win.

Second, I can guarantee you that if we telegraph that we are going to look at a particular type of person when they come into the country, that Al Qa'ida will find somebody who does not look like that person to come in and carry a bomb. So we would be making a big mistake if we were so obvious and so kind of unsophisticated in what we do.

And, third, obviously it strikes the fabric of our own country and what we believe in terms of our Constitution and our civil liberties to single out people based upon their religion. People who have consciously adopted an ideology of hate and war we should pursue without quarter. But those who are peaceful, religion should not enter into it.

Mr. PASCRELL. Thank you very much, Mr. Secretary.

Mr. LUNGREN. [Presiding.] Thank you, Mr. Secretary. Obviously, I am not Mr. Cox even though it says that. My name is Dan Lungren. I am a Californian.

As Secretary Rumsfeld said, I am a retread. I like to think I am a returning congressional veteran. That sounds better. I came back here because of 9/11. I know you have taken this commitment because of 9/11.

I guess my first question is because of the need for certainty and continuity, is it your intention, if you continue to have the con-

fidence of the President, to stay for the rest of his term in this position?

Mr. CHERTOFF. As long as the President wants me to serve, I will serve.

Mr. LUNGREN. Secondly, with respect to risk assessment, you know, we can all talk about the failure to complete that task to this point by the Department, but the Congress bears a great deal of that burden, as well. My observation is we have not made the transformation after 9/11 by recognizing that we need to reorganize ourselves and reprioritize with respect to that.

I would just ask you very simply, you have not been described to me as a wallflower in any of your previous experiences. I hope that you will—if you think those of us in Congress, in terms of the legislation we are presenting or the pressure that we put on your department do ignore risk assessment, you will feel emboldened to tell us that and to loudly tell us that.

Mr. CHERTOFF. Well, I will, Congressman. I think I have already been pretty blunt, and hopefully, polite, but blunt in saying, you know, that I understand this approach of being risk-driven will disappoint some people. What I can hopefully hold out is that we will at least present an analytic approach that people will understand and respect, even if they disagree with it.

But you know, this is not an approach that says, "Let us give everybody a little something to make them happy." It is an approach designed to maximize the benefit of what we do to avoid the greatest risk.

Mr. LUNGREN. As important as it is to get that right, it is also important that we be able to articulate it in such a way that members of Congress can go home to their districts and explain why they may not be getting the money and why it is necessary, why we are national legislators. So not only in terms of the substance, but in terms of the ability to articulate, and frankly, we need you in the bully pulpit doing that. And I hope you will.

Let me turn to the question of the Safety Act, because it appears to me that the effort of the Congress was to try and stimulate the development of technology transfer that you talked about in your testimony by setting up a mechanism by which we could have some limited protection in terms of liability.

I come from the legal arena, as do you. We know we have had legal reform here in the Congress, and it has been somewhat controversial. Here you have something where the Congress basically came together and said it is important for us to do that. And yet, if you look objectively at the results of that, I think you would have to be—at least I am—disappointed in the number of applications for that kind of a review and the assessment completed by your department.

It seems to me, if we are to look at setting priorities, and you have talked about the mechanism of the transfer of technology to aid us in that, that that would be one of the top priorities of your department. And yet, as I look at what has happened thus far—maybe it is just because of start-up difficulties, but I do not see that as a priority. Would you please comment on that?

Mr. CHERTOFF. Well, we did, I think, recently change the regulations to try to streamline them, because I think there was a sense

that the original set of regulations may be too onerous. And that will hopefully help, in terms of encouraging people to apply.

But I did—you know, I had the same observation when I came onto the job that it seemed we were not getting as much out of that program as one would have hoped. And so, you know, that is an issue which we are currently looking at as part of this review. I do not know whether the regulatory change is enough or whether we are being unduly nitpicky in terms of where we are requesting.

But I do think that is a powerful tool to harness the private sector, in terms of its ingenuity. And I think if we do not make full use of it, we are really shortchanging ourselves.

Mr. LUNGREN. And let me ask you this: Will there be a prioritization of the type of applications that are made? That is, if you make a risk assessment, and you determine that there are specific areas in which we really need some assistance, would it be your thought that the department ought to, in a sense, try and put that on the streamlined highway, maybe over something else that might be important technically but, in terms of your department's review of the assessment, would not fit the need as readily?

