S. HRG. 108–851

DEPARTMENT OF HOMELAND SECURITY OVERSIGHT: TERRORISM AND OTHER TOPICS

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JUNE 9, 2004

Serial No. J–108–81

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

22–802 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 THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
LARRY E. CRAIG, Idaho
SAXBY CHAMBLISS, Georgia
JOHN CORNYN, Texas

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
JOHN EDWARDS, North Carolina

BRUCE ARTIM, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah	1
prepared statement	112
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	3
prepared statement	115

WITNESS

Ridge, Tom, Secretary, Department of Homeland Security, Washington, D.C.	7

QUESTIONS AND ANSWERS

Responses of Tom Ridge to questions submitted by Senators Biden, DeWine, Kohl, Leahy, Cornyn, Feingold, Kennedy, and Sessions	33

SUBMISSIONS FOR THE RECORD

Border Trade Alliance, Richard Cortez, Chair, Phoenix, Arizona, letter	109
Ridge, Tom, Secretary, Department of Homeland Security, Washington, D.C., prepared statement	120

DEPARTMENT OF HOMELAND SECURITY OVERSIGHT: TERRORISM AND OTHER TOPICS

WEDNESDAY, JUNE 9, 2004

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, Chairman of the Committee, presiding.

Present: Senators Hatch, Grassley, Specter, Kyl, Cornyn, Leahy, Biden, Kohl, Feinstein, Feingold, Schumer, and Durbin.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Chairman HATCH. We are here today to hold our eighth hearing since last fall to oversee our Government's attempts to protect against and respond to acts of terrorism. We heard from Attorney General Ashcroft yesterday, and today we are pleased to have Secretary Tom Ridge, the leader of our Department of Homeland Security.

In the aftermath of September 11th, a new Department of Homeland Security was created. This was a massive undertaking, the likes of which this country has not seen since 1947, when President Truman reorganized our defense and security agencies.

I, personally, want to thank Secretary Ridge and his colleagues at DHS for your efforts, sir, in improving our Nation's security. You are to be commended for your leadership and the initiatives that you have implemented—initiatives to increase our Nation's ability to respond in time of emergencies to emergencies, to enhance the security of our borders, to increase our ability to defend against bioterrorism, and of course to improve our intelligence-gathering and information sharing, and to integrate our local communities within our Nation's homeland defense efforts.

Now, despite the daunting nature of your challenge, in just over a year, your department has successfully merged 22 agencies and 180,000 employees into a single department. That is amazing in and of itself. You have developed and implemented aviation security procedures, including explosives detection systems. You have issued new security directives, requiring enhanced rail operator protocols. You have tailored the Student VISIT Program to ensure that students who pose no threat to our country are permitted entry. You have streamlined the information-sharing process, which is a big, big move. You have established a Homeland Security Operations Center aimed at coordinating the efforts of the Fed-

eral, State and local authorities. You have enhanced port security, and you have provided substantial assistance to those on the front lines, our Nation's first responders.

By no means is this a comprehensive list of your accomplishments, and all would agree there is a lot more to be done in order to ensure the security of our homeland. Most recently, however, you have proven that you are a leader willing to take the constructive criticism and recommendations of others when it comes to safeguarding our great country.

By way of example, the Office of the Inspector General recently issued a report recommending a number of changes to the Visa Waiver Program. In response, the Department of Homeland Security announced that by the end of September of this year, it will extend U.S. visit requirements to travelers who visit the United States from visa-waiver countries. We have had 93 million visitors from these countries over the past 5 years, so naturally that is not going to be a very easy task. I commend you for taking this bold step forward to improve our visa waiver system and for working to secure this country against the threat of terrorists.

I do want to take a few moments to challenge the administration in an area in which I think we can do much better, and that is bioterrorism.

First off, let me recognize that our country is, in many ways, much better off to respond to various bioterrorism attacks than we were in the fall of 2001. Our first responders are much better equipped. There is much better coordination among the Federal, State and local Governments. We, in Utah, saw this firsthand during the Winter Olympics that went off so successfully there.

I want to commend the administration and my colleagues in Congress for their work on the biofield legislation. Senators Gregg, Frist and Kennedy have consistently moved the ball forward on this issue.

Vice President Cheney and Secretary Thompson have provided leadership in this area. One of the favorites of mine, Dr. Tony Fauci at the National Institutes of Health is coordinating Government, academic and private-sector scientists and, as always, is pushing the envelope of the scientific knowledge forward. Unfortunately, the results to date are simply inadequate. We know that there is a list of some 57 known bioterrorism threat agents. It is my understanding that there are only two—just two—FDA-approved countermeasures to these known threats. That is correct, just 2 of the 57 threats, have responses.

And the truth of the matter is that the R&D pipeline is less than robust. That is one reason why Senator Lieberman and I have proposed bipartisan legislation whose goal is to provide a variety of incentives designed to stimulate private-sector biotechnology firms to develop new research tools, diagnostics, therapeutics, and vaccines.

Our legislation includes tax incentives, intellectual property incentives, such as patent term restoration and extension of current marketing exclusivity periods and up-front liability negotiations. We should not let any politically expedient, antidrug antipathy to interfere with the attempt of the Lieberman-Hatch bill to unleash the creative genius of the private sector because that is where treatments and cures are going to have to come from.

And, sure, we need to create a well-capitalized biodefense industry that will respond to our needs as any of these threats arises or evolves. Now, that is the goal of the Lieberman-Hatch bill. I commend my partner, Senator Lieberman, for his vision in this critically important area. Although the year is moving along, I hope in the weeks ahead to hold a hearing on some of the novel intellectual property and liability provisions of the Lieberman-Hatch bioterrorism bill.

Now, Mr. Secretary, I hope that the administration will carefully review our bill and provide experts to participate in the hearings on that matter.

Now, let me close by saying that I know that everyone on this Committee shares the common goal of protecting our country from additional terrorist attacks, and I believe we are all committed to achieving that goal, with complete respect for the fundamental freedoms of our American people. This Committee has an historical tradition of examining, debating and resolving some of the most important legal and policy issues that have been presented to Congress. Sometimes we get in fistfights on this Committee. It is one of the toughest Committees ever on Capitol Hill. It is always the fault of the other side, of course—

[Laughter.]

Chairman HATCH. —but through these tough times, we are able to do a lot of great work on this Committee thanks to great Senators on both sides of the dais here.

We are, once again, faced with an important task that will have a profound impact on our country's security and liberty. I have every confidence that we are up to that task, and I have every confidence in every member of this Committee to put our country first and to do what is best under the circumstances.

Above all, I hope everybody in the Congress and people throughout this country cooperate with you, as you do this very almost impossible job to try and keep up with everything that possibly could occur that can damage our country, our people, and of course cause a lack of optimism in this country which we have always had. I, personally, want to thank you for the hard work that you have done.

[The prepared statement of Senator Hatch appears as a submission for the record.]

I turn now to Senator Leahy.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Well, thank you, Mr. Chairman. I like your analogy of the fistfights. The Chairman, of course, a former boxer, I am just the punching bag that he works out on every day. But if I can serve my country that way, I do it willingly.

Chairman HATCH. Well, I am so pleased he is willing to be that punching bag and serve.

[Laughter.]

Senator LEAHY. Well, I have now for a period of time.

I want to thank my friend, Secretary Tom Ridge, for being here. Actually, I also want to thank you for your willingness to serve your country in such a difficult position.

We are discussing the state of our homeland security efforts. I worry that we see the American people uneasy about their security as they enter the summer traveling season. Part of the unease may be some of the conflicting signals they are getting from their Government. Yesterday, we heard from the Attorney General, who, 2 weeks ago, took to the Nation's television screens to warn all of us of an impending al Qaeda attack, but it had the appearance of the unilateralism that we have come to expect from the Attorney General's Office.

Earlier the same day, Mr. Secretary, you had appeared on many of those same television screens, and you encouraged Americans to go out and have some fun this summer. I think the American people are left to doubt whether they should be summering in fallout shelter or living their lives the way they had been accustomed before the September 11 attacks. Certainly, I would hope that people in my State, your State and all of the other States could take your advice that you gave to enjoy the summer. We are a great and good Nation blessed with so much, and we should be able to enjoy that.

But the doubts that are in the American people's minds stem, in part, from the administration's failure to follow the process that Congress mandated in the Homeland Security Act of 2002. Under the act, the Secretary of the Homeland Security Department is the only person authorized to issue public threat warnings. And in broadcasting his own independent warnings, of course, the Attorney General ignored the law of the United States.

And I agree with the words of Christopher Cox. He is a well-respected Republican Chairman of the House Select Committee on Homeland Security. He said, "In the Homeland Security Act, DHS was assigned the central coordinating role in this process. The absence of Secretary Ride from the news conference held by the Attorney General and the conflicting public messages their separate public appearances delivered to the Nation suggests that the broad and close interagency consultation we expect, and which the law requires, did not take place in this case. The American public, State and local law enforcement, Governors and mayors, and private-sector officials with the responsibility for critical infrastructure all deserve crystal clarity when it comes to terrorism threat advisories." And I agree with Congressman Cox.

I think the administration's lingering ambivalence about the Department of Homeland Security seems to be a residual byproduct even from the way the Department came about. As we review the administration's failure to hew to the charter of the Homeland Security Act, we should think about the history of the Department's founding. We know, of course, that the President initially opposed the efforts of Democrats—and we had been joined by some Republicans—when we asked to create a Department of Homeland Security. He then flipped over on the issue and embraced the creation of a new agency. Interestingly enough, timing the hurry-up announcement that he had now changed his mind and supported to coincide with the oversight hearing of Coleen Rowley, the FBI agent who accused the administration of negligence in its reaction to the arrest of Zacarias Moussaoui the month before the September 11 attacks. Even the White House admitted the timing was no coincidence.

After the President's conversion, he then barnstormed the Nation. He campaigned against Democratic Senators like Max Cleland, who had, right from the outstart, had supported a Department of Homeland Security, but Senator Cleland wanted one that would respect the rights of the men and women who are working to keep our Nation safe.

Well before the Department was established, the White House, for more than a year, ignored outright—without even a dialogue or an acknowledgment—the appeals many of us had made for implementing the provisions of the PATRIOT Act that authorized help to our partners in homeland security, our State and local first responders, the people that if something happens out in Utah or in Texas or in Vermont or anywhere else, the first people that are going to respond are not going to be us, here in Washington, it is going to be the first responders.

So I would like to be able to tell Americans that, despite the conflicting guidance from their leaders and the President's history of playing politics with homeland security, that their Government was doing everything possible to keep them safe. We cannot say that today. There is much left undone in securing our Nation.

And we have recently learned that a White House budget memorandum circulated within the administration last month states that if he is reelected, President Bush intends to cut spending for homeland security by $1 billion in his next budget—the first budget he will be able to submit knowing that he will not have to face the voters again. So, if we have gaps today, and we go ahead with the administration's plan to cut a billion dollars, there is going to be greater gaps. Apparently, this is because of the fiscal consequences of the tax cuts, but I think that we should worry first not about the wealthiest Americans, but worry about the safety of all of us.

Now, I would like to share some of my most serious homeland security concerns, starting with the administration's failure to provide enough for the first responders. As the costs borne by law enforcement agencies across the country, in communities of whatever size, continue to rise, we should increase funding for our Nation's first responders. Instead, the President has proposed cutting overall funding for our Nation's first responders by $800 million. That will affect every State, large or small.

The Hart-Rudman Report on Domestic Preparedness argued that the U.S. will fall approximately $98.4 billion short of meeting critical emergency responder needs over the next 5 years under the President's budget. Clearly, the domestic preparedness funds available are insufficient to protect our people.

In fact, a 2003 report by the Council on Foreign Relations found a number of serious flaws in the preparedness of our first responders. They found that only 10 percent of the fire departments in the Nation have the personnel and equipment to respond to a building collapse. They also wrote that most cities do not have the necessary equipment even to determine the kind of hazardous materials they may be responding to.

In February of last year, I introduced S.315, the First Responders Partnership Grant Act. I have repeatedly asked Chairman Hatch to mark up this bill. He has declined to do so. That is his choice as Chairman. But the bill would provide $4 billion annually

to support our State and local public safety officers in the war against terrorism. Grants would be made directly to State and local Governments and Indian tribes for equipment, training and facilities. I think it is essential Federal support that our law enforcement officers, firefighters and emergency medical services need. I think it is unfortunate that this Committee will not even consider it. Vote it down if they want, but at least consider it.

I have raised a number of concerns in my remarks. I do not mean by doing that, that I am suggesting you have an easy job. You do not. I told you at the time you got appointed I did not know whether to offer you congratulations or condolences because of the difficult job you have.

I am very proud of the fact that you have made yourself so available to members of Congress on both sides of the aisle. When the calls have gone out, you have not asked whether it was a Republican or a Democrat. You have answered. I wish the Attorney General would do the same, but I admire you for doing that.

I think that the administration should take into consideration these concerns. The Chairman said all of us up here, it does not make any difference our party, we want this Nation, this most wonderful, blessed Nation to be safe. But simply saying we want it safe does not make it safe. And simply saying we are safe, does not make it so. It requires really difficult work, not arbitrarily cutting the budget of our people who have to keep us secure, but working together.

You, Mr. Secretary, have shown a willingness to do that. Please bring the message back to the rest of the administration that you have both Democrats and Republicans who want to work with whomever is President to keep this country safe.

Thank you, Mr. Chairman.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Chairman HATCH. Thank you, Senator.

Senator SCHUMER. Mr. Chairman?

Chairman HATCH. Sir?

Senator SCHUMER. Thank you, Mr. Chairman.

Before we begin, what is the schedule? I have heard that we are going to end this by the time the vote occurs, and some of us will not get to ask questions; is that—

Chairman HATCH. No, I intend to try and follow through.

Senator SCHUMER. We will come back after the vote.

Chairman HATCH. Try to come back. But I know the Secretary is busy, and we are going to have to end it—

Senator LEAHY. If that happens, if we are not able to have all of the Senators have a chance on both sides to get the questions they want, could he come back, say, on Tuesday and continue?

Chairman HATCH. I think we can finish it today.

Senator SCHUMER. Thank you, Mr. Chairman.

Chairman HATCH. We will do our best to do so.

Senator SCHUMER. Thank you.

Chairman HATCH. And I hope, Mr. Secretary, you can give the time to us. We would appreciate it.

Mr. Secretary, we will be glad to take your statement.

Let me just say, though, if we are going to end it, we will continue through the early part of the vote. Those who want to question are going to have to go vote and then come back real quickly so that we do not waste any time.

Mr. Secretary?

STATEMENT OF TOM RIDGE, SECRETARY, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Secretary RIDGE. Mr. Chairman, I would certainly be willing to accommodate that schedule, even if we have to wait a little bit to accommodate your colleagues with a Q and A.

Chairman HATCH. We appreciate it.

Secretary RIDGE. Mr. Chairman, to you, to Senator Leahy, to members of the Committee, I certainly do appreciate the opportunity to appear before you today to discuss our progress at the Department of Homeland Security and our continued efforts working with you to help secure our Nation.

As we all know, the tragic attacks of 9/11 required a swift and drastic change to our understanding of what it actually means to secure America. The Department of Homeland Security was envisioned as a means to bring together some of the most critical homeland security entities in the Federal Government under one central authority to better coordinate and to better direct our security efforts.

We knew, from the outset, that our vast scope of protective measures had to build upon our existing strengths to more importantly be reconstructed in a way that unified and facilitated speed, openness and easy access for all of those involved in the hard work of securing our country every day. With that in mind, we have worked to build more integrated and coordinated homeland security, intelligence and law enforcement communities, communities that connect capabilities and people, that share information swiftly and effectively and that add layer upon layer of security to make our Nation safer and more secure.

Knowledge is both a fundamental principle and instrumental resource in our efforts to secure our borders and our people. The Department has made widespread coordination and information sharing the hallmark of our approach to homeland security. Presidential initiatives like the USA PATRIOT Act and others have helped tear down the walls that prevented our policymakers from having the benefit of intelligence analysis that were based on all available information.

As we have developed new tools for communication to share that information, tools that reach horizontally across Federal departments and agencies, and vertically down to our partners at the State, local, territorial and tribal levels.

Within Homeland Security, we see communication as a two-way process. We collect information from the field and listen to what our partners need from us in order to do their jobs better. This means heightened awareness, better intelligence, wiser decisions, and improved coordination at every level of Government, not just within the Federal Government.

First, we interface with all of the components of the intelligence community, including the Terrorist Threat Integration Center, the

acronym TTIC, in which Homeland Security is a full partner in order to synthesize, analyze and apply information collected from thousands of sources.

Now, let me be clear. The Department of Homeland Security is not in the traditional intelligence collection business, although many of our components collect significant amounts of information. We are definitely in the analysis and application business of that information. It is our job to turn the information into action and implementation. That happens primarily under the umbrella of the Homeland Security Advisory System.

This communication tool includes not only the color-coded threat condition, as well as several projects such as the information bulletins and threat advisories that allow the Department to tailor specific information for specific recipients within the States and local communities, as well as the private sector.

This communications process represents the first-ever centralized, integrated effort of its kind in the Federal Government and a vast improvement from the fragmented system that existed before. It not only outlines threats, but also recommends specific steps that can be taken to heighten readiness or improve physical protections. So this is much more than simply the dissemination of information. This is about achieving the right security outcome, supplying the necessary information and recommendations to decisionmakers on the ground who could then take appropriate action to protect the citizens of their respective communities.

To accomplish this, we have created several new two-way channels of communication, including our National Infrastructure Coordination Center, created strictly to reach out and to have daily contact with the private sector, and the Homeland Security Information Network, created for use by Government entities.

The National Infrastructure Coordination Center provides a centralized mechanism for the private sector, industry representatives, individual companies, and the Information Sharing and Analysis Centers—or ISACs—to share and receive situational information about a threat, an event or a crisis.

The Homeland Security Information Network is a real-time collaboration system that allows multiple jurisdictions, disciplines and emergency operation centers to receive and share the same intelligence and tactical information so that those who need to act on the information had the same overall situational awareness.

This year, we are expanding this information network to include senior decisionmakers such as Governors, statewide homeland security advisers and emergency operation centers in all 50 States, territories, Tribal Governments and major urban areas. And by the end of the summer, we will achieve real-time, nationwide connectivity, more information, more integration, better coordination.

Both of these important communication networks support the Homeland Security Operation Center, a 24-hour-a-day, 7-day-a-week nerve center that enables the Department to monitor activity across the country. This combination of new abilities in information sharing and improved two-way communication has given the Department capabilities that the Federal Government never had before.

Most importantly, it means we have improved our efforts significantly to prevent terrorist attacks and protect Americans. We have emerged from a very static security environment into a dynamic, real-time, action-oriented system of layered protections of air, land and sea and constant two-way communication with our partners at the State and local Government level, as well as within the private sector.

Of course, we build layers of security designed to keep terrorists out. We must not forsake our National character as a country that is both open and welcoming to citizens of all lands. I know this is an issue of particular importance to this Committee, as it should be, and not just to members of the Committee, as it should be to all Americans.

Our homeland security policies have been designed to keep our borders closed to terrorists, but open to legitimate, law-abiding visitors. And programs such as U.S. Visit and One Face at the Border are helping us do just that.

And while stopping a terrorist at our border is a critical accomplishment, we want and need to go even further. We want to stop them before they ever board a plane or a ship destined for the United States. So we are hard at work with other Nations to strengthen visa processes and policies at consular offices abroad, yet we want to do so in a way that does not place an unfair burden on our allies or inhibit legitimate trade, travel and commerce.

An example of this is the Visa Waiver Program which allows citizens of participating ally countries to travel to the United States for business or tourism for 90 days or less without obtaining a visa. To strengthen the security of this program, participating countries are now required to issue machine-readable passports that incorporate biometric identifiers. While this will add an important layer of security, we have learned that the deadline originally set for October of this year will be difficult, if not impossible, for many of these Nations to meet. I must say it is not because of a lack of will, but due to the difficult technical issues of putting such a system in place and, frankly, a lack right now of a consensus around the technical requirements around having a machine-readable passport with the biometric enablers within it.

Secretary Powell and I support a 2-year extension of the deadline to not only give us time to work out the technological issues, but also to ensure that the systems we build is one that is interoperable for all countries.

And I might add, Mr. Chairman, you noted that as of the end of September this year, even the visa waiver country entrants, because we are hoping to get this deadline, but will be part of the US–VISIT program, so they will leave a digital photograph, as well as the finger scans, with us so we can have a record of their entry while we are trying to work out the technical differences among the countries.

By working with our allies and assisting them with time and resources to get this program up and running, we not only can make our Nation safer, but we can also protect the vital flow, the critical flow of travelers to and from our shores. It is this kind of commitment to cooperation and partnership that has led our homeland security efforts from the start.

By working with communities, citizens, business leaders, State and local Government officials, first responders, members of Congress, we have forged a course of protection defined by the integration of our efforts. Everyone pledged to freedom's cause, everyone freedom's protector because everyone is freedom's beneficiary. And as we move forward to secure our land for future generations, we must do so with constant vigilance against our enemies, continued commitment to each other and then unwavering support for the protection of our liberties and the preservation of our freedoms.

I thank the Chairman, the Ranking Member, for the opportunity to testify and appear before you today.

[The prepared statement of Secretary Ridge appears as a submission for the record.]

Chairman HATCH. Thank you, Mr. Secretary.

Let me just ask you this question. We all know that one of your primary responsibilities is gathering threat information and communicating with the public your assessment of the threat level. Now, you performed, I believe you performed this task incredibly well during this past December's holiday season.

And as you know, several weeks ago, the Department of Justice informed the public about an escalation in the chatter among al Qaeda terrorist and the possibility of a summer attack. You and your Department were criticized for not appearing with the Attorney General—unfairly, in my opinion—and for not raising the threat level.

So I would like to give you an opportunity to respond to both of those criticisms.

Secretary RIDGE. Thank you, Mr. Chairman.