Mr. CHERTOFF. Well, I would hope we can actually get this to the point that it is all pretty streamlined. I think we do want to encourage certain kinds of technology. And there are some other tools that even may be more powerful than the Safety Act, which, of course, is really a liability-capping act.

But there are things—you know, we have a version of DARPA called HSARPA. And you know, DARPA was a great tool for the Defense Department. I want to make sure we are using that tool and also that we are—a part of what we need to do is get our procurement system more unified and then connect it up with our research, so we really have kind of a powerful economic engine to drive important technological advances.

Mr. LUNGREN. Thank you very much, Mr. Secretary. My time is expired.

The gentlelady from the Virgin Islands, Ms. Christensen?

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

And welcome, Mr. Secretary. I am encouraged like the others by your statements, your brief opening remarks, and your responses, and especially, of course, knowing that you have come from the Third Circuit.

Mr. CHERTOFF. We are the Virgin Islands—not initiated.

Mrs. CHRISTENSEN. Mr. Secretary, as you work to change and improve the working culture at the department, I wanted to add another challenge, a basic one, and that is that the department respect this committee's work and responsibility and be fully forthcoming with the information that we need to work with you, and to give you the support you need, and to fulfill the tasks for which we are charged. That has not always been the case.

I want to ask a question, again, around port security. The OIG report on Port Security Grants generated a national debate within the maritime community and how grant funding ought to be distributed. Some say funding should be distributed solely on risk. Others feel that the Maritime Transportation Security Act is a federal mandate as is on all ports, and therefore all ports should receive security funding regardless of risk.

Some of the op-eds that followed criticized the fact the ports in the Virgin Islands specifically received grant funding because they believe that these ports do have the same risk compared to the larger ports, such as New York and Los Angeles. As a member of the committee, I do that more financing is needed at all of our country's ports, but I believe that we ignore the smaller ports at our peril, as well.

And while ports in the Virgin Islands may not have as many containers moving through as New York or some of the other ports, our ports are host to cruise ships, passengers, anywhere from—very rarely at 5,000, and maybe as many as 12,000 on any given day, second only to Miami.

So if you feel that homeland security should be risk-based, what would be your definition of risk? Because in a maritime environment, I feel it has to go beyond just looking at containers.

Mr. CHERTOFF. Well, I do not think risk is only containers. I think risk is—but I think it is at the end of the day consequence, vulnerability and threat. And as I said, I mean, that will not necessarily result in everybody getting something. But I think to put it in perspective, it is important to know that our entire effort in port security involves a lot of different things.

And I think there was some confusion about the role that the port grants play, in terms of container security. The port grants are designed—or were designed, since they are now rolled into the total infrastructure program, they were designed to deal with the actual security of the port itself.

But the security of containers, which is a cargo function, is addressed in a lot of additional ways. It is addressed through customs and border protection, and the screening and inspection, and the security initiative. Coast Guard plays a direct role. There are, depending on where you are, there may be state grants or UASI grants that are available also for ports.

So unfortunately, when you isolate a single program, particularly one that is directed at a particular function, you are not, frankly, capturing all the resources that are brought to bear. And I think the thing I would ask when people evaluate how we do, is they recognize that sometimes we may accomplish a result using a different set of tools.

And again, you know, we are ultimately capability-and mission-oriented. We want to get the job done. We want to keep the bad stuff out. If we do it by having Coast Guard do something as opposed to giving a port security grant, if we get to the right result, that is good. And that is the kind of philosophy we are going to take.

Mrs. CHRISTENSEN. Well, I appreciate that, and that means that perhaps our Coast Guard will be getting some more funding and more assets, as well. Because I appreciate your approach that brings all of the different components together in a smooth-working, smooth operation.

You have undertaken a overview, a look at the department with an eye to reorganizing it around threat, vulnerability and consequence. We are about to—we are reauthorizing the departments—I surprised this question was not asked before—and we may do it before the end of the month. What is your opinion as to

whether we should not extend the current authorization until such time as you have completed your assessment, so that we can do this—at least take into consideration, as we reauthorize the department, some of the recommendations that you, the Secretary, would be coming up with?

Mr. CHERTOFF. Well, I have to say, I am not—I am sufficiently versed in the legislative schedule to know what a normal schedule is like. I think it probably would not be a good idea for me to be specific about that. I hope, obviously, that whatever is done—I am going to try as hard as possible to at least get to you what we can in a timely fashion, to have it incorporated in.

Mrs. CHRISTENSEN. And what is your timeline?

Mr. CHERTOFF. Well, I am looking to have recommendations—I have set a deadline for recommendations, or substantially all the recommendations, by the end of May. But there may be some things, you know, working with the committee, that if there are some things that we can identify ahead of time that might require some legislative action, that might be something worth exploring.

Mr. LUNGREN. The gentlelady's time has expired.

We have the Secretary for 29—well, no, 19 more minutes. And we have seven people who are in line. So I intend, or the rules are, to recognize people for 5 minutes. But if they could possibly do less than that, you might allow another member to ask a question.

Congressman Rogers from Alabama is recognized for 5 minutes—.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. LUNGREN. —or such time as he may take of that 5 minutes.

Mr. ROGERS. I got it.

Thank you, Mr. Secretary, for being with us. I want to talk about first responders. I am of the opinion that currently our organization for training first responders does not meet our nation's needs. And I would like to specifically reference the Gilmore Commission Report from December of 2003 which recommended the Department of Homeland Security develop a comprehensive process for establishing training and exercise standards for first responders. And I agree with that statement.

What I would like to know is your thoughts on the current organization of training within DHS and your plans for maybe improving the organization and provision of those training programs.

Mr. CHERTOFF. I think through our preparedness process, in which we have laid down capabilities across the board, which includes response, and then the underlying, supporting template of the kinds of functions, you know, that is designed to drive us in all layers, including responders, to see, you know, what do they have to have the capability to do? What does that mean, in terms of the kinds of tasks they have to be able to perform?

And then that, in our view, and it is not in a final—we do not have the final product, but we have kind of created successive cuts of this that are more precise. That should be the guidance for what, from our standpoint, we need to have first responders capable of doing. Not necessarily every community do everything, but every community be covered geographically by some capability that can perform those functions.

And the idea is to get—you know, use regional support networks to make sure we are not simply giving everybody the same thing over and over again.

Mr. ROGERS. Right.

And the last thing—I would just like to make a comment. Earlier, my colleague from Mississippi talked about his concerns, mainly on several senior management positions within your department that are vacant. And I think that is a very real problem, and it could have some real management consequences down the road if that is not remedied.

I see the number of vacancies, and are not just people you may reference to something similar happening in the military. These people have left the department. I think long term, while your idea of people being cross-trained is good, we have got to find a way to keep that institutional knowledge that we are building for our long-term benefit.

Mr. CHERTOFF. I agree with that.

Mr. ROGERS. Thank you. Thank you, very much.

That is all, Mr. Chairman.

Mr. LUNGREN. Well, the gentleman yields back.

Mr. Etheridge of North Carolina is recognized for 5 minutes or such time as he may consume—.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Mr. Secretary, welcome. And you have got an important job and a tough one. And today, you have been very candid thus far.

Over the last several years, I have raised the issue with people as they came before this committee about an issue that they say is a local level, and that is our public schools. What we saw in Russia and we have seen recently, that can, number one, be a high-profile, and number two, it can send terrible shock waves.

So when you look at the whole issue of threat vulnerability and—you may not fit the first two categories, but you know it has got huge consequences. And all the other things we may do will slide off the sheet when that hits the front page, and it will, when you are dealing with people's children.

So I hope, as you go through your second stage of your review, that this will be an issue that you will pay a lot of attention to, how you provide not only just a template to the local levels, but we have a plan for assistance. Having been state superintendent of schools, I can assure you that should be a higher priority than we are paying attention to.

And I will just leave that where it is. And I will ask that question again when you come back.

Mr. CHERTOFF. Okay.