First of all, I hope everyone understands that the Attorney General, the FBI Director and I are literally on the same page with regard to sharing of information. We see the same intelligence. We meet daily, and then our organizations, along with the balance of the intelligence community, meet by secure video twice a day. And General Ashcroft and I had a lengthy conversation the other day, understanding that there was some confusion that arose between my public comments in the morning and his statement in the afternoon.

Let me make it very, very clear that we understand we created some confusion and that we have pledged ourselves to make sure that the language we use describing whatever information we are sharing with the public, we are going to do a lot better job coordinating that effort.

It is very important to note, however, that as the two chief law enforcement agents within this country, as the Department of Homeland Security is in the business and given the responsibility of coordinating an administration-wide effort to secure America, that there will be many, many occasions when the Attorney General and the FBI Director will talk to America about the specific law enforcement measures that are being taken as part of a nationwide administration effort. I do not think there should be anything read into the fact that I appear or did not appear with my colleagues. We admit that there was some confusion that arose from that, but we pledge to make sure that it does not happen again.

Chairman HATCH. Well, thank you. As you know, the administration has asked Congress to extend the October 26th deadline for biometric passports, and you have raised that in your opening remarks. We are dealing with cutting-edge technology here, and the fact is that neither the visa waiver countries nor the United States can comply with these current deadlines.

Now, Secretary Powell has also asked the Committee to extend this deadline and has called me personally about it, but time is running out. We can, and must, turn these visionary scientific breakthroughs into a reality.

Now, Secretary Ridge, what might be the national security implications of extending the deadline?

Secretary RIDGE. Well, first of all, I think, in the long term, the national security implications are substantive in the sense that if we can reach a technical agreement within the next year and then get the compliance—there certainly is a will there. The problem right now is technological not a matter of commitment—then it will have very long-term and very positive implications for homeland security. Our ability to be able to use biometrics to identify those who enter the United States, confirm both their identity, as well as validate their passport, is extremely helpful to us.

As you well know, Senator, Congress, well over 10 years ago, had asked the Executive Branch to establish an entry/exit system. It was not until the Department of Homeland Security was created, and then within the Department the decision made was to not only create an entry/exit system, but also to include biometrics. That is the technology of the 21st century that will significantly enhance security. So it is our hope that Congress will give us sufficient time—our request is for 2 years—so that these countries we can all work out to our mutual satisfaction the technical requirements. But while we are doing that, we plan on, and we have told these 27 countries who benefit from the Visa Waiver Program, that their citizens will still be subject to the US–VISIT identification, verifying their entrance and, as we work on the exit model, verifying their exit as well.

So I think it is a very positive step. If we extend it so we can reach agreement on the technical requirements and, in the meantime, we will have them participate in the US–VISIT program, so we will have of a biometric identification of their entry.

Chairman HATCH. Thank you. I reserve the balance of my time and turn to Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman. You did not want to use your remaining 50 seconds?

Senator GRASSLEY. Do not encourage him.

[Laughter.]

Senator LEAHY. Mr. Secretary, just parenthetically, when Secretary Powell called me about extending the biometric, and we probably will, I recalled some urgency in getting that bill signed in the first place. I wish that some of the thoughts had been raised I suggested to him at that time. But I also understand the technology, and it is very complex—digital photographs and digital fingerprints, and you want to get it right so you do not have a lot of people turned back.

We had 100-percent certainty from the Department of Justice that they had the digital fingerprint of a man out on the West Coast, supposedly involved with the bombing in Madrid, and they seized all of his property, his computers, and totally disrupted his life, locked him up and all, and then after a while said, "Whoops, now we are 100-percent certain we have the wrong fingerprint." I do not think we want to, in this beckoning country, to have that sort of thing going on.

Incidently, the impression may have been given that you were criticized about the warning given a couple of weeks ago. You were not the one criticized here by Republicans, and Democrats and the media, it was the Attorney General who was criticized for stepping outside—I just want to make that clear—the criticism was not made of you, it was made of the Attorney General for stepping outside the rules of the homeland security law, which gives you exclusive authority to issue threat warnings to the public.

Do you believe, today, that it constitutes a threat warning to state that, "Credible intelligence from multiple sources indicates al Qaeda plans to attempt an attack on the United States in the next few months," as the Attorney General said in May?

Secretary RIDGE. I think not only has the Attorney General said that, I have said it, other members of the administration have said that there are reports from credible sources, the talk of the intent, whether it is in response to what they perceive to be the influence on the outcomes of the elections in Madrid or not remains to be seen, but there are reports from credible sources that indicate that that is a desire or an intent. There is no—

Senator LEAHY. Do you feel it was a high enough level to go from what you said in the morning about enjoying our summer to—

Secretary RIDGE. No, I do not. I do not. I mean, we are at an elevated level of risk. The threat is fairly substantial. But our job every day within the Department, Senator, there is the normal pace of operations, and you will understand because that is a requirement the Congress gave to the Department, we do not need to raise the threat level to continue to improve security and enhance protection around the country, and that is what we are doing every single day.

If the intelligence dictates, and there is a consensus within the President's Homeland Security Council that we would raise the threat level, then obviously that is a recommendation we would make to the President, and if he agreed, then I would be the one to announce it. But the Attorney General and I had a good conversation about what transpired and admit the confusion that arose.

But substantively, his piece, his discussion of the be on the lookout and the photographs, as well as the task force that he was putting together, again, was part of an administrationwide effort that we would be doing, and are doing, regardless of raising the threat level.

Senator LEAHY. So you would agree with Congressman Cox that the broad and close consultation that the Act requires did not take place in this instance.

Secretary RIDGE. In this particular instance, again, the consultation on the substance occurred. I knew very well that the Attorney

General was going to talk about the BOLOs. We have been working with the Attorney General's office and the FBI about the task force. Again, it is part of the administration-wide effort. But we also decided that not only do we worry about sharing information on the substance, but the tone that need to be projected. We need to make sure that we do a better job with our language, both of us.

Senator LEAHY. I am not trying to play "gotcha" here, but the American people have a great deal of—they give you a great deal of credibility, as I believe they should. And we cannot live in constant fear every day. This Nation, just as most of Europe and a lot of the Asian nations have for decades, we will face terrorist threats probably for the rest of your life and my life, if not from these people, from others.

Secretary RIDGE. Correct.

Senator LEAHY. We are the most powerful Nation on Earth, and we are not having to face, thank God, the threat of armies or air forces or navies coming against us because we are too powerful for that. But there are always going to be those who are going to resent us, for whatever reason, theocratic, political, or anything else, who will come after us. So there will always be a threat.

But I would hate to think that in this great and good country that we are always running, cowering from that. I think we rely on people like you to follow those threats, do everything possible to protect us, wherever they come from. But, you know, we sometimes use too loosely this "we are at war." I was just in Normandy over the weekend with the President and others. That was a war. This is a threat that we will always face, and we will do our best to stop it. But it is a lot different than the war we were at during that time when all of Western civilization as we know it could have disappeared.

Last weekend, Defense Secretary Rumsfeld spoke in Asia about the war on terrorism. The Associated Press reported that he said that the troubling unknown was whether the extremists, whom he termed zealots and despots bent on destroying the global system of nation states, are turning out newly trained terrorists faster than the United States can capture or kill them. He said, "It is quite clear to me that we do not have a coherent approach to this." These concerns are similar to what he had said in his earlier, well-publicized memo in the war on terror.

Do you agree, one, that the revelations of torture and abuse are providing strong motivation for terrorist recruiters? And have you seen any evidence during the 15 months you have held your current posts that the number of terrorists seeking to harm the United States has declined?

Secretary RIDGE. Senator, I am not sure anyone around the world can actually put a firm figure on the number of terrorists that have been generated, not just in the past year or two but over the past 10 or 15 or 20 years, as extremist schools have been funded around the world and there has been a concerted effort within that extremist jihadist community to attract terrorists. I would like to think that we have made it certainly more difficult for them to operate with the destruction of much of their leadership core, at least al Qaeda and the difficulty we have created for them in terms of access to money and communication. But I don't think we should

kid ourselves that—at the very least, I think it is better to think of it in terms of a more permanent condition that you have talked about. We are going to be dealing with this threat, whether it is bin Laden and al Qaeda or a successor to bin Laden and successive organizations to al Qaeda, for the foreseeable future. In my judgment, that is years and decades.

Secondly, I think it defies common sense to suggest that these extremists wouldn't use the unfortunate events around the treatment of the prisoners to try to improve their recruitment.

Senator LEAHY. Thank you, Mr. Secretary, and I will submit my other questions for the record, Mr. Chairman.

Chairman HATCH. Well, thank you, Senator Leahy.

Senator Grassley?

Senator GRASSLEY. Mr. Secretary, the first point I want to make you can't know anything about, but I would like to call it to your attention and have you see if we could get answers to some letters by the end of the week: a March 4th letter, questions to the Bureau of Immigration and Customs Enforcement regarding money laundering; February the 12th, question to Under Secretary Hutchinson regarding your Department's handling of illegal border crossings other than Mexicans, OTMs; and July 23, 2003, questions regarding whether the Department has followed recommendations from internal reports about border security issues, including letting a suspected terrorist under investigation become a citizen. I would appreciate answers to those letters.

Now, my first question to you: money laundering and terrorist financing. Yesterday I asked the Attorney General what role the Department of Justice plays in identifying and confronting the vulnerabilities in our financial system that terrorists and money launderers use to finance their operations. What role do you believe the Department of Homeland Security should play in identifying these vulnerabilities? And, two, who should be responsible for coordinating our Government's response to these vulnerabilities? And how is this responsibility being executed?

Secretary RIDGE. Senator, the overall coordination responsibility rests with Justice and the FBI by specific direction of the President. The GAO commented just a couple of weeks ago on the integration of the efforts between the Department of Homeland Security and the FBI as it relates to terrorist financing.

As you now, we inherited that traditional responsibility in our Department that used to reside in Treasury to go in and explore financial vulnerabilities within the financial services community. Oftentimes, the exploration of those potential vulnerabilities, if you follow the chain of evidence, led to the possibility that the vulnerability was being exploited by a terrorist organization.

To make sure that we would harmonize our approach and to ensure that the FBI would have overall coordinating responsibility, we entered into a memorandum of understanding with the Department of Justice and the FBI nearly a year ago, and the GAO took a look at the relationship since that time and concluded that it is working very effectively. And I think that is a feeling that is shared by both and within both Departments.

The lead responsibility for coordinating is the FBI. Oftentimes, our investigations, based on traditional responsibilities to examine

vulnerabilities within the financial institutions, leads us into a potential terrorist financing investigation. We coordinate with the FBI, give them information. Oftentimes, we continue that investigation, sometimes with their support, sometimes without it. But it is all coordinated through the memorandum of understanding, and it is working quite well.

Senator GRASSLEY. Okay. Information sharing, I hear complaints—I suppose I should say continue to hear complaints from local law enforcement that criminal intelligence does not flow to them from the Federal level. I know that both your Department and Justice are attempting to address the problem. However, I am concerned that various strategies compete rather than cooperate with each other.

Three questions: Which agency is the lead for sharing information with State and local law enforcement? How do your Department's and Justice's strategies fit within the national criminal information-sharing plan? And how does the Department of Homeland Security's strategy work with the regional information-sharing system?

Secretary RIDGE. The FBI historically, through the Joint Terrorism Task Forces, has had an infrastructure that dealt with the police and law enforcement community of not only the major metropolitan areas, but generally to the States and to the local police chiefs through that system. We have a compatible system that we have developed because of our need to—and more often than not, we coordinate our message with the FBI, to establish a linkage with State and local law enforcement as well.

I would say in response to your question that there are times when, depending on the kind of information we are sharing, the primary responsibility may fall either to the FBI or to us. Generally, we work very hard to coordinate those messages so when they are going down either through the FBI's chain or through ours, we have basically signed off and feel it is necessary to send the same message. We don't want to be inconsistent, again, in delivering the message to the State and local governments.

I would tell you that we are developing through the Homeland Security Information Network the ability to connect via the Internet by the end of July real-time Internet-based exchange of information with our Homeland Security Operation Centers for the 50 largest urban centers in this country. During the December time frame, when we went up and raised the threat level, we actually had that kind of connectivity with Los Angeles and New York City. We will have it with the 50 major areas by the end of July, and we will have secure channels to pass that information by the end of the year.

So the objective is to coordinate information, which we do on a regular basis. There are times when we will send out independent pieces of information, depending on the kind of information we are trying to share; some may be far more law enforcement-intense than what we might otherwise send out. We send out bulletins and advisories to State and locals all the time. We coordinate it with the FBI. And, again, we took a look at this Internet-based system, which was the Joint Regional Information Exchange System—JRIES was the acronym. It was actually something they were

doing in California and New York—and said this is a system that ought to be national, it ought to be hooked up to our Operations Center, and we are going to use it to stay in touch with the Governors, the homeland security advisers, the Operations Centers, and the chiefs in the law enforcement community in the 50 largest centers, and we will build out from there. But that is the goal, and that will be the information exchange system that we use within the Department.

Senator GRASSLEY. I have two questions I will submit for answers in writing.

Chairman HATCH. Thank you, Senator.

We will turn to Senator Kohl.

Senator KOHL. Thank you, Mr. Secretary. A little more than a month ago, I wrote to you about potential security breaches at General Mitchell Airport in Milwaukee. An investigation by a local news reporter indicated problems, including the fact that passengers are able to easily identify Federal air marshals. In Milwaukee, the marshals were, or perhaps still are, required to show their badges and register for duty in full view of the general public.

I was troubled by this security gap, and I met with Thomas Quinn, who, as you know, is Director of the Federal Air Marshals Service. I commend Director Quinn for quickly meeting with me, and through his cooperation I believe there have been some improvements. But, to your knowledge, has the situation been resolved in Milwaukee? And on the national scale, what more can we do to make the check-in process for the marshals more discreet, that is, a process whereby an air marshal does not have to report to duty in front of the very people that he is supposed to be protecting?

Secretary RIDGE. First of all, Senator, thank you for the graceful way you pointed it out to us by the letter and the discussion you had with Director Quinn. It is pretty clear that that is not in anybody's interest that we identify for all potential passengers who the Federal air marshals are.

I am afraid that the condition that you reported in Milwaukee was not unique to other airports. We do a better job some places than others, and it is leading to a full-scale review of how we can effect the—nationwide, how we can effect the entrance of the Federal air marshals on to these aircraft. We don't want to do it in a fashion that indicates who they are and what their purpose for securing a seat on the flight is. So it is something that we are grateful you brought to our attention. We are doing a better job in some airports than others, but we are looking at a systemwide change. And as we effect those changes, we would be pleased to report to you, either publicly or privately.

Senator KOHL. I appreciate your interest. Director Quinn said it was his number one priority. And usually when somebody of his stature and influence to be able to move the system indicates a number one priority, there is some reason to believe that there will be some action and on a fairly quick—

Secretary RIDGE. It is. And it has become—

Senator KOHL. He, in fact, said that with respect to Milwaukee, he would give it particular attention. And I do not believe the problem has yet been rectified. And while I am not trying to make this,

you know, into a huge, huge issue that needs to be taken care of this morning, I would like to ask whether or not I could hope to see Director Quinn give that airport and other airports, which, as you point out, are equally important, his attention.

As you said, it doesn't make any sense to have Federal air marshals known to the public. It defeats in a large way the purpose, doesn't it?

Secretary RIDGE. Yes, sir, it does. And, again, to your point, it has become his number one priority as it relates to the FAMS and, therefore, as it relates to the FAMS, our number one priority in the Department. And based on his conversation with you and an assessment of some of the procedures at other airports, we have clearly determined that we need to make some significant improvements in that whole process. And we will be pleased to report you what we intend on doing and then give you a schedule as to when it will be done.

Senator KOHL. I do appreciate.

Secretary RIDGE. Yes, sir.

Senator KOHL. Thank you.

Thank you very much, Mr. Chairman.

Chairman HATCH. Thank you.

We will turn to Senator Cornyn next.

Senator CORNYN. Thank you, Mr. Chairman.

Secretary Ridge, my questions relate to the US–VISIT program and implementation, but first I want to refer to the letter that you and the Secretary of State wrote with regard to the need to extend the deadline for the implementation of the biometric passports under the visa waiver program.

You make some persuasive points in the letter, one of which I want to highlight, though. In addition to the security concerns, which are paramount, there is a concern that the need to acquire individual visas might suppress demand for travel to the United States with tremendous economic consequences in the country. The last sentence said "possibly resulting in multi-billion-dollar losses to our economy and reducing employment in one of our economy's most dynamic sectors."

My question with regard to the US–VISIT program is the implementation of that program along our Southern borders. And, of course, in Texas, as you know, we have about a 1,200-mile border with Mexico. I am sure that Senator Feinstein and Senator Kyl perhaps have similar concerns to make sure that not only that our border security is established, which, again, is our paramount concern—and I know yours as well—but that it be done in a way that does not adversely impact the economy in South Texas, for example, along the border, which are traditionally some of the poorer counties in parts of our State.

Since the advent of NAFTA about 10 years ago, fortunately, we have seen huge economic growth in South Texas. But out of all of the entries into the United States—I believe INS inspects more than half a billion entries into the U.S. each year, but about 80 percent of those, as you no doubt know, are at land borders, and about 800,000 alone occur between the United States and Mexico.

I must tell you that I have been struck by the differences in comprehension of life along our U.S.-Mexican border, between that

area which I know so well and Washington, D.C., because I think we tend to think in global, sort of broad-brush terms. But, specifically, what I would like to ask for your help on—and your staff has been very attentive to these concerns, but I just want to make the point with the boss. There is a tremendous concern about the use of the laser visa, which, ironically, does provide the kind of biometric identifier that US–VISIT hopes to ultimately accomplish for all entries, but with limitations on the time that non-immigrant visa holders, these laser visa holders, can come into the United States to shop and conduct business, which provides a tremendous economic benefit to the border region of the United States, including South Texas.

So I would like to ask for your continued attention and cooperation and just raise this matter to your attention because it is a profound important issue to my State, and particularly the South Texas border region. And it corresponds precisely with the concerns that you and Secretary Powell raised in your letter with regard to the implementation of the visa waiver program.

If you have any comments on that, I would appreciate it.

Secretary RIDGE. I do, Senator. Thank you. I can recall giving very specific directions within a couple of weeks after I came to Washington to initially serve as the Assistant to the President for Homeland Security, when he related the facts associated with making security paramount as of September 11, 2001, at both our Canadian and Mexican borders. We made it paramount, and we basically shut down travel and commerce. We had traffic backed up for literally miles and delays that sometimes went almost as long as a day, if not longer.

So it is pretty clear that along our land borders we have to layer in different means of identifying the people and the products that come across to make sure that they are legitimate and lawful and that the people coming across are law-abiding. And we began that in the Smart Border Accord where we have identified—prescreened certain people, pedestrian traffic, people coming across in commercial traffic, pre-screened shipping companies and the truck drivers that bring that traffic across, looking at various kinds of technology to really apply to the border, again, as part of the layered effort to provide security so we can move literally hundreds of thousand of people across the border back and forth every day.

One of the other things we are looking at is to extend the time and the distance that people with the laser visa can travel, which, again, is part of our effort to—we can legitimize they are coming over for legitimate purposes, but if we make them go back and forth every single day when, in fact, they plan on staying for two or three or 4 days, whatever it may be, it will reduce the pressure on the border.

So we want to layer in different levels of security at the border, and we will continue to work with you and your colleagues on the Southern border, but as well the colleagues on the Northern border, to effect the outcomes that we want, and that is a successful US–VISIT system by the end of this year at the land borders, at the 50 largest land borders in America.

Senator CORNYN. Thank you, sir.

Secretary RIDGE. You are welcome.

Chairman HATCH. Thank you, Senator.

Senator Feinstein?

Senator FEINSTEIN. Thank you very much. And welcome, Governor Ridge.

I wanted to spend my time discussing the visa waiver program because I have carefully read the May 13th report of the Office of Inspector General, and you have got a program that is very sloppy and is in great disarray. It involves 27 countries and 13 million people in 2003 that came into this country without a visa.

We know that this program has been used by terrorists. Specifically, Richard Reid, the shoe bomber, used a British passport; Ramzi Yousef, the 1993 World Trade Center bomber, used a British passport; Mr. Moussaoui used a French passport under the visa waiver program; and Ahmed Ajaj used a Swedish passport. And this report details many others as well. So it is a point of maximum exposure for terrorist intrusion. The management is sloppy, and it goes on and on and on from there.

I wrote you a letter last month, and I referred you to a specific FBI classified memo involving the thefts of large numbers of travel documents relating to this program. Now, the only reason for the theft of large numbers, well in the thousands, of these documents is really to sell them to people who want to fraudulently use them.

The report points out that even when they find a fraudulent passport, the passport is returned to the individual because the individual has to return to their country. So that fraudulent passport is still out there.

I was part of this Committee when we considered the timeline for the biometric passports, and we carefully considered it, and it has already been extended, as you know, a year.

Secretary RIDGE. Correct.

Senator FEINSTEIN. And now the October date is coming up, so the proposal is extended another 2 years. I am one that won't vote for that extension of 2 years because I believe this is an enormous security risk for our country.

If the management problems can't be remedied, I am one that believes we should declare a moratorium on the program. And I know this has raised the ire of the business community, and the concern. But if you measure concern to concern, the concern about terrorist intrusion, which we know this program has been used exactly for that, is much greater, in my view, than the concern about loss of business because somebody has to get an actual visa to come to this country.

We know the problem in US–VISIT. They are documented here. So my question of you specifically on the concerns in this May 11th OIG report is: How much of it has been remedied? How can you assure this Committee that this program cannot be used as an entry program for terrorists?

Secretary RIDGE. Senator, first of all, I think it is important to note as just a matter of public record that the visa waiver program is not a creation of the Department of Homeland Security. We are obliged under an Act of Congress to allow these citizens from the 27 countries in without a visa. So if there is going to be any change in the visa waiver program, it would probably require an Act of Congress to do so since Congress set it up.