Mr. ETHERIDGE. In the 2001 Hart-Rudman Report, "Roadmap for National Security: Imperative for Change," the authors stated that the greatest threat to our country at that point, prior to 9/11, second only to the detonation of a weapon of mass destruction would be a failure to manage properly science, technology and education for the common good over the next quarter century.

That being said, the Department of Homeland Security has got a tough job. You have got to deal with this stuff, sir, today that you see immediately, but at the same time, you have got to balance those current trends with long-range planning.

Let me share some statistics with you. Education may not be your responsibility, but we should better be paying attention to it. And I hope you are meeting with the other secretaries.

Currently, one-third of all U.S. science and engineering doctorate degrees, and 40 percent of the PhDs in computer science go to students who are outside the United States, come here and get an education. Some stay; many go home. It is a great plan, but a problem is, if we do not do a better job of training here, we have got a challenge.

So my question is this: How is the department planning to address our nation's current and future needs for technically and mathematically proficient students who we are going to need to maintain that cutting edge in science and technology to be able to meet the challenges for our homeland security?

Mr. CHERTOFF. Well, I do think, you know, we have, I think, programs in terms of science and technology that deal with centers of excellence. And I think we may also have, or are contemplating having, some programs that would try to encourage people to get into areas of research and study that have an application to the kinds of issues we deal with in homeland security.

Obviously, the Department of Education is a separate department, but I could not agree more that the long-term advantage we have in this war is the advantage of our technology and our science. And we cannot afford to lose that competitive advantage.

Mr. ETHERIDGE. Mr. Secretary, let me encourage you to have that meeting. And number two, I know, within your department, that you have some of those funds to encourage that. And I would hope that you would encourage your folks to spend some time, because I think this is a critical issue.

Mr. CHERTOFF. I agree.

Mr. ETHERIDGE. And I think it is not only long term, it is short term. We need to pay a lot of attention very quickly. And if you will do that, I will appreciate that follow-up—.

Mr. CHERTOFF. I will.

Mr. ETHERIDGE. —from that, if you would.

And I will yield back.

Mr. LUNGREN. Thank you.

Mr. McCaul from Texas is recognized for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman.

Mr. Secretary, it is an honor to have you here today. It was an honor to serve under you in the Justice Department. And you did a great job then. I think you are doing a great job today. You have a lot of challenges, but I know you are the right man at the right time for the Department. So I thank you for that.

I also applaud the Department's support for the risk-based funding. I toured the Houston Port Authority with Senator Cornyn last week. And it is the largest port in the United States. It is obviously a target. And I think the fact my state, and California, and New York, are at the low end of the funding, a change would be for the better, based on risk.

I want to focus on—and I know when you were assistant attorney general, you saw this issue coming up quite a bit. In my view, the number-one mission is, and should be, in the homeland security

department protecting our border, protecting our citizens from threats from outside coming in.

And we have a situation that I believe is really getting almost on an epidemic level, in terms of the number of crossings illegally. But my biggest concern has to do with what I am sure you are familiar with, it is called the Catch and Release Program. And it involves people not necessarily from Mexico but countries other than Mexico.

As you saw in your intelligence when you were at the Department—I probably saw some of the same things. And we have the Mexican border in our jurisdiction. And it is a real concern of mine. The thought of a terrorist crossing with a nuclear or biological capability is truly frightening.

In the case of the people from other than Mexico, because of the repatriation process, as you know, they do not—it takes 2 weeks. In many cases, they do not have any space to detain.

In the McAllen sector in Texas, 90 percent of these people get basically released into the streets with a notice to appear, and then they do not show up. You recall Ramsey Yusef, the perpetrator of the 1993 World Trade Center bombing, got into this country that way.

So my question, without giving a speech, is simply, what is the Department doing on this issue? And how can you make members of Congress and the American public feel safer on this issue?

Mr. CHERTOFF. We are doing two things.

First of all, we are—they reason, in terms of when we release, the decision, there are priorities. And we do pay attention to whether we are dealing with somebody who is a special interest person. So those people are not released. Likewise, people who have criminal issues are not released.

You know, this is a problem, obviously, that global law enforcement faces, when you release people on bail, you—you know, we want everybody to appear, but we certainly prioritize detaining those who pose a threat to the community. So that is our template.

Second, we have actually begun and are vigorously pursuing a project of pursuing absconders, people who do not come to appear when they are supposed to appear. And actually, our numbers of people apprehended have increased since the program has begun. That is a very important program, in terms of getting compliance.

We are trying—for example, we did a repatriation program with Mexico. Frankly, if we free up beds for other people, we then have more beds for people we cannot move out that quickly. So another part of our strategy, again, is to try to cut the time that we are holding beds for people who we can deport more readily so we can have additional beds for people that we want to hold.

But it is a serious problem. And at a minimum, what we need to do is make sure we are prioritizing and keeping the people we really have to be concerned about in custody.

Mr. MCCAUL. And as you know, I am in favor of the prioritizing that issue and making those appropriations for that purpose. I think there is no greater issue or threat facing this country. So I thank you for being here.

Mr. CHERTOFF. Thank you.

Chairman COX. [Presiding.] The gentleman's time has expired.

The gentleman from Florida, Mr. Meek?

Mr. MEEK. Thank you, Mr. Chairman.

Thank you, Mr. Secretary, for being here.

I wanted to talk a little bit about the grant process and some of the nuts and bolts of the Department. But I cannot help but resist sharing with you, which you probably already know in your first evaluation, as before the hearing, I told you I was from South Florida, which is unique in itself, as it relates to protecting the homeland. I think there is no other place in the country that faces some of the issues that we face, not only as it relates to immigration but also threat.

I know you are familiar with the act that was passed by the Congress, which is the Federal Information Security Management Act, which, as you know, the Department has received an F 2 years in a row, as it relates to securing its own technology and systems. And we can talk about protecting the homeland, but if the other side, those that are working to infiltrate or to harm us are able to hack our computers, we have a serious problem.

We can have TOPOFF programs throughout the country. They can go in and find out exactly where we are weak from the privacy of their own home. We have a real issue. And with the Department of Homeland Security receiving a threat out of some 24, 25 agencies, and we are supposed to be the leader in securing our information, I think we have a real situation. I think it is very alarming.

I also would—as you know, there is a GAO report that has been written. And the chairman of our subcommittee, and also the Ranking Member, and the chairman of the overall committee, we are going to be having a hearing tomorrow on this issue. Obviously, we are going to be hearing some people—some folks who are in the private sector have served on the subcommittee last year that put forth a bill. Two fine members of this committee will be introducing that same legislation, from what I understand.

But the Department within, I would like to hear as much as you can share at this point of what are some of the steps we have taken to protect some of the information, I mean, as simple as patrols on the borders, as simple as, you know, some of the main functions of the department as it relates to intelligence.

If someone can—if we are getting an F, and there is other agencies that are getting C's and B's, I do not see the improvement. And if there is improvement that is ongoing now, we would like to hear about it.

And I have one other small thing that I want to share with you, but I would appreciate an answer.

Mr. CHERTOFF. Well, my understanding is that, even within—I do not see any other reaction to an F than disappointment. I mean, there is no way you can sugarcoat that or make it seem good.

I think that, notwithstanding the F, and I think it was an F in a prior year thing, there has been some improvement. But there is question more generally speaking that, as a department, our IT function needs a lot of work.

I mean, we were—you know, we inherited IT functions from a number of different legacy departments. Those have not been fully integrated. And bringing somebody onto—it is going to be important to make sure we get that integration process right, not only

to upgrade our ability to defend ourselves but also to make us more interoperable.

I mean, we cannot function in the 21st century without an ability to have an integrated computer system. So I think you are right to point that out as a significant challenge for us.

Mr. MEEK. And of course, you know, this is a bipartisan feeling here in the Congress. It is not, you know, being in the minority side saying, you know, "What are you doing in the administration?"

A couple of my colleagues, including the Ranking Member, addressed the issue of attrition and turnover within the Department at some of the highest levels. Some of the leadership positions in the Department that receive some of the highest security clearance, I mean, they are spending 8 months, 6 months in some cases, and moving on to the private sector and doing other things.

And I do not know if it is an issue of pay or attention or it is so much work to be done, we are saying we are doing something we are not actually doing. And I do not want anything to happen under my watch, so I am out of here. That could be one.