The concerns you raise, notwithstanding the origin of the program, are legitimate and very much I believe the reason that this Committee and I think Congress generally supported the requirement that citizens from visa waiver countries on a particular date start appearing at our borders with machine-readable passports with biometric enablers within it.

I would share with you, Senator, that I do not believe that there is anything other than agreement that is growing, I think even internationally, that using biometrics to protect not just our borders but borders of other countries is something that the international community has begun to embrace holistically.

It is interesting, the nature of the conversations that have occurred, and I have seen the evolution over the past 12 to 18 months. The Attorney General and I just concluded a couple of days with our colleagues from the G–8 countries. I just had a luncheon with 25 Ambassadors from the European Union. Everyone is focused now not just on America's borders but the use of biometrics to secure their borders as well.

So I would say to you that, one, we will get compliance, and we are hoping to get the extension, and we will push very, very hard to get the compliance and an agreement around the technical solutions. Two, in our discussions with the EU and the G–8, this notion of fraudulent passports and stolen passports was a critical part of that discussion, and we are working with them to use your poll as a central repository of information about stolen passports and trying to work within their law enforcement communities as well so that we get immediate notice of any of these lost passports.

And as you know, one of the requirements for a country to continue to be on the visa waiver list is that they report to us as quickly as possible lost or stolen passports. And we are going through that whole process now.

Senator FEINSTEIN. Let me just respectfully interrupt you there.

Secretary RIDGE. Sure.

Senator FEINSTEIN. This report points out that even when they report to you the serial numbers of the stolen passports, you can't pick them up unless it is done manually. And I think that is the soft underbelly.

Secretary RIDGE. Well, again, as we develop the technology at our ports of entry, I would tell you, Senator, I believe we are transferring—we are beginning to transfer that information via technology. But we have turned away people at the borders who appeared with a stolen European passport. We do get that information.

Senator FEINSTEIN. Why don't you confiscate the passport? Why do you give them back the fraudulent passport?

Secretary RIDGE. Senator, I am not—on that specific matter, I am going to be discussing that and some other things with my IG this afternoon, and I am not sure that is the case across the board. But I am going to—

Senator FEINSTEIN. It is according to this.

Secretary RIDGE. I understand, and that is why I wanted to discuss that issue with the Inspector General to make sure that if that is—if that is not an aberration, that that is policy, then we change the policy.

Senator FEINSTEIN. Page 25 of the report.

Secretary RIDGE. I understand. We read it.

Senator FEINSTEIN. Okay.

Secretary RIDGE. He and I are going to have a conversation this afternoon.

Chairman HATCH. Senator, your time is up.

Let me just say this: This is a very significant and important day. They have asked that we all be in our seats to vote from our seats on this resolution. The vote is to begin at 11:30, so what I would suggest is that we head over to the floor. As soon as that vote is over, we will come right back. I apologize for this interruption, but it is an important one. And I think by the time we go through one more, some of us would be late to get to the floor.

Secretary RIDGE. I understand, Senator.

Chairman HATCH. And I think we need to show that kind of respect at this particular time. So, with that, we will recess until we can return from the floor, which I hope will be, you know, within a half-hour.

Senator SPECTER. Mr. Chairman, before we break, may I just say a word of welcome to Secretary Ridge, distinguished former Governor of Pennsylvania, now distinguished Secretary of Homeland Security. Nice to see you, Mr. Secretary.

Secretary RIDGE. Good to see you again. Thank you, Senator.

Chairman HATCH. For that we apologize to you, Mr. Secretary.

Secretary RIDGE. I understand, Senator. Been there, done that.

Chairman HATCH. If you would like to come over with us, we would—

Secretary RIDGE. I have been on the other side. Not a problem.

Chairman HATCH. We will recess until we can get back.

[Recess from 11:05 a.m. to 11:45 a.m.]

Chairman HATCH. Mr. Secretary, I am sure you have enjoyed this interlude. I apologize to you. I never thought it would take 40 minutes, but we are grateful for your patience, and we appreciate your being here. And we are going to try and go through this as quickly as we can.

So Senator Kyl will be next, and then we will go to Senator Feingold.

Secretary RIDGE. Thank you. Thank you, sir.

Senator KYL. Thank you, Mr. Chairman. Thank you, Mr. Secretary, and please convey to all of the folks with whom you work how appreciative we are of the work that they do to help provide security for this country.

I would like to return to a subject that Senator Feinstein raised, and others have raised, and it has to do with the Visa Waiver Program. And just to remind folks, if they need reminding, how important this program is. While we work cooperatively now with I believe 27 different countries to ensure that their citizens can gain fairly easy access to this country without obtaining a waiver, there are security issues with that as well. People like Zacarias Moussaoui, Richard Reid, the shoe bomber, Ahmed Ajaj, one of the 1993 World Trade Center bombing organizers, these are the kind of people who came into this country under this Visa Waiver Program. So it is an important program for commercial and other purposes, and yet there are terrorist concerns about it.

One of the things that we asked is that a biometric identifier be created—we did not ask, we legislated—that a biometric identifier on the passports of these people be put into place so that we could ensure that security would be maintained notwithstanding the fairly lax standard with respect to these 27 countries.

The State Department and your department, have asked for a 2-year delay in the implementation of that program because of the inability of the other countries to come together on a standard that we agree with and to implement that standard, as I understand it.

Tentatively, we have a hearing scheduled for next Tuesday, the 15th, in the afternoon. We would like to hear from somebody from the State Department and from Homeland Security to talk to us about precisely how it is that we are going to get our other countries, the 27 countries here, to succeed within that time frame in meeting our objectives—in other words, not to simply say we need an extension, but to come up with a plan on how we are going to succeed in getting the job done by the end of that period of time, if not before. So I will be interested in hearing from the State Department and from your folks about how we can ensure that we can get the job done and not simply have another delay.

Now, you have done a lot of things in response to this IG report, and I want to complement you for that. I know one thing, and you commented on, it was the US–VISIT program. I have two basic questions, and let me just ask them and then you can take the rest of the time to respond.

It is well and good that the VISIT program will be applying in this interim period of time, but of course the question is whether it will also apply after. And that is what I understand the law requires; in other words, that both the entry and the exit aspects of US–VISIT will apply, even after the Biometric Identification Passport Program is completed. I assume that is the case. We would like to get confirmation of that.

Second, there were some other things in the IG report that raise questions about compliance with law. For example, one of the legal requirements is that there be a biennial review to evaluate each country and whether or not they should be maintained on the list and, as a matter of fact, a couple of countries have been dropped as a result of the review.

And in the case of Belgium, they have been put on provisional status. But that requirement under law is not being routinely carried out, and we need to know whether the Department will be able to comply with the legal requirement that every 2 years the effects of the Visa Waiver Program are evaluated with respect to each country, specifically as to law enforcement and security interests.

I note, in that regard, for example, that some of the countries like Belgium, and Sweden and Denmark have very liberal naturalization laws, which the Inspector General noted allows third-country nationals to obtain citizenship in as little as 3 years. Other countries like Ireland and Italy allowed derivative citizenship. And so there are good reasons for evaluating whether, in each case, we want to continue the Visa Waiver Program for these particular countries.

And then just a final point. According to the Inspector General report, there is no DHS department with clear responsibility for the Visa Waiver Program. I do not know that to be the case. If it is, obviously, you are going to be correcting it. If that is not correct, then I would like for you to tell us.

So, if you could respond generally to what I have said and then the specific questions, I would appreciate it very much.

Secretary RIDGE. Thank you, Senator, very much. I am glad we have an opportunity to come back to the question that the Senator from California raised because it is an important question, and we do deal with millions and millions of visitors from visa waiver countries. So I am glad to continue to explore not only the IG's report, but what we are doing about it, particularly since we are the ones that requested an extension.

First of all, it is my belief that the US–VISIT system has been refined to a point where it is not inconvenient at all. It is very much accepted by people coming across our borders. And even when the countries comply with our requirement for a machine-readable, biometrically enabled passport, I see no reason why we would not want to just continue to have them comply with the entry/exit system. I mean, I just think it makes a lot of sense. Congress mandated that we come up with an entry/exit system, and I do not think, in light of 9/11, that you are going to draw an exception for anybody. And I think it is easily done. I think it is easily done.

Secondly, as you know, Senator, the legislation that created the Visa Waiver Program initially said we ought to conduct a review of the status of these visa waiver countries every 5 years. The initial legislation was in 2000. In 2002, Congress said, under the circumstances, every 2 years—very appropriate. I do not know the Inspector General's reference to his data point, but that is a process of review that we are presently conducting and have been conducting or began conducting before the date of his report. But notwithstanding that, we will have those reviews of those countries completed by I believe September 30th of this year.

To the point you made with regard to the unique qualities associated with the policies of 4 or 5 countries—I think you mentioned Belgium, Ireland, places like that—that is something over which we have no legislative or regulatory authority to include in our assessment as to whether or not these countries should have visa waiver status.

Congress has been very prescriptive. They said you need to look at these five or six different things, and based on these particular components of your report, then you need to make a decision as to whether or not they are eligible to remain on the visa waiver list. I do not need to remind my colleagues, but the Visa Waiver Program is basically administered by the Department of State. Our responsibility within the Department of Homeland Security is the biennial review.

And Senator Feinstein made an interesting point. I went back to check it—actually, I was glad to have the break—with regard to getting the passport, discovering that it is fraudulent, and then handing the passport back to the visitor. As I understand it, first of all, we did not set that requirement, and it is done on a case-

by-case basis because some of the countries will not let the offending citizens, the person that tried to get into our country with a fraudulent passport, back into their country unless they have the passport with them.

Now, the State Department has seen that as a vulnerability and has identified and going back on a country-by-country basis and saying, look, I suspect they are saying it is a fraudulent passport. We want you to let your citizen back, but we do not want to put the fraudulent passport back into circulation. So at least I had a little opportunity to find that information and share it with you.

And then, finally, Senator, Secretary Hutchinson, who is the Under Secretary for Border and Transportation Security, really has been overseeing the visa waiver requirements that the legislation has imposed on us in a very, very aggressive way, and I would be happy to send you—we have taken a look at the recommendations. Some of the data points we do not think were particularly accurate.

But notwithstanding that, there are things that need to be changed. There are things that we need to do. We are doing them, and it will take a lot longer than 6 minutes to respond to your question, but I would be happy to send back to you and members of the Committee an answer in writing—a recommendation of what we are doing. I think you will be satisfied that we took the report seriously and are taking action on it.

Chairman HATCH. That would be great.

Senator KYL. Appreciate that very much. Thank you.

Chairman HATCH. Thank you, Senator. We would appreciate having that information.

Senator Feingold?

Senator FEINGOLD. Thank you, Mr. Chairman.

Secretary Ridge, good morning.

Secretary RIDGE. Good morning.

Senator FEINGOLD. Thank you for coming back and spending all of this time here.

Your testimony for today's hearing includes many positive steps the Department has taken to keep America safe. However, as you are aware, the administration has continued to place a tremendous burden on our Nation's first responders, many of whom work in law enforcement. The administration has again proposed slashing many of the most critical law enforcement programs like COPS, Byrne grants and local law enforcement block grants.

As it has in previous years, the administration's current budget proposal would consolidate several law enforcement grant programs into one program—the Justice Assistance Grant Program. The request for the Justice Assistance Grant Program is $284 million less than is currently appropriated for these programs with regard to the time when they continue to be separate.

In addition, the administration has proposed a $1-billion cut in the Homeland Security Grant Program from the fiscal year 2004 appropriations and $250 million from the Fire Act grants. These grant programs are essential in providing funds to our first responders, police officers, ambulance drivers, doctors, nurses, fire workers and EMT workers, and I do oppose these dramatic cuts.

I believe we need to do more, not less, to support our first responders if we want them to be successful. There has never been,

obviously, a more critical time for adequate resources, specialized training, and sufficient equipment for first responders. Local law enforcement, fire departments and community organizations in Wisconsin have repeatedly expressed to me their need for upgraded equipment so they may better communicate, especially in times of emergency.

Mr. Secretary, do you support these proposed cuts, and how can this administration justify these repeated attempts to cut assistance to those who put their lives on the line for the rest of us day in and day out?

Secretary RIDGE. Senator, first of all, I think you know that we have about $8 billion in the pipeline, and right now we are working, frankly, with your State and all of the other States and the territories to break the logjam that has I think frustrated the immediate disbursement of these dollars. That is a real challenge we have, and I think we can find some ways to get the dollars that you have appropriated out. That has been part of their frustration.

Secondly, Senator, the President, in his 2005 budget, requested, in the aggregate amount, the same amount of money he requested in the 2004 budget. And the reductions that you refer to are the difference, by and large, between what the President requested in his 2004 budget and what Congress decided to appropriate.

It is an interesting challenge that executives have. I had the same experience when I was Governor. There were certain programs that I knew that, regardless of the baseline, the legislature would probably add a few dollars onto it. And in trying to control the budget, oftentimes I just went back to the number in the preceding year, anticipating that there would probably be some increase in the following year. But I just wanted to dispel the notion that there has actually been a cut.

I think if you take a look at the aggregate in 2005, while the President did not request in his budget the dollars that Congress ultimately appropriated, the line items for most of those are precisely the requests in 2004. We will, whatever Congress chooses to do with those line items, add, subtract or shift, we will obviously deal with.

But right now I would tell you one of the biggest challenges we have, Senator, is getting a couple of billion dollars that seems to be cut in between the States and the locals distributed to your colleagues in your State and around—we have got a real solid group of people working on some very specific recommendations which we hope to have—no, not hope—we will have delivered to me by the end of June.

We still have a couple billion dollars out there that some of the mayors and the Governors have legitimately expressed some public concerns about. It is not the Federal Government. You told us get ready to allocate that money within 45 days. We are ready to write the checks, but there is a maze of different ordinances, laws, depending on the different States. So we will continue to work on that and hopefully improve the flow of those dollars.

Senator FEINGOLD. I hate to interrupt you, but I have very limited time.

Secretary RIDGE. I am sorry.

Senator FEINGOLD. Just a couple of points.

First of all, I can tell you that, at least with regard to the Byrne grants, and I do understand the role an executive has to play in trying to budget, but it is not a useful exercise to have the administration propose cutting this each time and then having to go around and say how terribly important the Byrne grants are for local law enforcement. This is one at least where the administration should just acknowledge the tremendous support for the program.

Let me also say I know there are some pipeline issues in some parts of the country. But in my State, our experience has been that our people know how to take the fire grants and take the resources for first responders and use them very, very effectively. So I do not want our people painted with that brush, and I think, frankly, States that show that they are able to use the money efficiently should be acknowledged in that regard. And I think it is very important for the safety of the people in my State, as well as the people in the country.

Secretary RIDGE. Senator, I appreciate the correction. There are some States that are doing a lot better job of getting the dollars out the door, and it is those best practices that we want to share with the other States. I apologize for that. I did not mean to paint everybody with the same brush.

Senator FEINGOLD. Fair enough. As you may know, Senator Lautenberg has introduced a common-sense piece of legislation, Senate Bill 921, the State and Local Reservist First Responders Assistance Act of 2003. I have cosponsored the bill. It would authorize the Secretary of Homeland Security to make grants to reimburse State and local Governments and Indian tribes for certain costs relating to the mobilization of reserves who are first responder personnel.

Under the bill, grants can be sought to replace reservists who serve six or more consecutive months of active duty. The administration's decision to extend the deployments of our men and women who are serving in these situations is obviously understandable, but I am wondering what your reaction would be to this sort of a piece of legislation.

Secretary RIDGE. Senator, I cannot give you a public reaction, but would be happy to once I took a look at the legislation. As a former Governor, I appreciate the direction the legislation goes, but I do not have a position one way or the other. I would be happy to review the legislation and share it with you.

Senator FEINGOLD. I look forward to it.

I thank you, Mr. Chairman.

Secretary RIDGE. Thank you.

Chairman HATCH. Yes, Senator.

We will go to Senator Schumer now.

Senator SCHUMER. Thank you, Mr. Chairman.

I want to thank you, Mr. Secretary. As you know, we go back a long time. I have tremendous respect for you. But I have to tell you the frustration in New York at these funding formulas is just through the roof—bipartisan frustration, mayor, Governor, myself, our whole delegation. And so I have to ask you some questions about it.

Secretary RIDGE. Please.

Senator SCHUMER. When we have talked, you have always been very positive, but so far nothing has happened, and that is the problem.

First, on the State Homeland Security Grant Program. This was from the PATRIOT Act originally.

Secretary RIDGE. Correct.

Senator SCHUMER. This was DOJ. The act mandated a .75-percent State minimum. That means about 40 percent of the money went out by formula, and New York and Wyoming got the same amount of money. But then we granted the Executive Branch the ability to give out the money, the rest, the 60 percent any way they wanted. And DOJ decided to do it on a per-capita basis, compounding the problem because we all know that high-need areas should get this money if it is not going to be just pork. I know everyone has a problem. That is why we have a set for everybody.

You have never said a thing on this. Do you think the formula should be changed? It is now something that you would have a lot of say over because this occurred before your department. We have not seen any real leadership on that. It results in New York getting $5.47 per capita, Wyoming getting $38.31 per capita.

Secretary RIDGE. First of all, Senator, I have said publicly, time and time again, I do believe that every State, regardless of the size, regardless of the population, regardless of the risk, should receive from the Congress some financial support to build up, over a period of time, the kind of infrastructure that we are trying to build up nationwide.

But I think the President's budget reflects, in a very dramatic way, when we have shifted, I think, if I recall correctly, about $700 million from the pot that would have been distributed simply based on the formula over to the Urban Area Security Initiative is where we think most of those dollars should go.

Senator SCHUMER. Yes, I will get to that in a minute, but I had—I understand that.

Secretary RIDGE. We have tried to work, recognizing having, because we do go back such a long time, trying to work out a formula with 535 members of Congress in terms of how you distribute those dollars. We have been up here talking and working on it. We have not been able to find the magic formula yet, Senator, but we do think more money should go to high urban areas.

Senator SCHUMER. Would you support changing, though, these grants away from a per-capita basis, the 60 percent in your discretion? If you could give me a yes or no on that because I have two more questions, and we have limited time.

Secretary RIDGE. I will support whatever formula, within existing fund, puts more dollars into an urban area, but how you go about making sure that everybody gets a certain amount of money—

Senator SCHUMER. But, sir, this is done per capita. You made the—your administration, not Congress—made the decision that 60 percent should be per capita. That sends a State without any rural areas getting the same exact amount as to—I mean without any urban areas—the same amount of money per capita as a highly urbanized State. It contradicts what you are saying here.

Secretary RIDGE. But in the aggregate, Senator, in the aggregate, what these smaller States receive, in comparison to what the large urban areas receive, as I said, there is a stark contrast. And all I am saying to you is—

Senator SCHUMER. There is not, not on this formula.

Secretary RIDGE. Not on the per capita. I understand that. I have not been able to come up with a formula that gets 218 votes in the House or 51 votes in the Senate in order to get it done, and as soon as I—

Senator SCHUMER. In all due respect, sir.

Secretary RIDGE. —as soon as I do, I will make the proposal.

Senator SCHUMER. With all due respect, we have not heard a peep. When we tried to lobby this last year, we did not hear a peep out of the administration about what they wanted, how to change it, et cetera. It is not, frankly, that you failed to persuade Congress. You have not attempted to persuade Congress. You sort of let it happen.

But I am going to ask a second one. This is on the High-Threat Urban Area Fund and which you mentioned. We had set aside some money for high urban funding and, again, before you were there, Mitch Daniels was sort of the guy in charge, and I negotiated with him that. And he had promised me that this would go to the high-threat areas. And the first year it did. Of the $800 million, New York City got $160 million.

In 2004, the next round, you gave it out to 50 cities and 30 transit areas, and New York's share dropped to 9 percent. That was on your watch.

Secretary RIDGE. Right.

Senator SCHUMER. Different than the previous year.

Secretary RIDGE. Correct.

Senator SCHUMER. And do you think that New York's threat percentage went down so much that New York, relative to the rest of the Nation, became so much safer? For New York City, which has been the focal point, the only two international major terrorist incidents have had in this country have been aimed at New York City, for New York City to get 9 percent of that is a disgrace, and that was again totally—that had nothing to do with Congress. That was totally your discretion.

And so I would ask you to comment on that, and then I am going to ask you just on two other things because my time is running out.

Secretary RIDGE. Sure.

Senator SCHUMER. There are two bills in the House. One is by Young and Latourette. It continues to give homeland security funding on a per-capita basis regardless of threat of terrorism. That is the Latourette bill.

And it also, an amendment—that is the bill in the Transportation Committee. It also allows these homeland security funds to go to all hazards—tornadoes and fires. There is an alternative bill that Congressman Cox has put together which directs them on the real basis of need. What is the administration's position on, A, the transportation bill, the per-capita bill; B, the Cox bill, which is the Energy and Commerce bill, which is on need; and, C, the provision that allows this money now, which is supposed to go to homeland security, to go to tornadoes and forest fires?

Chairman HATCH. Senator, your time is up, but if you would answer the question.

Secretary RIDGE. I would like to, Senator, and I am not trying to avoid a public answer. I need to get back to you because I do not believe we have a—we have been working with Congressman Cox on the formula, but we have not come up with a position on either measure, but I will get back to you within 24 hours to tell you specifically what we are doing.

Senator SCHUMER. And with a position, I hope.

Chairman HATCH. That would be great.

Senator Durbin?

Senator SCHUMER. Because the problem, if I just might, Mr. Chairman, is the administration says they are for good things and never takes a position on any of these things.

Secretary RIDGE. And I just did want to say, Senator, we have, on both occasions, whether it was on somebody else's watch or our watch, recognized the importance, and the vulnerability, and the sensitivity to New York City's needs. I think, over the past 2 years, they have received twice as much as any other city.

Senator SCHUMER. Nine percent. Do you think 9 percent is fair, when we received 20 percent the year before?

Chairman HATCH. Let him answer the question.