Mr. CHERTOFF. Well, I mean, I think—.

Mr. MEEK. The other could be—I could see if there were great opportunities within the Department, and you saw talent, and you say, "Hey, I need you over here to be able to fill this void," these folks are gone. I mean, they are out of there.

And so we are starting from A, as it relates to the whole training issue, and that is what the GAO report was addressing, that the issue of training, the issue of retention, the issue of occurring, being able to testing of contingency plans, I mean, these are issues that are not there.

Some of those issues are IT issues, but some of them are human resource issues.

Mr. CHERTOFF. Sure.

Mr. MEEK. And we have to address those. But I know that you have limited time.

Mr. Chairman, one last thing I want to share with the Secretary. There was a letter that myself and the Ranking Member sent to you as it relates to some of the reporting that the Department has to make to the Congress to help us and give us guidance on what we are doing good, or what is working and what is not working.

Mr. Secretary, I would ask, as you do your review, hopefully before the second review, start to hopefully report back to the Congress, which is statutorily mandated that we receive this information. Because it will help us in resolving some of our shortcomings in protecting the homeland.

Mr. CHERTOFF. We are going to—I want to try to improve our responsiveness on these issues.

I also have to make a plea that we get some relief from too much reporting and also some sense of priority. I mean, if we know something is really important, we can move to that first. And you know, it is perennially an issue. I mean, sometimes I feel it is the nature of an agency, everybody feels they have to touch something before it goes out the door. And I want to try to streamline that process. But you can help us—that.

Mr. MEEK. Mr. Chairman, I know I am out of time. Mr. Chairman, I just would like to ask that hopefully you can speak with the

Ranking Member and maybe sharing with the Secretary what is a major priority of what we need as it relates to the work that we are going to be doing, because I think that will be helpful.

Some report is better than no report, and I think the Secretary has put an offer on the table that is good.

Chairman COX. Thank you. The gentleman's time has expired.

The gentlelady from Texas, Ms. Jackson-Lee?

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

Thank you very much, Mr. Secretary.

I was impressed, first of all, by your focus in your opening statement that seemed to suggest that you, too, believe that one of the important aspects of security and the functioning of the homeland security is understanding the aspects and facets of the department. And your reference to having initiated a comprehensive view of the organization, operation and policies, I think, is very positive.

I think, however, the Congress may have made a mistake. I would like to be proven wrong. I am very disturbed at the size, as it has become very clear, of the department. It is 180,000 personnel, I am sure all very hard-working. But I have a sense, as this review may show us, that we have a problem with one hand not knowing what the other hand is doing.

I would refer back to the Ranking Member's comments about the number of vacancies. And I know that you are just about 2 months on the job. I would like to pinpoint really a pointed answer on what will be the steps taken, immediate steps taken, so we are looking for good people to fill some of those very vital spots, particularly in border enforcement and security.

My next question would be—I can just do all the three of them—is the dilemma that ICE is in. Before the Judiciary Committee, ICE representatives came and said thing such as, "We do not have uniforms. We do not have badges. In the transition, we are still carrying the same badges and I.D. that we had in our previous position." There was a reprogramming of money, allegedly $500 million. You might comment on whether that has occurred.

But finally, I would say that I hope that, as you look to the policy—as I see the theme throughout your statement, if there is ever a need for policy cooperation, it is in immigration.

We have failed in immigration. We either spend more time stigmatizing it, labeling it, criticizing it, disregarding it, not wanting it. It is here to stay. And I think you need to have a combination of the policy part of it on immigration benefits and enforcement.

I did not hear one statement—and I understand it was a level of frustration on these citizens' part—but I did not hear one statement commenting on the existence of Minutemen on the border of the Arizona—on the Arizona border. Comments being made that the next state would be Texas.

I understand citizen frustration. But if we are to have our hands around homeland security as Congress indicated, it should be, as this department's establishment suggests that it should be, then the frustration of citizens to the extent that Minutemen are on our borders and no policy has come from the administration, meaning no policy statement has come from the administration to suggest that that is intolerable, or that we seek to fix it, or that we will

immediately dispatch numbers of Border Patrol agents possibly from other areas, to me is a silence that we cannot tolerate.

So I would appreciate and look forward with you on these issues. I am particularly interested in the border. We have spent a lot of time in that area, being from Texas. But I do think that what we have on the Arizona border poses a dangerous combination for disaster, for the citizens who mean well and for our Border Patrol agents who every day are putting their lives on the line to do the best job that they possibly can do.

I welcome your thoughts, Mr. Secretary, and I thank you for staying for all of us, so we are here at the very end.

Mr. CHERTOFF. I am appreciative of the congresswoman—.

Chairman COX. Mr. Secretary, I would just alert you that it is just a few minutes after 4:30. I understand that you have a hard deadline that we have agreed to for you to depart. I want to give you the opportunity to do that.

I also want to let you know we have only one member remaining who—.

Ms. LOFGREN. I will hang in there, but I will talk fast.

Chairman COX. —if you can stay, we would very much appreciate it.

Mr. CHERTOFF. I will try to deal with each of the three.

In terms of the vacancies of the senior leadership, again, I mean, in some instances, frankly, I think people who are leaving are leaving because they have done a good job and they are being promoted or moved to something else. And we do have some very talented people who are in the process, I think, of being considered.

We have already got some positions that are filled or we have nominations. And frankly, of course, to the extent where we deal with confirmed positions, and this is an issue for the Senate, obviously, you know, it is a long process. And so we want to move as quickly as possible.

As far is ICE is concerned, the reprogramming documentation has come up. I think it came up a couple of weeks ago. We believe that that will finally at least fix the financial problem that emerged when they broke the original INS and Customs apart.

We need to get that fixed. We are looking hard at the question of how we can improve their financial management—they got cut short with that—including the possibility of having another component step in to take over that function. And that would be a big help.

Beyond that, I think ICE does a tremendous job. And I need to find a way to elevate its profile within the Department and make it clear how much—what a valuable contribution ICE does make.

They have done a tremendous job in dealing with this MS–13 gang and dealing, obviously, with things like child pornography, but also with, you know, human trafficking. I mean, there are huge, very high-profile and very important areas of investigation that they have a premier role in. And I want to make sure that is appreciated and understood.

Finally, as far as immigration is concerned, I think—I mean, the President has it exactly right. He has proposed a temporary worker program which would enable us to identify, you know, those people who are in this country illegally but with no intent to harm and

pull them into the system in a way that would be regulated and controlled, thereby freeing up the resources to focus on people who do not want to operate within the system and who are potentially a threat.

At the border, we added over 500 Border Patrol agents. We moved them into Arizona as part of our Arizona border control initiative. And that was very successful last year. We hope it will be successful again. We have got sensors. We are working on getting UAVs stood up over the summer.

There is no question, I completely agree with you, we have got to—this is a big concern of American citizens, rightfully so. We have got to put a package together. I think the President's package of having, you know, temporary worker effort but also, you know, stepped up and smarter enforcement is exactly the approach that we need to take.

Chairman COX. The gentlelady's time has expired.

The gentlelady from California, Ms. Lofgren?

Ms. LOFGREN. Thank you, Mr. Chairman.

And thank you, Mr. Secretary. I will be quick, and I appreciate your staying.

It has been a pleasure to listen to you here today. And I am—you said much that there is to like here, in an approach that is methodical, and organized, and logical. And frankly, that has not always been presented to us. So I am very eager to work with you in the years ahead.

I would like to—and I very much agree with your emphasis on technology. That is the key to our being successful in this mission.

Just a couple of issues that I wanted to raise, and perhaps you can comment on them.

In terms of technology, I have focused on the issue of immigration functions for several years. The press is reporting that the data integration project at the immigration function has been abandoned for budget reasons. I do not know if that is true. If it is true, I would like to know and if, whatever the case, what the plans are, we are still creating paper records. And obviously you cannot search the database if it is a paper record.

I firmly believe that, unless you have all of the records computerized with a biometric, you are really not going to be able to search them. And that gets me to my second question.

We have never really, so far as I am aware, settled on with probably the assistance of NIST, the appropriate biometric or metrics—they can be redundant. And we have deployed systems that are now incompatible and therefore not fully usable. So I am wondering what you plan to do about that problem.