Secretary RIDGE. It is in excess of $300 million, and they would be the primary beneficiary where they would benefit more than any other city if Congress would accept the President's proposal.

And if you can keep the funding formula per capita, the argument is diminished substantially, if you reduce that pool and keep the formula, which would probably be the easiest political solution, and just reduce that pool and take substantial dollars over and put it in the Urban Area Security Initiative Program. And, again, the city that is at the top and the city that will get proportionately more than everybody else is New York City because of population density, because of critical infrastructure.

Senator SCHUMER. I would just say, in conclusion, it is not even close to the needs, and it is not a fair formula. No one thinks it is, and we need your voice and your activity on the Hill, which we have not seen thus far.

Chairman HATCH. Senator Durbin?

Senator DURBIN. Thank you very much, Mr. Chairman.

Governor Ridge, thank you for being here today and for your service to our country.

We spoke briefly before about the interoperable information systems, which has been an issue of concern. I met with your chief information officer, Steve Cooper, on March 3rd. He really was impressive. I think things are moving the right direction.

In your appropriation bill, I asked for a report. I am sure you are always glad to have a request from Congress for a report. If you would be kind enough to take a look at it and ask your people to respond, I would appreciate that very much.

Secretary RIDGE. Sure.

Senator DURBIN. If I could ask you two specific areas.

One of your responsibilities now, of course, with the new consolidated department, is in the area of immigration. There is only one immigration reform proposal that has been reported to the floor in

the 108th Congress, and it came from this Committee. And it relates to a measure known as the DREAM Act, which Senator Hatch and I are co-sponsoring. It passed from this Committee on a 16-to-3 vote, and it relates to providing immigration relief to a select group of students of good moral character who want to pursue college education or military service for example.

This bill has a lot of support, 48 sponsors and cosponsors, but the administration has not taken a position on it. Do you know what the administration position is on the DREAM Act?

Secretary RIDGE. I think you just told me officially there is none, but I would prefer to have the opportunity to review it myself and get back to you, as I have tried to do with some of your other colleagues on some of the other pieces of legislation.

Senator DURBIN. If you would, please.

Secretary RIDGE. Sure.

Senator DURBIN. I have certainly had a lot of differences with this administration, but I have publicly saluted the President for raising the immigration issue, a difficult, difficult issue, but one that we cannot ignore. And I think Senator Hatch and I have found a reasonable way to deal with a specific group of young people who will make a great contribution to America given that chance. So I hope that you would ask the President when you see him and get back to me. That would be very helpful.

Now, I want to speak to an area that is a little more controversial—the Special Registration Program. That explicitly targeted Arab and Muslim males, requiring them to register with your department.

Secretary RIDGE. Right.

Senator DURBIN. The Justice Department created the program. You inherited it. We found that singling out a large group of Arabs and Muslims, it turned out that the vast, overwhelming majority of them were innocent people and really did not, that effort did not help in our efforts to combat terrorism. We, in doing so, though, have alienated a very important community of people in our country.

Due to inadequate publicity, and misinformation from the Department of Justice, many of those who were supposed to register did not or registered late. More than 83,000 people have registered so far. Almost 14,000 have been placed in deportation hearing proceedings because of this. Many were here in the country legally and are being deported simply because they failed to comply with all of the requirements of special registration.

Over the past year-and-a-half a lot of people have expressed concerns about this program. I wrote to you on January 23rd to ask a number of questions about this program. I think this program has failed us, in terms of making America safer, and in fact has created an undue hardship on innocent people. Will you terminate the Special Registration Program?

Secretary RIDGE. Senator, first of all, because you h v paid very close attention to the program, you know that it was our department that did inherit it, but eliminated the 30-day call-back and the annual review. And I would tell you that we are presently, because we now have a good and a robust entry/exit system, we think

our long-term goal should be to treat everybody the same way as they come across our borders, not targeting anyone.

And so we are looking at some of the changes, some of the adjustments we made to visa policy and some of the adjustments we made immediately after 9/11 to see the impact of that. And one of the areas we are looking at very, very carefully is what, if anything, we should do to either modify or eliminate the NSEERS program—that is what you are talking about—with the goal being that regardless of the country of origin, regardless of ethnicity, you will be treated, when you come to our borders, you will be treated the same way. And that review is ongoing.

It would be my intention to make some recommendations not only on that, but other areas of visa policy, to the administration within the next 35 to 45 days. And once that review is completed, I would be happy to, either by phone call or by visit, to tell you what we intend to do about it.

We share the same goal. If you come to the United States, we are an open, welcoming country. We benefit from that kind of openness, and we all know the enormous benefits which treat everybody the same way. In order to do that, we have to make some adjustments to things that we did right after 9/11, for which we are not going to make an apology, but it is time to look at them and see if they really served the purpose for which they were intended, with the goal being one policy applied universally regardless of country of origin.

Senator DURBIN. That is a fair standard, and I think it is one that all of us would applaud. And I commend you for aspiring to that goal in a timely fashion.

I would ask you, as you take a look at this program, that you pay special attention to several things. Individuals who are under this Special Registration Program can still only leave the United States from certain points of departure and have to register their departure with an immigration officer.

And I guess the most troubling aspect is that there were many who were placed in deportation proceedings, and face deportation, not because they were here illegally, but simply because they either registered late or failed to register under the terms of the program.

I think I detected in your remarks the notion that perhaps there were decisions made soon after 9/11 which we can now reflect on and say, all right, now, we were doing those in our best efforts to make America safe. Some achieved their goals, some did not. Now, let us be honest about those that did not and not punish people if we created a program which, in effect, has led to their deportation or some punishment that they did not deserve.

And I hope, when you take a look at it, you will take a look at that particular aspect.

Secretary RIDGE. I will.

Senator DURBIN. Because I think that is a hardship that we ought to try our best to alleviate.

Secretary RIDGE. I think it makes very good sense for us to, on a regular basis, review what we do in terms of our borders, with an eye toward always enhancing security, but that the outcomes we hope to achieve, the benefits we hope to achieve, did we actually realize them? Again, that is tied to the larger goal of we have his-

torically been as open, and as welcoming, and as diverse a country as there is on the face of the earth, and we do not want to let the terrorists change that rather unique, extraordinary quality of America.

That is why the goal, as we review the adjustments we made in a post-9/11 world, is to bring back that universality of application of whatever the policy might be.

I would be pleased to reflect on both these particular elements in that review process.

Chairman HATCH. Thank you.

Senator DURBIN. Let me say, in closing, Mr. Chairman, Governor, thank you for your hard work and your accessibility. I know there are some who are troubled by Congressional meddling in your Executive Department, but you have been patient, to a fault, and submitted to questions time and again. It makes a real difference. And I think it increases the confidence level and the level of dialogue, and I think that is very important for our country.

Thank you.

Secretary RIDGE. Thank you, Senator.

Chairman HATCH. Well, thank you, Mr. Secretary. We really appreciate your taking the time. You have been very patient and especially with that delay, but it was in honor of former President Reagan, and I think we all understand that. But you were very gracious about it, and I personally appreciate it. And I appreciate the way you have answered all of the questions here today, and I appreciate the terrific job you are doing. It is almost an impossible job to do it completely, but if anybody can, you can, and we are very grateful to you.

With that, we will recess until further notice.

Secretary RIDGE. Thank you, Senator.

[Whereupon, at 12:39 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Questions for the Honorable Tom Ridge
DHS Oversight: Terrorism and other Topics
Senate Judiciary Committee June 9, 2004
Senator Joe Biden, Jr.

Resources/Impact on State and Locals

Assistance programs for state and local law enforcement were drastically cut in the President's 2005 budget request— down $1.57 billion from FY 2004 enacted levels. The President's request for assistance in DHS's budget is down *$535* million from last year, a decrease of 16%, and funding from the DOJ is down $1,035 billion. And if you exclude the Urban Area Security Initiative (UASI) from the DHS budget, which only funded fifty (50) cities last year, the decrease in assistance is $2.1 billion, down 53%. These decreases have been a trend every year of the Bush Administration, and this year's request *represents the first time since September 11th that assistance & funding to state and local law enforcement has decreased,* And, the President's budget request does not contain one dime to hire personnel: no funding requested to hire cops, no funding requested to hire firefighters, and no funding requested to hire other necessary personal. The International Association of Chiefs of Police has determined that the President's budget, which fails to fully fund 1)115 and DOJ programs "will reduce the effectiveness of state and local law enforcement agencies and weaken their ability to combat crime and terrorism and protect the communities they serve."

Today, local agencies are called upon to provide dual services. The are required to prevent "traditional" crime, and they are now being asked to identify and apprehend potential terrorists who have different motivations and objectives. Each lime the DHS sends out an alert or raises the terrorist threat level, additional responsibilities are placed upon local law enforcement personnel, and due to tightening budgets there are less and less police on the street to respond to those threats. A recent study found that six out of ten police departments are losing officers, Los Angeles, California has lost 570 officers since 2000 and, as a result, has bad to rely on overtime — up 86%. Others examples include: Boston, MA, 84 cops lost, Detroit, MI 224 cops lost and New York, NY unbelievably has lost 3400 police officers. As a result, most police chiefs have had to cut many of their grass root initiatives, and they are beginning to see rising gang activity.

Most law enforcement officials believe that anti-crime activities also helps prevent terrorism. It just makes sense that the more officers there are to patrol sensitive locations, such as airports, train stations, and others make them safer. In addition, the local patrol officer (700,000 strong) has an intimate knowledge of the communities they serve, and therefore they are uniquely situated to investigate, identify and apprehend suspected terrorists. Just as we need human intelligence to disrupt a terrorist ring in the Middle East, we need on-the-ground, local knowledge to disrupt terrorist cells in our communities.

Question: Is it the position of the DHS that there currently exists sufficient personnel at the state and local level to meet our homeland security and criminal justice needs?

Answer: DHS does not have a position on the "correct" staffing levels for state and local law enforcement. Such requirements have long been driven by state and local criminal justice policies and resources. DHS is committed helping state and local law enforcement improve their capability to prevent and respond to terrorism incidents. Equipment, training, exercises, information-sharing, and improved coordination are the most effective means of achieving this important goal, as they improve the effectiveness of officers already on duty.

Question: Is it the position of the DHS that more local officers and emergency services personnel on the streets would not enhance homeland security?

Answer: Homeland security is not just a Federal responsibility. DHS must rely on the judgment of state and local officials to support public safety staffing levels sufficient to respond to homeland security needs. As DHS evaluates the capabilities of state and local law enforcement, our initial priority to address the equipment and training needs of existing officers. Adding new officers while others lack such equipment and training would not enhance homeland security.

Question: Can you explain the administration's decision not to fund programs, such as COPS, Byrne and LLEBG, that have been determined by local law enforcement officials and Attorney General Ashcroft to be very successful?

Answer: The Department of Homeland Security can not speak to the President's Fiscal Year (FY) 2005 budget request for the Department of Justice. It should be noted, though, that the President's budget request includes strong support for our Nation's emergency prevention and response community, which includes the country's more than18,000 law enforcement agencies. Through the Department of Homeland Security's Office of State and Local Government Coordination and Preparedness, law enforcement agencies will receive substantial support from the $1.43 billion requested for the state formula grants program and the $1.45 billion requested for the Urban Areas Security Initiative. As part of the state formula grants program, the Administration requested $500 million for the Law Enforcement Terrorism Prevention Program (LETPP), which seeks to provide law enforcement communities with enhanced capabilities for detecting, deterring, disrupting, and preventing acts of terrorism. LETPP provides law enforcement communities with funds for a wide-array of activities, including information sharing to preempt terrorist attacks, target

hardening to reduce vulnerability of selected high-value targets, threat recognition to recognize the potential or development of a threat, intervention activities to interdict terrorists before they can execute a threat, interoperable communities, and management and administration costs.

Question: Does the DHS collect statistics related to the economic impact that raising the Threat Advisory from Yellow to Orange has on local on state and local law enforcement?

Answer: The Department does not collect statistics related to the overall impact of raising the Threat Level System. The Threat Level System was instituted to improve communication with public safety officials and the public. We recognize that there are additional costs incurred at the state and local level when the Threat Level is raised from Yellow to Orange.

Question; Has the DHS undertaken any survey, study, analysis or other method intended to determine the economic impact on state and local law enforcement of raising the threat level?

Answer: GAO, at the request of Congress, addressed the question of cost data when they did their HSAS Costs Review. Here are relevant excerpts from the GAO Report:

"Finally, it is important to note that although periods of code-orange alert do result in some additional costs for many federal agencies, states, and localities, the available cost data have many limitations, are not precise or complete, and thus, any conclusions based on these data must reflect those limitations."

" DHS collected information on critical infrastructure protection costs states and localities reported incurring during the March 17 to April 16, 2003, May 20 to 30, 2003, and December 21, 2003, to January 9, 2004, code-orange alert periods through its State Homeland Security Grant Program - Part II and the Urban Areas Security Initiative - Part II. However, this cost information does not represent all additional costs incurred by states and their localities during code-orange alert periods. The U.S. Conference of Mayors also collected and reported estimates of costs localities incurred in response to code-orange alerts. Additionally, a Director with the Center for Strategic and International Studies estimated and reported costs incurred by federal agencies during code-orange alerts. However, because of limitations in the scope and methodologies used in these estimates, the cost information reported may not be adequate for making generalizations regarding additional costs federal agencies, states and localities incurred in response to code-orange alerts."

" In general, the states that have numerous critical infrastructure sites, as identified by DHS, were the ones that reported the most additional code-orange alert costs collectively for the state and its localities. Additionally, DHS officials noted that overtime costs for law enforcement or security personnel appear to be the primary expense incurred by states and localities. You also requested that we determine the extent to which DHS analyzes available cost data related to code-orange alerts and the role that OMB plays in providing guidance to DHS on capturing such costs. Though not required to do so, DHS has not analyzed the cost data collected to identify trends or assess the financial impact code-orange alerts have on states and localities. DHS has not tallied individual or overall state and local costs for any of the increased threat alert periods. However, as cost information submitted by states for reimbursement through SHSGP II and UASI II does not include all costs incurred by states and localities during code-orange alert periods, such analysis may not be appropriate using these data. According to an OMB representative, OMB has not provided specific guidance to DHS in capturing and totaling additional costs that states and localities incurred during periods of heightened national threat levels, nor is it required to do so. However, the representative noted that OMB is concerned about the funds that the federal government expends on these programs and activities.

Publicly Reported Cost Information May be Insufficient for Assessing Financial Impact of Code- Orange Alerts Prior to this report, the U.S. Conference of Mayors and a Director with the Center for Strategic and International Studies have been the only organization or official to attempt to report estimates of costs incurred by various governmental entities in response to code-orange alerts. However, despite their efforts, the information reported by the U.S. Conference of Mayors and a Director at the Center for Strategic and International Studies Homeland Security Initiatives, may not be adequate to draw conclusions regarding the extent to which responding to code-orange alerts imposes a financial burden on governmental entities."

Question: If it is determined that additional costs (overtime charges, etc.) are incurred by state and local law enforcement during periods of high alert or in response to an elevated alert level does the Federal government have any responsibility to provide adequate assistance/ reimbursement?

Answer: The Threat Level System was instituted to improve communication with public safety officials, not as a rationale for Federal reimbursement of state and local homeland security expenses. However, DHS has provided states and localities with some flexibility in using existing grant funds for protection of critical infrastructure during a DHS-declared Yellow and Orange Alert. Funds may be used for the

reimbursement of public safety overtime, contract security, overtime and backfill at state and local Emergency Operations Centers (EOCs), and state National Guard deployments. DHS does place limits on such expenditures as they divert funds from long-term capability enhancements.

Question: Has the DHS defined "homeland security" to exclude community policing? Wouldn't you agree that more police officers on more streets, patrolling airports and train stations and responding to threats make the country more secure than it is now?

Answer: The term "community policing" is subject to considerable ambiguity. DHS does not believe an unfocused effort to simply put more officers on the street will enhance homeland security. Instead, DHS is encouraging states and localities to consider more targeted strategies for r detecting, deterring, disrupting, and preventing acts of terrorism. This includes improved information sharing to preempt terrorist attacks; target hardening to reduce vulnerability; t threat recognition training; intervention activities and interoperable communications. Homeland Security awareness and terrorism prevention training should be an integral component of the training for community policing officers.

Bio Terrorism Funding Reallocation

The Department of Health and Human Services (HHS) is attempting to reallocate resources for bio terrorism. HHS has proposed to reprogram $55 million in FY 2004 bio terrorism funds from the states to 21 large cities. *Many states, including my state of Delaware, will be hurt by this proposal.* In fact, most small states will be hit particularly hard - for example, Delaware would lose over 15% of its federal bio terror funding while Pennsylvania would lose only 3.6% of its funding. The bottom line result for Delaware is that it will remove over $1 million in FY 2004 in bio terrorism funds.

Many states have already established their plans contingent upon receiving this funding, and they have proceeded in good faith with the expectation that funding would be continued. For example, this decrease will interrupt important progress that my state, Delaware, is making. Specifically, it could negatively impact important technology programs that will allow Delaware to detect disease and monitor mass medication dispensing operations.

Question: Do you support Secretary Thompson's effort to reallocate bio terrorism funds?

Answer: More details have recently come to light concerning the threat of a catastrophic attack from a biological weapon, such as anthrax. In such an event, all persons potentially exposed would have to receive treatment within an extremely short, specified period of time depending on the agent used – a daunting task under even normal circumstances. Densely populated urban areas and their surrounding locales are quite vulnerable under such a scenario; however, the plans for dispensing prophylaxis within the allotted span of time must be perfected if lives are to be saved. The Department of Homeland Security recognizes this issue as one that should be addressed quickly, and supports the Department of Health and Human Services in its quest to ensure the ability of states and localities to mitigate the effects of a bioweapon attack.

Question: Was the DHS consulted about this action?
Answer: The Department of Homeland Security understood that resources would be required for the development of more robust state and local distribution capabilities, though it was unaware of the source of funding.

Question: Can you describe the process by which HHS actions, such as the one described above, are coordinated with your Department and other agencies involved in homeland security?

Answer: For some months, HHS has had the assistance of DHS in its

attempts to improve state and local capability to distribute the contents of the Strategic National Stockpile, in the event of a catastrophic bioweapon attack. The DHS Office of State and Local Government Coordination and Preparedness has been the primary interface with HHS from a coordination perspective, and DHS/FEMA has provided support from its Preparedness and Response Divisions, as well as from the National Disaster Medical System.

Question: Do you anticipate or recommend any further shifts in homeland security funding away from states and toward the large cities? If so, what are the standards and assessment methodologies for determining where extra funding would be allocated?

Answer: As you know, the language in the President's Fiscal Year (FY) 2005 request for the Department of Homeland Security recognizes that factors other than a minimum formula and population should be considered in making overall funding allocations. The language further states that the Secretary should have the latitude and discretion to make this determination based on a number of factors, including population concentrations, critical infrastructure, and other significant terrorism risk factors.

Terrorism and the threat of terrorist acts are not static, as is the current formula included in the USA PATRIOT Act. Instead, threats, risks, and vulnerabilities are fluid and can change based on a number of factors. The Department of Homeland Security should not be constrained by a formula and distribution method that does not change to meet current and future security needs. As you know, each state has submitted an updated homeland security strategy as a requirement of receiving and distributing FY 2004 Office for Domestic Preparedness grant funds. It is the Department's expectation that these strategies, and periodically updated strategies, will provide invaluable information to determine appropriate funding levels for all states – large and small, urban and rural.

Further, the Department of Homeland Security is presently working with interagency teams on the Homeland Security Presidential Directive 8 (HSPD-8) effort. One of the directives within this HSPD states that "In making allocations of Federal preparedness assistance to the States, the Secretary, the Attorney General,....and the heads of other Federal departments and agencies that provide assistance for first responder preparedness will base those allocations on assessments of population concentrations, critical infrastructures, and other significant risk factors, particularly terrorism threats..." To this end, ODP is formulating recommendations on these revised funding allocations.

Rail Security

Since 9/11 the Administration has spent approximately $11 billion on airline security while only $100 million has been designated for rail security. Investment to secure our air transportation system is certainly necessary, however, it seems that threats to our non-aviation mass transit are being ignored. The recent tragedy in Madrid painfully demonstrated the massive loss of life and economic impact that can accompany an attack on railways. Yet, the Administration has failed to take any meaningful actions to address these vulnerabilities. The Administration has failed to request adequate funding; the Administration has failed to propose legislation or speak out regarding pending legislation that would provide additional resources to increase the safety and security of rail passengers; and the Administration has failed to set forth a comprehensive plan for securing our railways.

Question: What is the Administration's position on the threat level on our non-aviation mass transit systems?

Answer: Ensuring that our nation's transportation systems are secure must be accomplished through effective partnering between appropriate Federal, State, local, tribal, and private industry entities. We have consistently held that that this responsibility must involve the coordination of appropriate partners, many of whom were already in the business of providing security for their particular piece of the transportation sector prior to 9/11. TSA's main charge, both under the Aviation and Transportation Security Act (ATSA) and as part of the DHS family, is to help coordinate these efforts under the guidance of the Secretary and the Under Secretary for Border and Transportation Security, identifying gaps and working with appropriate partners to ensure that existing security gaps are filled.

As part of the FY 2003 Urban Areas Security Initiative, the Department's Office for Domestic Preparedness (ODP) provided nearly $65 million to 19 mass transit systems. The FY 2003 program was an extension of the larger effort administered by the TSA. Additionally, in FY 2004, as part of the UASI program, ODP provided $50 million to 25 transit systems. For both of these programs, ODP worked closely with TSA and Federal Transit Administration to determine how funds would be distributed, but decisions were based primarily on ridership, track mileage, and presence of critical infrastructure. For the FY 2003 and FY 2004 program, eligible activities included planning, specialized equipment acquisition, training and exercise support. Congress provided an additional $150 million for continuation of the transit security program through the FY 2005 Department of Homeland Security Appropriations Act, and these amounts will be administered by ODP. The application kit is currently under development and will be published in the next several months.

In the months preceding the Madrid and Moscow incidents, DHS, in close coordination with our partners at the Department of Transportation (DOT), State and local

governments, and transit and rail operators, took a number of steps to address vulnerabilities in the rail and transit systems to improve our security posture against such attacks. These efforts spanned the spectrum of security, from information sharing and awareness through prevention, response and recovery to a potential terrorist rail attack in the United States.

In addition to the grant dollars awarded by various DHS components, on March 22, 2004, Secretary Ridge announced additional measures to strengthen security for our rail and transit systems. .

Based on assessments from law enforcement and intelligence agencies, specific threat assessments and analysis, and the use of risk management principles, TSA continually evaluates, sets priorities, and targets the use of available funds to reduce or eliminate the security threat.

Question: Why has the Administration failed to take a position on any legislation designed to provide additional resources and help strengthen rail security?

Answer: DHS has reviewed and commented on two rail/transit bills pending in the Senate—S. 2273 and S. 2453. These comments are included in the official DHS Views Letters, copies of which are attached.

Question: Does the Administration support S. 2273, recently reported by the Commerce Committee? If so, would the Administration be willing to make this support public? If not, what are the concerns of the Administration related to the legislation? Would you be willing to work with Congress to improve this legislation?

Answer: Please see attached views letter on S 2273. The Administration does not support the authorization of $4 billion in new grants for rail transit security. the Administration will continue to work with the Committee, and upon request, make recommendations for improving legislative proposals.

Question: Has the Administration taken <u>any</u> steps to enhance security of hazardous materials that are transported by train?

Answer: Enhancing hazardous materials security has been a critical component of DHS' comprehensive plan to protect our homeland. Since the terrorist attacks of September 11, 2001, the security of hazardous materials shipments has received growing scrutiny. Specifically, the transport of chemicals classified as toxic by inhalation hazardous materials(TIH). Increased concern has centered on the possible effects on public safety of an intentional release of TIH as they are transported through highly populated urban areas.

DHS and the Department of Transportation (DOT) have been working on various initiatives that support the development of a national risk-based plan to address the shipment of hazardous materials by rail and truck. For rail, DHS and DOT are focusing on the assessments of vulnerabilities of high threat urban areas where TIH are transported, the identification of practical alternatives to placards on rail tank cars, new rail car design standards, and the development of hazardous materials security plans to improve the adequacy and effectiveness of current industry security plans.

In July 2003, TSA hosted a workshop at the request of the Association of American Railroads (AAR). At this workshop, TSA brought together experts from the emergency response community, railroads, as well as government agencies to discuss placarding and security and safety issues related to hazardous materials shipments by rail. The result of the workshop was an agreement between the response community and rail community to work together in exploring alternatives to the hazmat placard system. Through an independent scientific study, this group will explore technological and operational alternatives to the hazmat placard system. Both groups agreed that TSA should take the lead organizing this study group. The contract for this study was awarded to Texas A&M's Texas Transportation Institute on July 1, 2004, and results are scheduled to forthcoming by the end of the calendar year.

TSA is also leading a multi-agency task force in the D.C. metropolitan area to conduct a comprehensive security review which includes a vulnerability assessment of the rail infrastructure, which may be used for the conveyance of hazardous materials. This review will be used to create a plan to address any vulnerability uncovered. TSA is working with all affected stakeholders, including the local first responder community, local government, railroad owners and users (VRE, Amtrak). The inter-agency working group will also conduct similar efforts in two to three other cities before making the vulnerability assessment tool available to the nation.

For highways, Congress appropriated $7 million in fiscal year 2004 for hazardous materials security and truck tracking program. TSA expects to competitively solicit proposals for the truck tracking initiative in the fall of 2004, and therefore specific information cannot be provided at this time. All interested parties will be invited to submit proposals in response to this announcement.

Coordination with States

As DHS officials have pointed out on many occasions, homeland security is not a Federal activity it is a national activity. However, the coordinating role is held exclusively with the DHS within the Federal government. As such, it is the role of the DHS provide the vision for homeland security and to coordinate activities with state and local agencies, to set concrete goals, to measure achievement, and to ensure compliance. Many states have indicated that the DHS has not been performing adequately in this role

and has failed to give the appropriate guidance to develop and implement a comprehensive plan to prevent a terrorist attack.

Question: DHS recently announced the expansion of the Homeland Security Information Network, which is intended to expand real-time interactive connectivity and promote a two-way flow of threat information within all fifty states and other local areas. How does DHS intend to support agencies in the states, territories, counties and localities to ensure that the HSIN meets this goal?

Answer: Since the official kickoff of the Homeland Security Information Network (HSIN) with Secretary Ridge on February 24, 2004, there has been significant progress on the national rollout. The Major Urban Area public rollout portion of HSIN occurred in St. Louis, MO on February 27, 2004 and the State level public rollout occurred in Florida three weeks after. The nationwide rollout, Phase One, began in earnest three weeks later to "hook up" the State capitols and 50 Major Urban areas. Currently, all states are connected and the major cities who wanted to be connected have been. In addition, major counties like Broward and Orange County have been hooked up as well. Follow-on training to enhance user capabilities has also been completed at all of these locations.

Phase Two of the HSIN rollout will be the connection of each State Emergency Operations Center to DHS at the Secret level. Connectivity at the Secret level will be carried via TACLANEs, a National Security Agency certified in-line network encryptor, on the CWIN portion of HSIN and will be available to the State and Territory's Emergency Operations Center (EOC). The Phase Two rollout began in December of 2004. Long term connectivity directly with a DHS system will be via the Homeland Security Data Network (HSDN). HSDN rollout will begin this year and should be completed over a four year period.

HSIN-Critical Infrastructure (HSIN-CI) was announced on June 23, 2004 in Dallas, TX by the Secretary and an FBI representative. This pilot program, modeled after the FBI Dallas Emergency Response Network, expands the reach of HSIN to critical infrastructure owners and operators in a variety of industries and locations, as well as to first responders and local officials. In addition, as part of the rollout, any citizen can pass counter-terrorism (CT) information to DHS via the FBI's TIPS program. Currently, HSIN-CI provides terrorist information and alert notification to over 40,000 public and private sector users. This program will be expanding to a nation-wide program throughout fiscal year 2005.

Planning for rollout to the county level will begin in September 2004. This planning will be done in close coordination with the State Homeland

Security Advisors and law enforcement to insure that officials at all levels have full access to relevant homeland security, law enforcement, and domestic incident management information. DHS is also coordinating with DOJ and the states and major cities to develop a model for information fusion centers.

Question: Describe the efforts DHS has undertaken to develop a uniform format for local vulnerability & risk assessments between federal, state, county, and local partners? How will partners gain access to this information?

Answer: DHS has required state and local vulnerability assessments as part of its State Homeland Security Grant Program. In particular, as a requirement to receive their FY 2004 State Homeland Security Grant Program funds, States and territories were required to conduct needs, threats, and vulnerabilities assessments. Based on this information, they developed statewide homeland security strategies on which they would base their funding allocation decisions. [OSGCLP should expand on this topic as needed.] In order to provide a uniform framework DHS is working with the American Society of Mechanical Engineers (ASME) to develop vulnerability guidance, vulnerability consensus standards, and risk guidance for owners and operators of critical infrastructure and key resources (CI/KR). As part of this effort, ASME is producing *Guidance on Risk Analysis and Management for Critical Asset Protection* (RAMCAP), which on completion will contain an overall methodology and a common framework for risk analysis for the 17 critical infrastructure and key resource categories. It is planned that the first RAMCAP modules (chemical and nuclear) will be completed by the end of March, 2005. The remaining modules will be completed over the next fiscal year.

Question: What is the status of the response goals intended to measure the readiness of localities, counties, and states in responding to incidents as set forth in Homeland Security Presidential Directive -8? Will the states and territories have the opportunity to review and provide input on these response goals?

Answer: HSPD-8 requires the creation of an all-hazards preparedness goal, mechanisms to improve delivery of federal preparedness assistance to States and localities, and an outline to strengthen preparedness for our nation. To this end, ODP has developed 4 initiatives to implement HSPD-8: (1) create a National Preparedness Strategy, (2) balance the Federal portfolio of preparedness investment, (3) establish a National Training and Exercise Program, and (4) develop a National Preparedness Assessment and Reporting System. To execute these strategies, a Senior Steering Committee has been put together to oversee the implementation and guide the interagency Integrated Concept Teams (ICTs). The ICTs must develop

comprehensive and executable program implementation plans. Since preparedness is capability based, the National Preparedness Goal will be determined by analyzing existing scenarios, defining baseline capabilities, establishing metrics, and issuing national guidance. This will help DHS establish preparedness requirements and scorecards that indicate gaps, deficiencies and excesses in the nation's preparedness. It will also help generate tools and processes to assist in the prioritizing the allocation of resources.

MAJOR MILESTONES

- March 26, 2004 – Secretary Ridge approves concept for HSPD-8 Implementation.
- July 31, 2004 – Establish Universal List of Mission Essential Tasks for the Homeland Security Community. Submit a multi-year Exercise plan to the President.
- September 1, 2004 – Submit to DHS a Program Implementation Plan and Requirements.
- September 15, 2004 – Submit National Preparedness Goal to the President.
- October 1, 2004 – First Annual Report on the Use of Funds for Preparedness Assistance Programs to the Secretary.
- December 31, 2004 – Complete Federal Response Capabilities Inventory.
- March 15, 2005 – Quantifiable Performance Measurement for Planning, Equipment, Training, and Exercises for Federal Preparedness.
- September 1, 2005 – Full implementation of Process to Develop and Adopt First Responder Equipment Standards and R&D Needs, National Training Program, and National Lessons Learned / Best Practices System.
- September 15, 2005 – First Annual Report to the President.
- September 30, 2005 – Full Implementation of a Closely Coordinate Interagency Grant Process.

State and local stakeholders have been closely involved in the planning and development related to HSPD-8. State, territorial, tribal, and local participation in the Integrated Concept Teams (ICTs) and Senior Steering Committee for HSPD-8 Implementation was carefully selected to balance stakeholder views. State and local stakeholder groups are represented on the ICTs, as well as the Senior Steering Committee. For example, the ICTs and the Senior Steering Committee include representatives from the Fraternal Order of Police, International Association of Emergency Management, National Association of City & County Health Officials, National Emergency Management Association, National Sheriffs' Association, and the National Association of Counties. Representatives

from State governors' offices are also included in the Senior Steering Committee.

DHS is committed to the nation-wide review of key drafts in the process - through an online electronic program management office (ePMO), targeted conferences for some activities, and other means. The intent is to obtain broad review before final drafts are submitted to the Senior Steering Committee and DHS Leadership.

Additionally, the initial version of the universal task list (UTL) is being reviewed by the preparedness community, including over 50 national associations representing State and local stakeholder groups and ICT members. The UTL will define the tasks that must be performed at the federal, state, and local levels to prevent, respond to and recover from the incidents described in the 15 Illustrative Planning Scenarios (IPS) developed by the Homeland Security Council. The IPS will define the range of threats and hazards for incidents of national significance.

Question: Does the DHS intend to sustain and maintain future the State Homeland Security Grant Program (SHSGP) grants?

Answer: Yes. The State Homeland Security Grant Program is a key element of the Department's aid to state and local governments. The Department strongly supports the continuation of these programs, and is committed to maximizing their impact. Annual funding levels will fluctuate, depending upon a range of factors, such as other homeland security priorities and the extent to which Congress supports targeting these grants towards the greatest risks, vulnerabilities, and needs.

Question: Will DHS assist the states by sharing of risk assessment and threat vulnerability data compiled by federal agencies located within the states?

Answer: DHS believes the robust exchange of information, ideas, and practices between all levels of government and the private sector is essential to adequately protect our nation's critical infrastructure and key resources (CI/KR). Sharing vital risk assessment and threat vulnerability data is a necessary component of this information exchange to ensure we are prepared for potential terrorist attacks.

An important component of our information sharing effort is the Site Assistance Visit (SAV) program. This program involves DHS physical security specialists visiting sites throughout our nation to assess vulnerabilities and gather representative data on a sector/segment-basis. These visits involve participation of site security personnel, as well as state and local authorities when appropriate. The objectives of SAVs are to:

- Better understand and prioritize vulnerabilities
- Provide results to assist policy makers at all levels
- Increase awareness of threats and vulnerabilities
- Enhance overall capabilities to identify and mitigate vulnerabilities
- Facilitate government information sharing (e.g., threat assessments, vulnerability reductions)
- Enhance vulnerability assessment methodology development

Information from SAVs is aggregated, normalized, and compiled to create sector and segment-based profiles of vulnerability. As part of its ongoing effort to share this information, the Protective Security Division (PSD) of DHS provides several analytical products to state and local government agencies, as well as owners and operators of critical infrastructure. These sector/segment-specific products, based on risk and vulnerability assessment data collected by DHS, are designed to help CI/KR owners and operators assess their own facilities by identifying, analyzing, and mitigating the risks and vulnerabilities that can make certain CI/KR attractive terrorist targets. The first of these products, *Characteristic and Common Vulnerabilities* (CCVs) reports, provide the insight needed to identify potential targets, analyze vulnerability, and address any gaps in protection to reduce the likelihood of terrorist attack. Secondly, *Potential Indicators of Terrorist Activity* (PITAs) call attention to terrorist surveillance, training, planning, preparation, or mobilization activities that may precede a terrorist attack.

An assessment is also performed as part of the Buffer Zone Protection Plan (BZPP) process. BZPPs expand the zone of protection out from the fence, into the community. They are meant on taking away the operational environment away from the terrorist. BZPPs are conducted by local law enforcement officials in conjunction with site owners/operators and, when necessary, with assistance from PSD personnel. These unclassified (LES/FOUO) reports are submitted to PSD through the State Homeland Security Advisor. States, then, already have this risk and vulnerability data.

By continuing to share the results of their analytical assessments, DHS and PSD work cooperatively with state and local government, as well as the private sector, to increase the overall protection of our infrastructure.

Urban Area Security Initiative Grant

The Administration has proposed funding for the Urban Area Security Initiative at $1.4 billion. This will allow the DHS Secretary to distribute funding to urban areas based upon threat assessment population density and others. While many agree that funding should be prioritized with respect to the areas of most need, most state and local officials feel that this should not be undertaken at the expense of other, more rural, communities throughout the nation. For example, more than 17,000 law enforcement agencies will not be eligible to participate in the UASI and will be forced to compete for assistance from a significantly smaller pool. This concerns many state and local officials who may not be able to adequately prepare for a possible terrorist attack with out Federal assistance. This concern is primarily based upon the fact that states have been given little assistance in determining their vulnerabilities, and the fact that terrorist will often look to so-called "soft" targets, which will make these smaller communities more vulnerable.

Question: What is the threat assessment/ analysis used to determine that funding should be designated to Urban Areas under the Urban Security Initiative Grant Program?

Answer: In FY 2005, the Department based funding allocations on a combination of variables, which resulted in an assignment of a terrorist risk and vulnerability estimate for each city. The variables were 1) a combined threat index derived from classified CIA and FBI threat data, along with the number of FBI terrorism cases opened in a region, 2) a count of critical public and private sector assets, weighted for vulnerability, and 3) and combination of total population and population density.

Question: Is the Administration making a determination that there is a lesser threat in more rural areas? If so, is there any data, studies, or analysis to support this contention? Is there a cut-off with respect to population, density, square miles, etc. to determine eligibility in the UASI?

Answer: While rural areas are not immune from potential attack, both past history and analysis of current threat data continue to indicate that major population centers are the most likely target of a major terrorist attack. In particular, the consequences of an attack in a heavily populated area would be more severe given the proximity of people and infrastructure. . The Department of Homeland Security (DHS) manages the risk of terrorist attack and uses the Urban Area Security Initiative (UASI) Grant Program as directed by Congress as a tool to address the unique security needs of major metropolitan areas.

The Department has not established a size or population cutoff for urban areas and instead considers a range of factors in the grant allocation process that include population density, threat information, and presence of critical infrastructure and key resources (CI/KR).

It should be noted, though, that the Department follows a two-pronged approach in providing support to State and local units of government. As described above, the UASI program focuses on high-threat, high density urban areas. Through the Homeland Security Grant Program (HSGP), the Department allocates funds to all the States, the District of Columbia, the Commonwealth of Puerto Rico, and the territories, who distribute funds based on assessments and determination of threats, risk, vulnerabilities and needs. In order to receive their allocated HSGP funds, they were required to conduct a comprehensive needs, risk and vulnerabilities assessment and develop a homeland security strategy. This strategy allows them to determine how resources should be allocated among urban, suburban, and rural areas. .

Question: Will the threat assessment and analysis used to make this determination be provided to the States?

Answer: While DHS has provided states with a range of information on potential threats, the specific threat analysis underlying the allocation of UASI funds includes classified information, which necessarily constrains wider dissemination. However, DHS provides continuous information, including threat data, to State governors, homeland security advisors, and other state officials as appropriate. This has included routine conference calls held by the Secretary and other senior DHS officials.

Additionally, the Department of Homeland Security's Office of State and Local Government Coordination and Preparedness and Information Analysis and Infrastructure Protection have briefed a number of Members of Congress and their staff on the UASI methodology, including classified briefings to describe reasons why a UASI site that had previously received UASI funds did not receive follow-on UASI funding. At these meetings, Departmental officials, largely from the Office of the Secretary, IAIP and SLGCP, have provided information to Members of Congress and staff, as appropriate, regarding sensitive information that was used by the Department to make final funding decisions. Overall it must be recognized that such data is extremely sensitive and must be managed with the utmost caution. The mismanagement of such data would be detrimental to the nation's overall safety and security.

Follow-up Question to Secretary Tom Ridge from Senator Mike DeWine
Judiciary Committee hearing on "DHS Oversight: Terrorism and Other Topics"
June 9, 2004

My casework office in Columbus, Ohio spends a lot of time assisting individuals who encounter problems when dealing with the immigration bureaus. Several issues have come up at this office, which relate to my conceits about cooperation and communication between agencies within the Department of Homeland Security.

First, my Columbus office has encountered a number of immigration related cases in which the FBI background check has been delayed for more than 6 months. These delays are not the immediate problem, because, understandably, there may be good reason for them. Rather, my main concern is that someone in a supervisory position in the Citizenship and Immigration Services Bureau has purportedly instructed the employees there to not contact the FBI to inquire about the status of these delayed background checks.

Similarly, sometimes Customs and Border Protection makes minor errors in issuing the standard form which all aliens receive when they arrive in the U.S. — the 1-94. The employees of the Citizenship and Immigration Services Bureau have been instructed to not issue corrected forms if the forms were originally issued by Customs and Border Protection. A March 30, 2004 Immigration Services memorandum states that the Service Bureau can issue a corrected form only if it has issued the original form. Presumably, both the Service Bureau and the Customs Bureau have access to the same information and both bureaus have authority to issue the original 1-94; but in issuing corrected forms, only the bureau that made the mistake can correct it. Understandably, this instruction may be the result of a security issue, but if it is just a turf battle — like the turf battles that we have found at the root of our failure to detect the September 11 plot — it needs to be corrected immediately.

Please look into and provide me with an explanation regarding these two situations. I would also like your comments on cooperation and communication between the agencies within the Department of Homeland security. What specific instructions or directives have been issued to facilitate cooperation and communication?

Answer: Since September 11, 2001, the processing of all immigration benefit applications by U. S. Citizenship and Immigration Services (USCIS) are subject to enhanced national security checks. Included in our security check procedures are FBI name checks. USCIS has found these checks to be comprehensive and provide significant information that assists USCIS in performing its mission.

Since that time, USCIS has sent the FBI nearly 4.8 million names to be checked against their databases. A recent review reflects that the FBI responds to USCIS within 30 days of submission 94% of the time. With the remaining 6%, the FBI has found information that requires further review to ensure that the appropriate information is provided to USCIS. This may take a considerable length of time. Of the 6% discussed above, 1% of the cases have been shown to have significant information that assists USCIS in the

adjudication of benefit applications.

USCIS has provided our field offices with a point of contact at our Headquarters who maybe of some assistance in determining the status of a specific case. It has been found that working through our Headquarters staff provides a clear conduit to the FBI vs. all of our field offices reaching out to the FBI.

Your second issue relates to communications between the three agencies that were once INS. We at USCIS have worked very hard with our counterparts at Customs and Border Protection (CBP) and Immigration and Customer Enforcement (ICE) to ensure that we work toward the common goal of protecting the United States. USCIS has effectively communicated to all of our employees that although we are no longer one INS, we are one DHS and it is imperative that the three Bureaus work together. This issue is seen as so important at USCIS, that we have created both internal and external communications components to ensure our success in communicating both up and down the chain. Additionally, USCIS has created a Fraud Detection and National Security Unit to serve as the clear liaison with ICE. This will ensure consistency of process.

Although there may have been bumps in the road, the cooperation and communication has improved over time and we expect this improvement to continue.

With regard to correcting mistakes on I-94s, USCIS and CBP did have discussions about this matter and it was decided that it was important that the agency that issued the document retaint the responsibility and accountability to correct or change I-94s. While it is true that we share access to several computer systems, a USCIS employee might not be able to determine from the automated system the reason the CBP inspector chose to make an I-94 valid for a specified period of time.

United States Senate Committee on the Judiciary
"Department of Homeland Security Oversight: Terrorism and Other Topics"
Written Follow-Up Questions for Secretary Ridge
Senator Herb Kohl

1. Since September 11th we have known that our aviation security has serious vulnerabilities. Now that nearly three years have passed, there is no excuse for leaving any of these problems unaddressed.

   The Transportation Security Administration (TSA) has been operating at its cap of 45,000 screeners for nearly seven months. The GAO recently suggested that staffing shortages hinder TSA's ability to fully staff screening checkpoints without using such things as mandatory overtime. We should not permit airport security checkpoints to be understaffed, And, it is equally as concerning to hear that we may have tired, overworked officers doing the screening.

   If providing adequate security at all airports would exceed the cap, that is something we need to know—so that we can lift it. We want to give you what you need to make this country more secure.