Finally, I served last year on the Cybersecurity Subcommittee. We have not made progress in implementing the cyber-plan. We have had turnover. Congressman Mac Thornberry, who chaired the committee last year, and I had a bill which we have reintroduced this year for an assistant secretary for cybersecurity so that we can get some attention to this area.

I am sure you read about the NSF funding to avoid what some has said a cyber-Pearl Harbor. We all hope to do that. And I am wondering if you have a position on that bill yet.

Finally, in terms of science, the HSARPA program is really taking a short-term approach. It is not taking the kind of DARPA long-term approach that I had envisioned. And I think, in terms of science and technology, we have faced some very huge risks.

My colleague from North Carolina mentioned the lack of computer, and math, and physics, and science graduates. Half of the graduate students are foreign students. Well, no more, because half of the universities in America reported that their foreign students in graduate departments did not show up because of visa problems. So that is also your department.

We can no longer get scholars into the United States, so the international science projects, the big physics, are going to have to be located in other countries rather than the United States because we cannot get Nobel Prize-winners into the U.S.

I am wondering if you have a plan for dealing with all of those issues. And again, I thank you so much for your approach. And I really look forward to working with you.

Mr. CHERTOFF. Thank you. I think I can touch on all of these.

I am not quite sure what the report is about us abandoning data integration. So it is a little hard for me to answer. I am not aware—I mean, clearly, we need to have, and we are moving toward, making available—and I believe we have at the ports of entry—an ability to search records to make sure we are getting watch lists searched. That obviously is something that is not complete yet, but we have a lot deployed there.

Likewise, with the issue of a biometric standard, I think I can tell you that there is significant progress made toward reaching a resolution of this debate about what is the appropriate biometric standard. And part of it is a recognition that there are different standards for different functions.

If you take fingerprints, for identification of one-to-one, actually one or two prints is enough. But for searching a large database against latest prints, which you want to do in case of terrorists, you probably need ten.

Ms. LOFGREN. If I may, I agree with that. But if you have got different algorithms on the two fingers versus the ten fingers, you cannot use the systems—.

Mr. CHERTOFF. It depends on what—you see, and you can use systems for different things. And in fact, sometimes you do not want to have one system, because you are—both the purposes of speed and purposes of actual privacy, not everybody needs everything.

In other words, if I get someone plugged into the system enrolled, I want to search the widest database and make sure they are not a terrorist. But once I have locked down that identity, and I am comfortable with the person, all I need to know is each time the person presents themselves it is the same person. And that does not require a full search. It requires a one-to-one.

So I think we are moving towards resolution in that area. On the area of cyber, I do think we have—that is a serious vulnerability. As to whether we should, you know, have an assistant secretary or particulars of a bill, I do not know that I am in a position to say that. But it is something that we have, or are clearly aware of, and we are looking at.

Finally, on the issue of visas for foreign students, I mean, I think we have already taken some steps, in terms of lengthening the stay period. It comes back to the original point.

Maybe I should close with the original point the chairman made. We want to have a balance. We need to keep bad people out. There is no question historically dangerous people have abused the student visa system. We have to figure out a way to weed them out, but then also welcome the rest of the world.

I believe, as I think you do, that technology and biometric properly deployed actually is the way to achieve both of those goals. To vet people to make sure we are keeping bad people out, but then to be able to give them a freer ability to go back and forth so as to make this really a friendlier place for the world so we attract the leading minds and the leading capabilities.

Ms. LOFGREN. I totally agree. And it is music to my ears.

Thank you, Mr. Secretary.

Chairman COX. Well, it is appropriate that we end this hearing on what can sometimes be a dismal topic with music and happiness.

[Laughter.]

And I wanted to thank you very much for spending so much time with us. Your testimony is very valuable.

I want to thank the members for their questions. The members of the committee may have some additional questions. We will hold the hearing record open for an additional 10 days.

And, Mr. Secretary, we would ask that you respond to any such questions in writing.

Ms. LOFGREN. Thank you very much.

Chairman COX. Thank you all.

The hearing is adjourned.

[Whereupon, at 4:43 p.m., the committee was adjourned.]

○