   In a perfect world, how many airport screeners would you deploy to ensure the tightest security possible at our airports?

   Answer: TSA reviews the workforce requirements for each airport on a periodic basis. We have contracted with Regal to develop a "bottom-up" model designed to use airport-specific data to derive highly accurate staffing and throughput projections. It takes into account originating passenger volume, air carrier scheduling and service changes, passenger and baggage screening equipment that has been deployed and installed throughout the nation's airports, and seasonal variations in travel and screening requirements. This tool, once operational, will be an important asset in TSA's efforts to ensure that our screeners are deployed effectively to maximize the safety and security of the traveling public. It will also allow us to engage in further discussions with the relevant Committees of Congress.

At this time, we are also completing a detailed assessment of the equipment and physical constraints at each airport. In a parallel effort, we are working closely with our stakeholder partners in obtaining projected airport expansion information, as well as August 2004 air carrier service and passenger volume estimates. With this data, TSA will be in a better position to forecast screener workforce requirements for each airport.

2. The University of Wisconsin, like many universities around the country, is reporting reductions in the number of applications by foreign students. Officials at the University of Wisconsin believe that lengthy delays in processing visas due to increased scrutiny are a primary cause for the reduction in foreign students.

These and other factors combine to create a perception among foreign students the United States is no longer a country that opens its doors to international students.

While security concerns are, of course, paramount, what actions are being taken to ensure that we are not unnecessarily draining resources and talent from our university system by deterring international students from studying here?

Answer: The United States welcomes students and exchange visitors and encourages them to enjoy their stay in America. DHS is working closely with the Department of State to identify ways to streamline the visa process, particularly for foreign students, and to implement such streamlining measures.

With respect to enforcement , failure to follow rules governing their stay in the U.S. may result in serious consequences. The Compliance Enforcement Unit (CEU), an investigative component of U.S. Immigration and Customs Enforcement (ICE), is charged with monitoring and investigating foreign students, exchange visitors and other non-immigrant visitors who violate their immigration status, and schools and school officials that violate immigration law. The CEU draws upon various government databases to gather and analyze leads on students and exchange visitors and enforces the consequences of status violations by those individuals through means of arrest, detention, and, most likely, removal from the U.S.

Prior to sending the leads to field offices, the CEU forwards the violator leads to a liaison at the SEVIS Program Office (SEVP). The SEVP liaison to the CEU acts as an ombudsman to review SEVIS data anomalies, facilitate data correction, and validate data accuracy prior to the CEU forwarding the data to field offices for enforcement action. In the process of examining SEVIS data, as a collateral benefit, the liaison provides information and assistance to foreign students and exchange visitors, and their educational institutions, to help them comply with SEVIS reporting requirements.

The CEU's lead generation and resolution processes reduce the chance of students and/or exchange visitors being taken into custody unnecessarily. In addition, the CEU makes every attempt possible to confirm violator leads at the headquarters level, thereby making those investigations less invasive in the students' lives.

Written Questions from Senator Patrick Leahy to Secretary Ridge

Fingerprint Databases

1. Earlier this year, Inspector General Fine issued a report on the slow pace of the integration of IDENT and IAFIS, the fingerprint identification databases of the former INS and the FBI. The report examined the case of Victor Manual Batres, a Mexican national with a criminal history who was twice simply returned to Mexico by Border Patrol agents whose database did not identify him as a wanted man. Batres eventually entered the country illegally, and then raped two nuns in Oregon, killing one. The Inspector General reported that the integration that would give Border Patrol agents access to the FBI database was two years behind schedule, and was not expected to be completed until 2008,
   a. What progress has been made on the integration since this report was issued?

      Answer: The integration of the IDENT and IAFIS systems is progressing on schedule. Prior to FY 2004, the responsibility for the integration of IDENT and IAFIS resided with the Department of Justice (DOJ). In FY 2004 responsibility for the acquisition and field deployment of IDENT/IAFIS workstations was transferred to DHS from DOJ. DHS saw the need to continue to deploy this capability and assumed the project management and fiduciary responsibilities for the rollout. DHS/US-VISIT spent approximately $4 million in FY 2004 to continue to deploy to Border Patrol and Inspections locations, and potentially more than $3 million in FY2005 to deploy the integrated workstations to the remainder of the DHS locations.

      DHS agents use the integrated IDENT/IAFIS terminals to collect fingerprints and send them to both the IDENT and IAFIS systems during apprehensions. These terminals account for approximately 50 percent of the total apprehensions of aliens within DHS. In 2004, DHS completed deployment of the integrated terminal to all Border Patrol stations, all air and sea ports of entry, and the 50 busiest land border ports of entry. In 2005, DHS will complete deployment to the remaining ports of entry and ICE field offices.

   b. Pending integration, the FBI has been providing DHS with periodic updates from its database. How often are these updates currently provided?

      Answer: Beginning in mid-June 2004, updates of "wants and warrants" from the FBI's IAFIS system have been performed on a daily basis. This is now a daily, automated process.

Visa Waiver Program/Biometric Passports

2. The Administration has sought an extension of the deadline to implement biometric passports for the Visa Waiver Program (VWP). One of the reasons cited was the need for additional time to resolve challenges related to privacy, data security, interoperability *(e.g.* reader interoperability), chip reliability and durability, production and procurement delays, and the desire to coordinate these efforts with the development of U.S. biometric passports. Please detail the nature and extent of these challenges, and the status of resolving them,

   Answer: Implementation of e-passports is a complex task. Only in May of 2004 did ICAO finalize the standards for e-passports. Preliminary tests conducted earlier this year showed that there was no IC chip proposed for e-passports that could be read by all of the readers on the market and no reader that could read all of the types of chips. In late July, US-VISIT hosted an international meeting where chip vendors, passport manufacturer, and reader manufacturers came together to resolve problems in interoperability.

   Acknowledging the state of technology, and the potential for harm to our international relations with our closest allies, DHS and DOS requested that the October 26, 2004 deadline be extended to November 30, 2006. In August 2004, the deadline was extended to October 26, 2005.

   For the most part, technical problems around the e-passports themselves have been solved and passport production has begun in some nations. However, many countries including the United States are running into problems related to contracting, budget, and acquisition cycles. Due to contract protest, the production of U.S. biometric passports is expected to be delayed several months. As a result, the live tests originally scheduled for February will be delayed because we need the U.S. passports to test in the live tests. Additionally, the volume of foreign passports needed to conduct a meaningful test are not yet available.

   Now the focus is on resolving problems related to the production of e-Passport readers and the integration of these readers into the inspection process. International testing is ongoing, which included a simulated port of entry test at Baltimore-Washington International (BWI) airport during the week of November 29, 2004. The BWI test demonstrated that there is still much work to be done to integrate e-Passport readers into the inspections process in a way that does not adversely affect the inspector's ability to do his/her job. To date, the readers that have been tested in the simulated port of entry environment do not yet meet the operational requirements of U.S. inspection systems.

   Both the passport production and reader integration problems, along with the live test delay, will cause further concern with meeting the October 26, 2005, deadlines.

3 It is my understanding that the early phase of biometric passports will require

security personnel to visually compare a traveler's appearance with biometric information pulled up on a computer screen via communication with the embedded passport. Are there plans to advance the program further to include facial recognition technology, such that this comparison process would be automated, and if so, please describe the protections and implementation schedule for use of this technology?

Answer: We conducted a mock Port of Entry (POE) test at the end of November 2004. Technical problems were identified with the readers but a formal evaluation is not yet completed. During this exercise we looked at facial recognition (FR) technology currently available. We are working closely with NIST to determine technical and ergonomic performance capabilities and impacts. The test focused on the operational aspects of this technology and how it may be utilized in the future. We do know that this is a long-term effort and will require major facility modifications; therefore, at this time, no implementation schedule for FR technology exists.

RFID-Based Security Initiatives for Baggage, Cargo and Boarding Passes

4. At the recent World Air Transport Summit, the airline industry agreed to use RFID for baggage tracking, which is expected to not only improve security, but also reduce customer inconvenience due to lost bags. Last year Delta, in conjunction with TSA, tested the use of RFID technology to track bags and the results showed accuracy levels ranging from 96.7% to 99.9% (as compared to 80 to 85% for the current bar code system), and following some changes, conducted another 30-day test in April of this year.
    a. What were the results of this second test?

Answer: The second set of tests with Delta Airlines and Jacksonville International Airport (JAX) were designed to incorporate technical challenges to understand better the true 'best installation and operational utilization practices' of implementing Radio Frequency Identification Device (RFID) technology in an airport environment for use by TSA, an airline, and an airport. The second test included the use of a new writeable tag and slightly newer reader design. The results for the two vendors tested ranged between 97.5% and 98.9%.

The test also included a trial of a process designed to simulate re-writing the tag as it moved down a sortation belt to simulate changing the status of a bag from non-selectee to selectee. The testing results for one of the vendors demonstrated an accuracy rate from 62% to 69.9% and the second vendor demonstrated an accuracy rate from 9.5% to 25.9%.

b. Even with potential savings of "tens of millions of dollars" the airline spends on locating misdirected bags each year, a Delta representative indicated in an April 2004 *Computer World* article that deploying RFID remains a very expensive proposition and that airline has no plans to launch the program system-wide.

i. Even with potential savings of "tens of millions of dollars" the airline spends on locating misdirected bags each year, a Delta representative indicated in an April 2004 *Computer World* article that deploying RFID remains a very expensive proposition and that airline has no plans to launch the program system-wide.

   i. Do you agree that it is currently financially prohibitive for RFID baggage tracking on a system-wide basis, and if so, given the falling prices for chips and readers, when do you anticipate that it will be financially feasible for RFID baggage tracking to be launched throughout the domestic airline system?

   Answer: No policy decision has been made regarding the security merit of RFID baggage tracking for Federal missions, TSA is monitoring assessments by the private sector of potential costs

   ii. It has been reported that TSA has shared part of the $125 million cost of deploying RFID baggage tracking systems in the McCarran airport in Las Vegas. What percentage of the cost was covered by TSA, the airport and the airlines?

   Answer: To the extent that the cost of facility modifications includes designs to accommodate a future deployment of RFID technology, the government's cost share is 75 percent pursuant to the Letter of Intent (LOI) between McCarran airport and the TSA to fund facility modifications necessary to accommodate an in-line electronic screening solution. The actual cost of deploying RFID technology is outside the scope of the LOI and would be borne by the airport.

   iii. How should cost be apportioned for deploying RFID throughout airports for baggage tracking, *e.g.* between TSA and the airports?

   Answer: There are presently no plans for cost sharing on the part of TSA for RFID.

   iv. It has been reported that TSA is also funding RFID bag tracking for other airports including Denver International and Los Angeles International. Please identify the airports where TSA has provided funding for RFID baggage tracking and the respective amounts of funding?

   Answer: At the present time, neither Denver nor Los Angeles International airports have included an RFID baggage-tracking system into their design plans for the in-line screening solution.

While TSA is working with San Francisco International Airport (SFO) to design an RFID baggage-tracking system, SFO would bear the cost. The costs for implementing such a system at SFO have been estimated at nearly $1 Million.

v. Will TSA require additional funding for RFID baggage tracking efforts, and if so, how much?

Answer: TSA has not developed a deployment strategy for an RFID baggage tracking program for Federal purposes.

That said, prior to the development of any implementation plan and cost estimate, expanded operational tests and evaluations in several areas would be undertaken to include the following:

- A full 860 to 956MHz worldwide UHF interoperability trial with many of the major airlines and airports to clearly demonstrate that UHF is the frequency to be chosen for RFID;
- Develop an airport test bed with one or more representative U.S. airports to evaluate new tags/readers as soon as they are available in a real world operational environment; and
- Develop a test bed with a baggage conveyor system manufacturer that has a fully functional laboratory sortation system so unique integration issues can be worked out offline prior to going into the airport test bed.

c. One of the challenges of using RFID to track baggage is interoperability with other systems. For example, the U.S. has been using 915 Mhz for RFID-tagged baggage; whereas Japan has been using 955 Mhz. In addition to varying international frequency choices, RFID deployment often varies by choices on chip size and data storage, as well as the nature, material surroundings and layout of the items being tracked, What are the plans to address these challenges, what role is TSA playing in promoting a standard both among domestic airlines, as well as internationally, and when do you anticipate that there will be international operability for baggage tracking?

Answer: DHS and TSA support the position of U.S. airlines for the establishment of an international UHF RFID baggage tag specification/standard that could serve worldwide, system-wide interoperability needs. A recent proposal to the International Air Transport Association (IATA) (presented by Delta Airlines in mid-June in Montreal) would standardize the tag storage minimum requirements, as well as allow for added data storage for individual user needs beyond what is required for airline worldwide interoperability.

In addition, TSA is exploring how to resolve the challenges presented by

the different UHF frequencies allowable worldwide. TSA either has or is in the process of conducting 2 of the three ultimate UHF interoperability trials that are required to confirm compatibility regardless of the UHF frequency at which they were programmed. The two completed trials are: HNL/NRT with 956 MHz and 915 MHz and PHL/FCO with 865 MHz and 915 MHz. The third trial would encompass the full frequency range of 865 MHz to 956 MHz.

d. Are there plans to mandate that domestic airports implement RFID for baggage tracking? Are there plans to mandate that bags arriving from international destinations also be RFID tagged?

Answer: There are presently no plans to impose a Federal mandate on the use of RFID for baggage tracking, domestically or internationally.

e. Please detail the plans to protect traveler's privacy and data security while implementing the RFID baggage tracking program.

Answer: DHS and TSA are committed to respecting privacy rights. Any future Federal role for RFID would likely only encompass baggage-tracking to ensure that baggage requiring enhanced screening procedures proceeds from the airline check-in counter to the appropriate screening location. While the baggage tracking system does have to capture the identity of the bag owner for the system to be of value in terms of security, the baggage tracking system does not have to permanently store that information.

5. The Department has considered the use of RFID technology to track and verify cargo to improve monitoring and security.
   a. The nature of cargo posses several challenges for the use of RFID. For example, certain materials, like metal containers carrying cargo or liquids can reduce the ability for readers to capture information on RFID tags. What plans does the Department have for addressing such challenges?
   b. What is the status and implementation schedule for using RFID to track and verify cargo?

Answer: TSA has conducted limited RFID trials involving the use of containers used by airlines to hold cargo and baggage; however, to date, TSA has not conducted a specific cargo RFID trial. TSA has initiated preliminary discussions with representatives from one of the major U.S. airlines concerning potential joint TSA and airlines trials related to RFID and cargo.

c. To what extent is TSA funding RFID efforts to improve cargo tracking? Is additional funding required, and if so, how much? In addition, how should the cost of deploying RFID for cargo tracking be apportioned, *e.g.* between TSA and the seaport operators?

Answer: TSA has not allocated funding specifically for RFID projects associated with cargo. Any funds that could be made available would be used to initially engage in cooperative trial(s) with transportation partners.

6. Following September 11, U.S. Customs (now the U.S. Customs and Border Protection) launched the Container Security Initiative. Countries participating in the initiative must meet certain eligibility requirements, for example, making available non-intrusive inspectional equipment like gamma or X-ray imaging. Are there plans to require use of RFID capabilities as part of the eligibility requirements for CSI?

   Answer: There are no current plans to require RFID capabilities in order to be eligible to participate in CSI. Currently under the "24-hour Rule", CSI ports get Bill of Lading data well in advance of the container being loaded onboard a vessel. This advance information provides the CSI officers to run data analysis, target any high-risk containers and perform any physical examinations prior to the container being loaded onto the vessel. With the advance Bill of Lading information provided via the "24-hour Rule", the use of RFID technology would not add to manifest information already being received.

7. Earlier this year, reports indicated that TSA was considering the use of RFID-tagged airline boarding passes for customers who sign up for a "registered traveler" program. This would allow travelers to pass through designated areas in the same way commuters use E-Z passes to go through toll booths.
   a. Please provide the status and implementation schedule for this plan?
   Answer: TSA is conducting five Registered Traveler pilot programs during the fourth Quarter of Fiscal Year 2004. The pilot sites are Minneapolis-St. Paul International Airport, Los Angeles International Airport, George Bush Intercontinental Airport - Houston, Logan International Airport, and Ronald Reagan Washington National Airport. The pilot programs will assess improvements in security and enhancements in customer service for passengers. Results of the pilots will be analyzed to determine the pilot programs' effect on security and customer service with initial results expected in January of 2005.

   During the RT pilot programs, TSA will test technology, in the form of biometric tools to enhance identity verification at the passenger security checkpoint, in conjunction with enhanced business processes, including potential reconfiguration of select checkpoint lines and lanes. The biometric tools to be used are fingerprint and iris recognition technologies.

   The Registered Traveler pilot program does not involve testing of RFID Technology.

b. Has the Department evaluated the timeframe and costs of embedding boarding passes with RFID chips, deploying readers throughout airports and providing software infrastructure to manage the RFID-collected data, and if so, what would those be?

Answer: TSA has no plan to use RFID enabled boarding passes with the Registered Traveler program.

c. What are the security and privacy challenges to implementing this program, and has DHS resolved these challenges?

Answer: The Registered Traveler (RT) Pilot Program is voluntary. Therefore, the primary security and privacy challenges involve the collection and storage processes for pilot participant enrollment data. DHS and TSA have addressed the privacy components associated with collecting personal enrollment data for the RT Pilot Program and have worked to ensure that the program is compliant with applicable security and privacy standards. These safeguards have been accomplished by implementing process controls surrounding the collection and storage of pilot enrollment data.

TSA will secure personal information against unauthorized access through the use of a layered security approach involving procedural and information security safeguards. Specific privacy safeguards can be categorized by the following means:

- *Technical limitations on, and tracking of, data access and use;*
- *Use of secure telecommunications techniques; and*
- *Limitation of physical access to system databases and workstations.*

This approach meets the requirements of the following laws:

- *Privacy Act of 1974, as Amended (5 USC 552a), which affords individuals the right to privacy in records that are maintained and used by Federal agencies.*
- *Federal Information Security Management Act of 2002 (Public Law 107-347), which establishes minimum security practices for Federal security systems.*

TSA developed and published on June 1, 2004 in the Federal Register the System of Record Notification. TSA has also completed the Paperwork Reduction Act (PRA) notice, the OMB83i, and the Privacy Impact

Assessment (PIA).

d. Does the Department plan to extend this initiative beyond the registered traveler program to include all travelers?

Answer: TSA will await the results of the RT Pilot Program prior to making any decisions or recommendations regarding the implementation of a larger scale program, including what costs, if any, would be incurred by those passengers who wish to participate in a future phase of the program.

e. Reports indicate that TSA plans to deploy RFID-tagged boarding pass in several African nations as part of its "Safe Skies for Africa Initiative." In what countries, and when do you expect this effort to commence? Does TSA have plans for use of RFID-tagged boarding passes in other areas, and if so, please identify those and the respective implementation schedules?

Answer: The Department of Transportation is the lead for the Safe Skies for Africa Program. However, TSA is providing technical expertise to support a government initiated RFID technology demonstration project initially at Nairobi's Jomo Kenyatta International Airport in conjunction with Kenya Airways. The demonstration will include a limited number of Kenya Airways' international departure flights for which checked baggage would be labeled with RFID baggage tags to support international bag matching requirements. In addition, the passengers for these same flights would be provided an RF-enabled boarding pass able to allow identification of these passengers at a key location within the airport to support verification of these passengers going to the proper flight departure area (i.e., international verses domestic gate areas). DHS is not aware of any other planned uses of RFID technology for the Safe Skies for Africa program.

8. The Department has planned various technology-based tracking and security initiatives that will result in large amounts of collected data.
   a- What are the Department's plans for the information technology and network systems necessary to manage this data?

Answer: DHS is consolidating its IT infrastructure and has organized these efforts around a portfolio management structure. This defines the DHS infrastructure mission space and identifies the associated technologies and investments that support that mission. An Infrastructure Transformation Program Office has been established and is developing and implementing a strategy to achieve the foundational work required to support the interoperability needs for legacy applications, as well as the new data collections resulting from enhanced screening, targeting, and intelligence initiatives. The basic premise of the strategy is to consolidate IT infrastructure (i.e., one network, consolidated data centers, unified

operations, one email) so as to provide an interoperable, sustainable, and scalable environment. This strategy is being developed and implemented following System Development Life Cycle processes and CPIC Investment Management requirements.

b. As data collected via RFID technology is transferred to databases, those databases could contain an extended digital diary of an individual's (both U.S. and foreign) travels to and from the U.S.

   i. How will this information be handled, shared and protected?

      As a matter of policy, the Department of Homeland Security has extended the provisions of the Privacy Act of 1974 to all persons: U.S. citizens, legal permanent residents, and foreign nationals. As a consequence, any information that is collected and maintained on an individual's travels to and from the U.S. will be handled in a manner consistent with the Privacy Act. Information is shared only when there is a bona fide "need to know" in furtherance of official business. In addition to complying with Privacy Act requirements, information sharing occurs subject to specific memoranda of understanding written to ensure that such sharing is accomplished in a manner that protects privacy. DHS employees are trained on the privacy and security of handling personal information. And the DHS Chief Privacy Officer conducts audits and oversees the entire process to ensure that the privacy of individuals is respected in all DHS initiatives.

      1. To what extent will this data be subject to other efforts like data mining, which for this question is defined as the application of database technology and techniques to discover hidden patterns or relationships in data?

      Because we live in an age of uncertainty brought upon us by terrorists who seek to harm the United States in ways that were heretofore unimaginable, it is important that DHS have available to it all necessary tools to protect the security of the United States. Technology allows us to uncover information quickly that might otherwise take months if not years to discern. That information may be critical in the war against terrorism.

      To the extent that DHS maintains information within the agency, the Privacy Act permits its use as long as there is a need for access to the record in the performance of employees' official duties. As noted in the previous answer, DHS employees are trained on their responsibilities under the Privacy Act and the internal use of information is subject to strong audit and oversight controls by the

Chief Privacy Officer for DHS, whose responsibility includes ensuring that technology is employed in ways that maximize rather than minimize privacy. To the extent that any data mining occurs, the resultant information will be handled in strict compliance with federal law and subject to strict scrutiny by the DHS Privacy Officer.

Accenture

9. The Department recently announced that it has awarded a contract to Accenture to implement the next generation of the US-VISIT program. Secretary Powell indicated in his testimony before the House Judiciary Committee on April21, 2004 that travelers under the Visa Waiver Program, which will include biometric data embedded in passports, will be included in the US-VISIT system. In addition, the Department has indicated plans to also embed U.S. passports with biometric information.
   a. To what extent has the Department given Accenture objectives or directives in addressing the privacy and data security issues connected with the use of biometric information? Please provide any documentation associated with these directives.

   Answer: As part of any application development activity, including that for biometrics, the Accenture integrator as well as any other DHS contractor supporting US-VISIT functionality is being overseen by the US-VISIT staff, and is following our policies and processes, such as our System Development Life-Cycle (SDLC). Information security and privacy is a key component of our SDLC.US-VISIT has instituted a process that requires the concurrence of the US-VISIT Privacy Officer at each SDLC gateway review .

   The US-VISIT Privacy Officer oversees and conducts Privacy Impact Assessments (PIAs) for the program as a whole and ensures that technology systems and system owners adhere to and update System of Record Notices (SORN) and other OMB and regulatory and legislative guidance as to privacy and information security.

   b. Will the technology and information infrastructure created by Accenture be expandable beyond the US-VISIT program to include or be compatible with any other government security initiatives that include data gathering?

   Answer: The US-VISIT Program Office has initiated its strategic planning effort and is being supported in this effort by Accenture and the other members of the Smart Border Alliance. The plan is taking the full immigration and border management enterprise into consideration, and principal stakeholders across organizations and agencies are included in the effort. Considering the challenges and requirements associated with

each stakeholder in the enterprise will ensure the plan provides a scope of implementation, subject to policy decisions and funding availability. Both the technology infrastructure and the information infrastructure will be oriented toward open and modularized services, with an emphasis on standards that would enable sharing across multiple government agencies involved in the immigration and border management enterprise.

Biometric Transportation Worker Identification Credential

10, Recent reports indicate that TSA has begun testing the Transportation Worker Identification Credential — a type of biometric smart card — in Florida and California to enhance security processing of transportation workers frequently crossing the border, and that the TSA will soon begin a pilot program in Canada.

a. What were the results of the pilot testing in Florida and California, including whether there were particular challenges to implementation?

Answer: TSA released a Request for Proposal (RFP) on May 10, 2004, to support the prototype phase and issued an award to Bearing Point in August 2004. Preparations are being made to conduct the Prototype Phase at select multi-modal transportation sites in three pilot regions: Florida, West Coast (Los Angeles/Long Beach), and East Coast (Philadelphia, Delaware, New Jersey, and Long Island, NY). The goal of the Prototype Phase is to assess the performance of the proposed TWIC identity management business processes (including sponsorship, enrollment, establishing a claimed identity, completing a threat assessment, secure card production, card issuance, and operational use for physical and logical access), and to develop a recommendation with respect to implementation. The Prototype Phase is scheduled to last approximately seven months. DHS would be pleased to apprise Congress of our findings upon the conclusion and review of the Prototype Phase.

b. Does this card rely on RFID technology to store and transmit biometric data, and if so, what specific technological, management and other protections in place to ensure the privacy and security of the data?

Answer: Decisions regarding the implementation of TWIC are pending a review of information being collected in the TWIC Prototype Phase. While RFID technology is not required for the main Prototype work, a pair of complementary studies is incorporating it.

During the TWIC Prototype Phase, the TWIC card itself will not utilize RFID technology. Rather, it will use the ISO 7816 smart card's contact integrated circuit chip (ICC) to store securely the reference biometric templates for 1:1 identity verification. The TWIC Program does not plan

to store biometric images on the credential.

c. Are the smart card and the TWIC program compatible or fully integrated technologically and logistically with other biometric security initiatives employed or planned by the Department?

Answer: One of the TWIC program's goals is to develop an identity management system that is interoperable with a broad range of existing government and private security initiatives. Therefore, TWIC is being designed to be fully compliant and compatible with the GSA Government Smart Card Interoperability Specification (GSC-IS), the OMB Federal Identity Credential Committee (FICC) policy, and the Government Smart Card Interagency Advisory Board (IAB) and Physical Access Interagency Interoperability Working Group (PAIIWG) recommendations, as well as with applicable government and industry standards. This approach supports and enables the use of available GOTS (Government off-the-shelf) and COTS (Consumer off-the-shelf) technologies and allows TWIC to maintain a non-proprietary environment in its development.

CAPPS II

11. In September 2003 and January2004, I wrote to the Department about its CAPPS II program and asked questions related to privacy, security and efficacy. To date, I have not received answers to these questions. But in February 2004, the GAO released a report critical of the Administration's handling of the Computer-Assisted Passenger Screening System ("CAPPS II"). That report indicated that TSA had not addressed seven of eight key issues identified by Congress, including privacy concerns. Specifically, GAO found weaknesses in TSA's ability to assess data accuracy, allow for corrections in data, address data security issues, prevent identity theft from thwarting the program, address potential hacking problems, ensure the effectiveness of search tools, and provide for appeals. GAO also raised questions about TSA's scheduling and cost plans.
    a. What is the status of TSA's efforts to remedy these weaknesses?

Answer: After a review of airline passenger prescreening programs, and bearing in mind GAO's findings, TSA has developed a new program, called Secure Flight, for pre-screening domestic airline passengers in order to enhance the security and safety of domestic airline travel. DHS believes that once a reasonable amount of testing has been conducted, it will be in a far better position to address and resolve the concerns raised by the GAO report.

Under Secure Flight, TSA will assume the process for comparing domestic airline Passenger Name Record (PNR) information against records contained in the consolidated terrorist watch list maintained by the Terrorist Screening Center

(TSC), which includes the No-Fly and Selectee lists. TSA will also apply a streamlined subset of the existing CAPPS I rule sets to PNRs, and build a "random" element into the new program to protect against reverse engineering by those who would seek to defeat it. The new Secure Flight program will improve the efficiency of the pre-screening process and reduce the number of people selected for secondary screening.

In accordance with Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), TSA began testing of Secure Flight on November 30, 2004 by utilizing all appropriate records in the consolidated and integrated terrorist watch list maintained by the Federal Government and comparing against historic PNR information submitted by air carriers pursuant to a Final Order issued on November 15 (69 Fed. Reg. 65619). Testing is on schedule and expected to conclude in February 2005. In the meantime, TSA is refining planned passenger redress mechanisms, working with the National Archives and Records Administration (NARA) to identify an appropriate short data retention period for test data, drafting a regulation for an operational Secure Flight Program, and is meeting regularly with privacy advocates and air carriers to answer question and address concerns expressed about the testing and operation program.

Secure Flight will be continuously monitored to identify and delete factors that do not contribute to the effective and efficient assessment of terrorist risk. Additionally, the TSA Civil Rights and Privacy Offices, and when appropriate the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office, will be involved in redress process for the new program. The full protection of privacy and civil liberties remains a core principle for any passenger pre-screening system.

b. Please provide a date certain when the Department will answer the September 30, 2003 and January 21, 2004 letters.

Answer: DHS seeks to respond quickly to inquiries from Congress in order to facilitate Members' exercise of their oversight responsibilities. In this case, the complexity of the questions and the evolving nature of the original CAPPS II proposal required additional response time to ensure that our answers are as accurate as possible. We are working diligently to deliver a formal response to your letters.

EU Agreement

12. On May11, 2004, the U.S. and EU issued "Undertakings" reflecting how the U.S. Customs and Border Patrol (CBP) will handle, process, store, and retain certain Passenger Name Records (PNRs) of EU passengers.
    a. Will CBP's treatment of EU-passenger data differ from the treatment of

U.S. resident PNRs during airline screening programs like CAPPS II and if so, please describe those differences and the reasons.

Answer: CBP's automated system applies the same set of risk assessment criteria in the screening of PNRs derived from flights between the U.S. and EU, regardless of the citizenship of the international passenger.

b. The "Undertakings" indicate that EU passenger PNRs may not be transferred to CAPPS II for testing unless testing of domestic airline data has been authorized. Reports earlier this year indicated TSA considered efforts to force airlines to release passenger data.
   i. What are the Department's plans for testing domestic airline data?

Answer: On September 21, 2004, TSA announced the release of three documents to enable the testing of Secure Flight.

- A Privacy Impact Assessment (PIA) that explains in detail the handling and flow of personal information and the protocols and privacy protections that are built in to Secure Flight to protect passengers;

- A System of Records Notice (SORN) that describes TSA's statutory authority and procedures to collect data and use it to conduct a test of Secure Flight; and

- An Information Collection Request (ICR) that requests approval from the Office of Management and Budget (OMB) to collect airline PNRs for testing purposes. This document includes a proposed order to all domestic airlines requiring them to provide PNRs for passengers who flew in June 2004. OMB has subsequently approved the collection of this data.

Following TSA's review and incorporation of changes to the order as a result of public comments received during the 30-day comment period, TSA issued a final order on November 15, 2004 requiring U.S. air carriers to provide one month's worth of historic PNR information to TSA to begin testing the Secure Flight platform. The order specifically enabled air carriers to elect to exclude PNRs that had flight segments between the EU and the United States. Domestic airlines efficiently complied with the order and began the transfer of data in time to allow testing of Secure Flight. On November 30, 2004, TSA began using historic PNRs from June 2004 to test the Secure Flight computer platform at full load and full speed. The testing phase is important to determine system capabilities, capacity and selection rates. Testing is on schedule and expected to conclude in February 2005.

Separate from the testing described above, TSA will also conduct a very limited test to determine whether commercial data will prove useful for reducing the number of false positive watch list matches, or for identifying

passenger information that is incorrect or inaccurate. TSA will use data that is already commercially available from data providers that currently support fraud protection efforts of industries where near-instantaneous validation of identity is critical for doing business, such as the banking, home mortgage and credit industries. TSA does not assume that commercial data is indicative of passenger intent.

In the Homeland Security Appropriations Act, 2005 (Pub,L. 108-334, Section 522(d)), Congress mandated that prior to commercial data testing, TSA was required to develop measures to assess the impact of using commercial data on aviation security and that GAO review those measures before commencement of testing. Strict adherence has been taken as to submission of those performance measures and a Request for Proposal (RFP) was publicly issued on January 21, 2005. GAO will continue to evaluate TSA's development of performance measures throughout the test phases. The limited commercial data testing is expected to conclude in April 2005.

TSA's testing of the use of commercial data is governed by strict privacy and data security protections, including strict prohibitions on the use of any passenger-provided information by commercial data providers. TSA does not incorporate the use of commercial identification authentication into Secure Flight unless testing confirms that:

- It enhances security;
- It does not result in inappropriate differences in treatment of any category of persons; and
- Robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain inappropriate access to or use passenger personal information inappropriately.

In addition, TSA will not incorporate the use of commercial data into the Secure Flight Program prior to the completion of testing, assessment of results, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Results of the testing, both of the comparisons of PNR information against names in the consolidated terrorist watch list and the use of commercial data, will be as publicly transparent as possible without compromising national security. Testing and eventual implementation will be governed by strict privacy protections including passenger redress procedures, data security mechanisms, and limitations on use.

iii. Does the Department plan to mandate that airlines turn over

passenger data, and if so, under what authority and when?

Answer: TSA has broad authority under 49 U.S.C. 40113(a) to issue orders necessary to carry out its functions, including its responsibility to provide for the security screening of passengers under 49 U.S.C. 44901(a). TSA also has authority to identify and undertake research and development activities necessary to enhance transportation security under 49 U.S.C. 114(f)(8) and to develop a successor system to CAPPS under 49 U.S.C. 44903(j)(2). As discussed in the answer to Q1798, on November 15, 2204, TSA issued an order requiring airlines to provide PNRs for testing of Secure Flight.

Based on the results of testing using historical PNR data, TSA will likely issue a regulation requiring airlines to provide certain standard PNR data to TSA for all domestic flights.

iv. What privacy and data security protections would apply during that testing phase?

Answer:

TSA believes it has taken action to mitigate privacy concerns by designing its next generation passenger prescreening program to accommodate concerns expressed by privacy advocates, foreign counterparts and others.

1. Under the Secure Flight testing phase, TSA will not require air carriers to collect any additional information from their passengers than is already collected by such carriers and maintained in passenger name records. Testing of the Secure Flight program will compare historic PNR information from the month of June, 2004, submitted by air carriers, against records contained in the consolidated Terrorist Screening Database (TSDB), to include the No-Fly and Selectee lists, in order to determine system capabilities, capacity and selection rates.

   Secure Flight will protect personal privacy because of its limited retention period for data collected and used.

   Separately from the testing described above, TSA will also conduct a very limited test to determine whether or not the use of commercial data could assist with identifying passenger information that is incorrect of inaccurate or assist with resolution of false positive matches. TSA will use data that is already commercially available from aggregators that currently support industries where near-instantaneous validation of identity is critical for doing business, such as the banking, home mortgage and credit industries.

TSA's testing of the use of commercial data will be governed by strict privacy and data security protections, including strict prohibitions on the use of any passenger-provided information by commercial data providers. TSA will not incorporate the use of commercial data until testing confirms that:

- It enhances security.
- It does not result in inappropriate differences in treatment of any category of persons.
- Robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain inappropriate access to or use passenger personal information inappropriately.

v. Does the Department plan to address the CAPPS II weaknesses identified in the February 2004 GAO report prior to testing any passenger data?

Answer: After a review of airline passenger prescreening programs, and bearing in mind GAO's findings, TSA has developed a new program, called Secure Flight, for pre-screening domestic airline passengers in order to enhance the security and safety of domestic airline travel. DHS believes that once a reasonable amount of testing has been conducted, it will be in a far better position to address and resolve the concerns raised by the GAO report.

Vermont-New York Cooperation

13. On May 25, 2004, the FBI announced that police in Vermont and New York will soon be able to check suspects instantly against federal terrorist watch lists under a first-of-its-kind, FBI-coordinated program. Some may be surprised that, 1,000 days after 9/11, this critical information-sharing program is still in its infancy. The Department of Homeland Security, however, has the Law Enforcement Support Center (LESC), which works 365 days a year, 24 hours a day with state and local law enforcement in all 50 states. That center works over the NLETS network--the backbone communications for local law enforcement--.to respond immediately to queries from local law enforcement officers in the field. Those officers are given results from searches of not only a criminal alien and absconders database but also a search of the National Crime Information Center (NCIC). Was the Department of Homeland Security involved in or consulted about the development of the FBI program? Should it have been?

Answer: The FBI did not consult with the Department of Homeland Security (DHS) on the development, deployment, and public release of this program.

This information is currently available through RISS, LEO, and NLETS as well as through the DHS Homeland Security Information Network (HSIN), which has been supplied by DHS to all states and many major cities. In the immediate near term, HSIN will also be extended to the county level and to additional cities. In addition, an HSIN Secret-level network structure will be in operation by the end of this year and will provide more robust information access than is currently available through Sensitive But Unclassified technologies.

The Law Enforcement Support Center was established primarily to provide a direct interface for law enforcement to obtain valid information on the immigration status and legitimacy of persons currently in the U.S.. Given that law enforcement officers have approximately 15-30 minutes to make a catch/release decision in the field environment, it was critical for DHS to provide a method to immediately address this requirement while other methods and technologies are developed.

In addition, as DOJ and DHS continue to improve the compatibility of RISS, LEO, and HSIN over the next few months, access to this information will be simplified, which may obviate the need for this separate FBI program.

Immigration Reform

14. In January, the President gave a speech before an invited audience of Hispanic leaders at the White House, offering a general plan for immigration reform, I believed the general outline had some merit, although it left important questions unanswered. As a result, I wrote the President and asked for those details, in the form of a legislative proposal Congress could consider, Unfortunately, no further details have been forthcoming. (A) What specifically does the President want Congress to do in the area of liberalizing our immigration laws?

Answer: On January 7, 2004, the President announced principles in creating a new temporary worker program that would match willing foreign workers with willing U.S. employers when no Americans can be found to fill the jobs. We look forward to working with Congress to develop legislation that incorporates the best ideas for the American worker and our foreign visitors. Through the principles outlined by the President, the best course to the end goal of opportunity, security, safety, compassion, jobs and growth can be achieved.

(B)I know that many Republicans in Congress and elsewhere noisily denounced the President's overtures on immigration, and I have noticed that the President has been silent about the topic in recent months. Has the President retreated from his immigration policy under pressure from fellow conservatives?

Answer: No, the President continues to call on Congress to develop immigration legislation based on the principles he has talked about and advocated for since his January 7, 2004 speech.

Immigration Reform

In January, the President gave a speech before an invited audience of Hispanic leaders at the White House, offering a general plan for immigration reform, I believed the general outline had some merit, although it left important questions unanswered. As a result, I wrote the President and asked for those details, in the form of a legislative proposal Congress could consider, Unfortunately, no further details have been forthcoming. ... (C) Many Mexicans - understandably unfamiliar with the American political process -believed that US immigration policy had changed after hearing of the President's remarks. As a result, we have seen numerous press reports about the increased flow of Mexicans across the border, and an increased number of fatalities in the Arizona desert. What steps are you taking to reduce the human cost of this misunderstanding among the Mexican people? Are you in contact with the Government of Mexico about this matter?

Answer: In September 2003, a U.S. Immigration and Customs Enforcement (ICE) Task Force, known as ICE Storm, was assembled to combat violent crime in the Phoenix metropolitan area, which had reached an unprecedented level with murder, kidnapping, extortion, and other crimes related to human, drug, currency and weapons smuggling. The city of Phoenix and its outlying regions had been invaded by smuggling organizations involved in the indiscriminate kidnapping of groups of undocumented aliens, with the proclivity for shootings and highway carjacking of smuggling loads, which was indicative of smuggling organizations' total disregard for life and property and a new level of criminal behavior.

ICE, under the auspices of the BTS Arizona Border Control Initiative, has addressed this public safety issue by partnering with other stakeholders in the federal, state, local and foreign law enforcement and intelligence communities. ICE, with extensive immigration, customs and money laundering expertise has had a significant impact on the criminal organizations engaged in this illicit activity through the vigorous application of money laundering and other federal and state statutes to deprive smuggling organizations of the criminal proceeds, disrupt their operation and decimate the organizational hierarchies in the United States and abroad.

Since the inception of ICE Storm, 311 defendants have been prosecuted for human smuggling, kidnapping/hostage taking, money laundering, narcotics and weapons violations. Over $5.5 million in currency and 157 weapons have been seized. During a press conference in January 2004, Phoenix Police Chief Hurtt attributed a 30% decrease in the previous calendar quarter of homicides in Phoenix to Operation ICE Storm.

First Responders

15. I have introduced S. 315, the First Responders Partnership Grant Act, which would authorize *$4* billion annually to support our State and local public safety officers in the war against terrorism, (A) Do you support this legislation?

Answer: The Department of Homeland Security supports the $3.6 billion funding level outlined in the President's FY05 budget. The Department is currently reviewing this piece of legislation, and will hopes to provide its comments to the Committee in the near future.

(B) Considering the severe resource problems among the nation's first responders that the Hart-Rudman Commission, the Council on Foreign Relations, and other nonpartisan organizations have pointed out, how can you *not* support this legislation?

Answer: The Department of Homeland Security believes the funding levels requested by the Administration have been sufficient to address essential homeland security priorities. Further, many states and localities are still assessing their homeland security priorities. The Department is currently reviewing this piece of legislation, and will hopes to provide its comments to the Committee in the near future.

Arar Case

16. I understand that the DHS Office of Inspector General is investigating the case of Maher Arar, a Canadian citizen who was deported by the U.S. to Syria. Mr. Arar claims that be was tortured during the ten months he was detained by Syrian authorities,

The Torture Convention prohibits sending an individual to a nation where there are substantial grounds to believe he would be subject to torture. U.S. law requires the withholding of deportation where it is more likely than not that the person will face torture in the country to which he is sent, President Bush himself has pointed to a long history of state-sponsored torture in Syria. Will the OIG investigation address Mr. Arar's claim that he told U.S. officials that he feared torture at the hands of Syrian officials before being deported to Syria? If not, why not?

Answer: I have referred the Committee's question regarding the OIG

investigation of Maher Arar to the Inspector General, and asked that he respond directly to the Committee.

Controls on "For Official Use Only" Information

17. In a May 11, 2004 management directive, the Department imposed several classification-like controls on sensitive but unclassified information that is "for official use only" (FOUO). These controls include a "need-to-know" provision and a non-disclosure agreement.

    a. Why is a non-disclosure agreement for unclassified information deemed necessary?

    Protecting sensitive but unclassified (SBU) information is an essential element of ensuring the nation's homeland security. DHS employees are entrusted with vast amounts of SBU information every day, and regularly and rightfully share it with other federal agencies and our partners in state and local governments, tribal officials, and the private sector. For instance, the information DHS shares might reveal the Department operations and functions, certain vulnerabilities in the country's infrastructure systems and facilities, and the nature of border and immigration protections. If this information were to fall into the wrong hands, damaging consequences may well be the result. While sharing information at unprecedented new levels, DHS must also protect that information.

    DHS requires contractor personnel to sign non-disclosure agreements (NDA). The use of such NDAs is commonplace in the interactions and relations between governmental organizations and commercial companies. In addition, DHS believes that they are useful instruments to promote awareness of the standards used in designating and handling sensitive but unclassified information (SBU).

    DHS formally required federal employees to sign an NDA. As of January 6, 2005, this requirement is no longer in effect. The NDA was designed as an interim measure to efficiently and effectively educate employees on the responsibilities associated with handling SBU information. Pursuant to the revised policy, the Department is implementing an education and awareness program for the safeguarding of SBU information.

    b. Are you aware of any other federal agency that routinely requires non-disclosure agreements for unclassified information?

    NDAs are commonplace in the interactions and relations between federal agencies and commercial companies.

    c. Does the non-disclosure agreement limit disclosures to Congress in any

way?

No. Section 15 of the non-disclosure agreement states that signing the NDA "does not bar disclosures to Congress."

d. Please provide a copy of the non-disclosure agreement.

A copy of the non-disclosure agreement is attached.

18. Designating information as FOUO under the May 11 directive triggers a series of security measures that may incur both operational and financial costs, e.g. by restricting information sharing, requiring secure document storage and transmission, etc.

a. What procedures are in place to ensure that information is not improperly or unnecessarily designated as FOUO?

The DHS Management Directive provides guidance as to what constitutes sensitive information. Indeed, it specifically designates certain categories of information as sensitive. For example, sensitive information includes that which could result in physical risk to DHS personnel, reviews or reports disclosing facility or infrastructure vulnerabilities, or information regarding assets and systems that, if disrupted, would significantly threaten public health, safety, and the economy. It is therefore necessary to safeguard critical information from exploitation by adversaries of the United States.

Designating information as sensitive, however, does not impose additional operational or financial costs, restrict information sharing beyond the need-to-share/need-to-know concepts, require secure document storage and transmission, or require the application of any other additional resources or security measures not already in place in a common office environment or within a Government information system. In addition, as the Management Directive indicates, the FOUO designation does not exempt information from release under the Freedom of Information Act (FOIA), or from disclosure to Congress or other authorized recipients.

To educate its employees and contractors regarding the proper handling and designation of sensitive information, the Department is actively providing education and awareness training. All new employees and contractors receive a security orientation regarding sensitive information. In addition, the Department is implementing an education and awareness program specifically for the safeguarding of SBU information. All employees and contractors will participate in classroom or computer-based training sessions designed to educate them on what constitutes SBU information and the standards for handling and disseminating it. Completion of this

training will ensure that each employee and contractor has the knowledge he or she needs to recognize and handle SBU information responsibly. Finally, the Office of Security Customer Service Center is available to address any specific issues or concerns that arise.

b. Whose responsibility is it to ensure that excessive restrictions on information are not imposed?

The Department of Homeland Security is committed to sharing information with the appropriate personnel within the Federal Government, as well as state and local government officials and private-sector individuals. Indeed, the Secretary has indicated that the sharing of information is a cornerstone to the DHS approach in protecting the homeland. The revised Management Directive and DHS policies do not impede the legitimate flow of information to those who require it.

It is incumbent upon the individual who designates the information as FOUO to follow the guidance provided in the Management Directive (as referenced above) regarding the proper use of the FOUO designation. Each DHS employee has the responsibility to designate information as FOUO only in proper circumstances. Indeed, DHS guidance indicates that designation of information as FOUO should not be used for unreasonable or illegitimate purposes, such as concealing government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.

To ensure that they have the knowledge required to recognize and handle SBU information responsibly, all DHS employees will participate in classroom or computer-based training sessions designed to educate them on what constitutes SBU information and the standards for handling and disseminating it.

Critical Infrastructure Information and FOIA

19. The Homeland Security Act of 2002 provided a significant new exemption to the Freedom of Information Act for "critical infrastructure information" voluntarily submitted by industry. The proffered justification for this exemption was the need to encourage industry to share such information with

government. An interim rule governing the Protected Critical Infrastructure Information (PCI]) Program" was published on February 20,2004. No final rule has yet been published.

a. Is the Department accepting PCII submissions under the interim rule?
ANSWER: Yes

b. If so, please respond to the following questions:

i. How many submissions of CII has the Department received from industry since the new exemption was enacted?

ANSWER: As of October 20, 2004, DHS has received 30 such submissions which, if validated as PCII, come within the CII Act's nondisclosure provision and become exempt from release under FOIA Exemption 3.

ii. How many, if any, of the new submissions would have been subject to disclosure under the Freedom of Information Act if the new exemption had not been enacted?

ANSWER: 22 of the submissions have been validated as PCII, 7 have been rejected, and 1 is in process as of October 20, 2004. The Government believed prior to passage of the CII Act that existing FOIA exemptions under b4 were sufficient to protect almost all voluntarily provided critical infrastructure information. Industry was concerned, however, with the strength of the existing exemptions and the consistency with which they are applied across the Government. They sought the additional protection of a statutory exemption to FOIA for such information. We believe that many of the submissions would have been exempted from FOIA under exemptions other than the PCII statutory exemption, but due to the statutory exemption, we have not been called upon to make that evaluation.

The CII Act of 2002 provides the statutory exemption to the Freedom of Information Act for critical infrastructure information voluntarily shared with DHS. A key element of the PCII Program, which implements the CII Act, is to let the private sector know whether their information qualifies for the FOIA exemption before DHS uses the information and incorporates the document into the Governments files. If the information does not qualify for the exemption the submitter has the option of withdrawing the submission or allowing DHS to retain it without CII Act protections.

iü. How many times has the Department invoked the new CII exemption to deny a FOIA request?

ANSWER: To date there have been two FOIA requests for PCII related

documents. The first did not involve PCII material and so the exemption under the CII Act's nondisclosure provision did not apply. The second is in process at the present time and will invoke the statutory exemption protection for any PCII material encompassed by the request.

iv. To what extent has the new FOIA exemption had the intended effect?

ANSWER: We believe the protections offered by the CII Act are viewed favorably by the private sector. We believe the limited number of submissions made to date is largely the result of two factors:

-- the fact that we are operating with an interim rather than a final rule adds an element of uncertainty to the program. The final rule should be issued in early 2005.
-- the PCII Program will be most effective when coupled with requests to the private sector to provide information. DHS has a number of efforts underway in this regard at the moment and PCII is a part of them.

In addition, there are a number of special projects underway to utilize the PCII Program:

-- The National Cyber Security Division is collecting cyber related information through the US CERT portal. In the near future entities will have the option to make such submissions under the PCII Program.
-- The Infrastructure Coordination Division (ICD) is working with the Electric Power ISAC to receive outage reports under the PCII Program.
-- ICD is also working with the Trucking ISAC to receive incident reports under the PCII Program.
-- Entities responding to data calls as part of the National Infrastructure Protection Plan and as part of Project SENTINEL will have the option to submit information under the PCII Program.

In summary, while there have been a limited number of submissions under the CII Act to date there are a significant number of efforts underway to substantially increase the amount of information submitted for PCII protection.

b. If the Department is not accepting PCII submissions under the interim rule, when will the Department issue a final rule, and when will that final rule go into effect?

ANSWER: Submissions are being accepted under the interim rule. The final rule is expected to be issued in early 2005.

c. The interim rule does not place any time limits on the verification process for PCII information that is voluntarily submitted to the Department This will

have the effect of granting PCII status to such information for an indefinite period of time.

i. In the final rule on PCII, will the Department include a time limit for Department staff to verify that PCII submissions are legitimately related to critical infrastructure protection?

ANSWER: The final rule is still being developed, and we are considering a number of questions, to include whether to establish specific time periods for making validation determinations. The Program Manager will be responsible for establishing reasonable metrics for the Program based on the work load. To date, validation decisions are generally made within one working day. If additional information is needed from the submitter to complete the validation determination, additional time is required.

ii. What level of staff and financial resources will be appropriated by the Department to the PCII verification process?

ANSWER: The authorized staffing level for the PCII Program Office is 12. The FY 05 appropriation for the PCII Program is $3.8 million.

U.S. Senator John Cornyn
Questions for The Honorable Tom Ridge
Secretary, U.S. Department of Homeland Security
Senate Committee on the Judiciary Hearing on June 9, 2004
"DHS Oversight: Terrorism and Other Topics"

1. In your opinion, wouldn't a temporary worker program reduce the difficulties you face in securing the homeland?

ANSWER: The Temporary Worker Program, as currently contemplated, would certainly provide an opportunity for the Department of Homeland Security to increase national security and public safety. It is presently estimated that there are approximately 8 million undocumented aliens living and working in the United States. Depending on how the final legislation is crafted, a number of people in this group would have an opportunity to regularize their status on a temporary basis, which will allow us to know who these people are, and where they reside. Additionally, capturing this data enables us to conduct background security checks on these individuals who already reside in our country. The Temporary Worker Program also contemplates a process for individuals who are overseas and would like to come to the United States on a temporary basis to fill a job for which there is a shortage of United States workers. This provision would provide the United States Government the opportunity to screen individuals applying for visas abroad. This screening would keep those who would wish to do us harm out of the country, yet would offer foreign nationals located abroad an opportunity to enter the Unites States legally with a job offer from a company in the United States.

2. While I appreciate the information your Department provided in response to my November 21, 2003 letter, I am still concerned with the slow progress of deportation of criminal illegal aliens. With almost 400,000 alien absconders and 80,000 of those have been convicted and served prison time, only 25,000 of which having been entered into NCIC, the number still unaccounted for continues to alarm me. What changes do you still need to make to account for and deport these criminal aliens?

Answer: We have taken several steps to identify more efficient and effective ways to address this problem.

The 80,000 represents a count of unexecuted final orders among criminals. At least one-half of these are incarcerated in state and federal prisons, in our detention facilities, or are on orders of supervision.

All identified criminal aliens are not necessarily qualified for entry into NCIC. Previously, immigration requirements were more restrictive than those required by the Criminal Justice Information Services (CJIS) for entering cases into NCIC. For example, all cases being presented for input into NCIC needed to be able to qualify for federal criminal prosecution, which includes extensive documentation and other evidentiary

requirements. This threshold is well above and beyond that which is required by CJIS. As long as ICE has a valid warrant issued, can positively identify the individual and agrees to respond to each NCIC hit (we are discussing fugitive aliens only in this scenario), then the case should be eligible for inclusion into NCIC. Another underlying factor is that most state and local law enforcement agencies do not recognize fugitives with "administrative" warrants lodged against them as criminal fugitives.

We have taken several steps forward in decreasing the number of alien absconders. Currently we have 18 teams deployed nationwide and during the first year of the ICE National Fugitive Operations Program (NFOP), we made over 8900 arrests of which 7200 were fugitive aliens. Of the 8900 arrests, 3738 (42%) were criminal aliens and 6015 (68%) have been removed from the U.S. In FY05, funding for 30 additional fugitive teams has been appropriated and once deployed these additional teams will significantly increase the apprehension rate of fugitive aliens.

We have also implemented and are refining how we receive and distribute leads. Currently we are tapping into existing DHS databases to locate "encounter" matches, which have led to the identification and location of fugitives. These initiatives include interfacing information contained within National Automated Immigration Lookout System (NAILS) and Deportable Alien Control System (DACS), and interfacing information collected from the Citizenship and Immigration Services (CIS) Administrative Service Centers and leads generated by the Interagency Border Inspection System (IBIS).

We are also experiencing improved success with information sharing with other federal agencies. Since October 2002, we have executed thirty (30) DACS information-sharing agreements -- Interconnection Security Agreements (ISA) or Memorandums of Understanding (MOU) – with federal, state and local agencies such as INTERPOL, the U.S. Attorney's Office, U.S. Marshal Service, Federal Bureau of Prisons, Federal Bureau of Investigation, U.S. Courts, Departments of State and Labor, and the New York State Department of Corrections and Parole.

As an example, we are cross-referencing our information with the Department of State in an effort to close out cases that no longer meet the definition of a fugitive. The Department of State, utilizing information from Foreign Service offices, is able to verify departure of aliens from the United States by verifying that they have returned to their home country. This case would no longer be considered a fugitive case for removal purposes.

We are also negotiating another twenty (20) information sharing initiatives, with federal, state and local governmental agencies, including the Social Security Administration, Department of Housing and Urban Development, the Chicago Police Department, and the City of New York Corrections Department. We are confident that once in place, these new agreements will provide more information that will lead to the apprehension of many fugitive aliens.
Furthermore, with the development of a Fugitive Operations Command Center (FOCC)

concept, ICE is confident that information sharing will increase and lead to increased success of the NFOP program. As designed, the FOCC will be the clearinghouse for the leads program. Leads from IBIS, NCIC, and the general public will go directly the FOCC for investigation and assignment to the field for action. This will lead to an increased number of apprehensions and case closures.

In addition to the initiatives mentioned above, which are designed to address the backlog of cases, we have implemented other initiatives to curb to the growth of the fugitive alien population, such as: Operation Compliance – Under this pilot in Atlanta and Denver, officers immediately detain aliens who have been ordered removed. Intensive Supervision Appearance Program (ISAP)– Implemented in eight cities this program uses tools such as electronic monitoring, home visits, and reporting by telephone to monitor aliens under proceedings but not in custody. ISAP is designed to maintain and better track those aliens who have been released to ensure their appearance at hearings and ultimately prevent them from absconding.

DETENTION AND DEPORTATION OF ASYLUM SEEKERS AND HAITIANS

There have been reports of ongoing inconsistent practices and policies of Immigration and Customs Enforcement Bureau on the detention of asylum seekers. There are guidelines for the parole of asylum seekers, but parole decisions sometimes seem to be based on other factors --such as availability of bed space, and local policies. When parole is denied, there is no process for appeal. Recently, Undersecretary Hutchinson acknowledged this problem of inconsistent parole policies for asylum seekers and said that it would be addressed.

3. As you know, the President has initiated a five year plan to reduce the average processing time for visas to 6 months. To date, even with approximately $100 million in funds ($20 million from fees, $80 million from appropriations) going to the USCIS for reducing the applications backlog, processing times in all categories are increasing. What measures is DHS working on to reverse this trend and realize the President's goal of a six month processing time?

ANSWER: USCIS has developed a 3-pronged approach to eliminating the backlog by implementing new management tools, employing better technology, and improving policies and procedures.

Management Tools:

The Backlog Elimination Plan was presented to Congress in June and USCIS has developed a tool to help each office manager measure progress against that plan.

Additionally, we have begun work on a staffing analysis that will allow us to right-size our offices to ensure that resources are appropriately aligned with our workload.

Further, employees, supervisors and managers at every level are encouraged to look critically at our day-to-day operations and then share their ideas about how we can improve business and eliminate the backlog.

Better Technology:

USCIS will ensure that long-term Backlog Elimination is sustained, customer service is improved, new fee-for-service business models are enabled, and a technology environment is deployed-all to support new processes and workflow aligned with DHS' mission and eGov standards.

USCIS has begun using systems support to identify low risk cases appropriate for fast-track processing. Also, since August, we have begun to store digital fingerprints, photographs and signatures and eliminate the redundancy associated with recapturing information. Technology-related initiatives like E-Filing, InfoPass, and providing case status online offer alternatives to standing in line at an office.

Improved Policies and Procedures:

USCIS-issued guidance will reduce unnecessary requests for additional evidence from applicants and ensure that, when possible, adjudicators make their decisions based upon the information included with the original application.

Further, USCIS has proposed a regulation removing the one-year mandatory expiration of Employment Authorization Documents (EADs). This would allow USCIS flexibility in issuing EADs for longer periods of time and reduce the burden placed on both customers and field offices to renew EADS every year.

Progress:

Since January, USCIS has reduced the backlog by about 2.3 million applications, reducing the number of cases that have been in process in excess of six months to a new low since the establishment of USCIS in March of 2003.

USCIS plans to build on this progress in the months ahead to make additional reductions in backlog levels and to eliminate the backlog in its entirety, in every office by the end of 2006.

4. The President's FY2005 budget request talks about the Department's intention to create a regional office structure to unify existing regional structures of DHS components, and harmonize Federal, State, tribal, local, and private-sector homeland security resources. What is the progress of this initiative and, specifically, what role do you envision these offices playing in DHS functions?

Answer: Following a baseline analysis that assessed the geographic, threat and infrastructure characteristics of seven component agencies with regional or field operations, initial recommendations regarding a regional concept of operations were crafted. Those recommendations are currently undergoing review by Department directorates and offices. A primary role of the Department of Homeland Security's mission is to lead the unified effort to secure America. The proposed establishment of the regional structure will support this mission by coordinating homeland security activities with federal, state, tribal, local and private sector stakeholders; integrating the core functions of DHS components within the regions; ensuring the effective and efficient delivery of DHS services to external stakeholders within the region; and strengthening the Department's ability to provide an integrated, rapid and robust response to contingencies and emergencies.

5. Several cities in Texas have been the beneficiaries of federal funds through the Department's Urban Area Security Initiative Grant Program. The program has been helpful to these high-threat, high-density cities, While I understand that some of the factors used to determine the distribution of these funds are considered highly sensitive or classified, I am concerned over what I see as possible disparities when Dallas is awarded funds and Fort Worth is consistently omitted. As you may know these two cities are very close in proximity and Fort Worth is home to 535,000 Texans, several key defense contractors, and other critical infrastructure that affects the entire Metroplex. Considering some of these compelling factors, why has this program not identified Fort Worth for funding?

Answer: As the Urban Areas Security Initiative program (UASI) is a discretionary program, the Secretary of Homeland Security has tasked the Information Analysis and Infrastructure Protection (IAIP) directorate within DHS to devise a formula to assist in the selection of the UASI participants. As such, a formula has been developed which takes into account factors such as threat, presence of critical infrastructure, population and population density. These factors are combined into a weighted, linear formula. A list of jurisdictions is matched against this formula and a rank-ordered list is produced. The Secretary will then select a number of jurisdictions to participate in the program.

In the Fiscal 2004 UASI program, three cities within Texas were selected to join the program: Dallas, Houston and San Antonio. The Core City for the Dallas Urban Area has been defined as the City of Dallas, and the Core Counties are designated as those entities within which the City of Dallas is located. The Core Counties for the Dallas Urban area are Dallas, Collin, Denton, Kaufman and Rockwall.

Although Tarrant County and/or Fort Worth are not designated as a Core City or Core County for the Dallas Urban Area, the State Administrative Agency (SAA) directed that the ensuing regional strategy should include Tarrant County (as well as DFW Airport and the DFW Hospital Council). These three entities have thus been non-

voting members of the UASI working group from the outset and have been active and fully participatory in the regional planning process. In addition, these entities will receive full consideration as funding allocations are made.

US. Senate Judiciary Committee
Hearing on "Oversight of the Department of Homeland Security: Terrorism and Other Topics"
June 16, 2004

Written Questions Submitted by Senator Russell D. Feingold to Homeland Security Secretary Tom Ridge

First Responders Abroad

I. At the Judiciary Committee hearing, you pledged to review Senator Lautenberg's bill, S.921, the State and Local Reservist First Responders Assistance Act of 2003.

(a) Do you support Senator Lautenberg's bill?

Answer: The Department of Homeland Security is currently reviewing this piece of legislation, and will hope to provide its comments to the Committee in the near future.

(b) If not, how do you propose replenishing our first responder resources as Reservists continue to be called upon to serve abroad for longer and longer periods of time?

Answer: The Department of Homeland Security is currently reviewing this piece of legislation, and will hope to provide its comments to the Committee in the near future.

Summer Travel

2. The Travel Industry Association of America is predicting a 3.4% increase in

leisure travel this summer. During the summer months, travelers are expected to make an estimated 275.4 million trips going fifty miles or more from home. As Americans prepare to travel the roads and skies this summer, there are security reports from the government warning of impending terrorist attacks. What specify initiatives to keep our citizens safe as they travel away from their communities to unfamiliar places where they don't know where to turn for information or guidance is the Department of Homeland Security considering or developing?

Answer: The mission of DHS is to lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. We will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce. Within DHS, the Transportation Security Administration has a mission to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. Keeping the traveling public secure is what we do.

TSA's security strategy uses a "system of systems" approach whereby each security ring contributes to TSA's overall security system but the overall system does not rely exclusively on any one component. These systems includes screening of passengers and their checked and carry-on baggage, the display of valid, government-issued photo identification, Federal Air Marshals, Federal Flight Deck Officers, hardened cockpit doors, and other enhanced security practices. Each security measure is designed to complement the efficiency and effectiveness of the others. The result is a system of enhanced security systems designed to provide a layered security that addresses a continuum of security threats with minimal impact on airline customers and operations, and on the free flow of commerce through the nation's commercial aviation infrastructure.

To address the increase in summer travel, TSA, in conjunction with the airports and major airlines, devised a strategy designed to help accommodate an anticipated 200 million air travelers nationwide between the Memorial Day and Labor Day weekends. The Aviation Partnership Support Plan (APSP) identifies numerous steps each partner can take to smooth the flying experience. The goal of the summer plan is to ease wait times at all the Nation's airports with particular emphasis on 25 pre-identified airports. Lessons learned at the 25 airports are being passed on to TSA's other 400-plus airports. The plan includes specific operational adjustments, such as improved techniques at passenger checkpoints and the deployment of airport and airline personnel to assist travelers. The plan seeks new efficiencies to keep wait times down by providing additional non-TSA personnel to manage the queue and assist passengers with divesture and putting personal items in X-ray bins. Individual airports have additional options to be decided on an airport-specific basis.

The APSP will be updated as new best practices are determined and shared

through inclusion in APSP updates. Additional updates to process, procedures, and guidelines will be implemented when properly tested to ensure security is not affected and customer service is enhanced. Our industry partners have committed to a wide range of initiatives from funding part-time non-screener support to the checkpoint and queuing lines, to assisting TSA with local outreach programs and providing more space surrounding the checkpoint for passengers to ready themselves for screening.

The plan also includes and an aggressive public information and education campaign. In late May, TSA launched its *Prepare for SUMMER Takeoff* campaign, building upon its successful Prepare for Takeoff theme that was launched to support the transition to Federal screening in late 2002. The goal of this campaign is to get passengers ready to go on their trip so that lines move quicker and passengers have a smoother experience. The campaign will educate passengers on the most common issues that are encountered at the checkpoints, including what can be packed in carry-on versus checked baggage, when to have their identification and boarding pass available, as well as issues that are germane specifically to the summer season. Our partners in the travel industry, including airlines, airports, travel agents, visitor and convention bureaus, and business traveler associations, to name a few, will all be critical in helping TSA to promote these important messages. Also, we will partner with the airports and online travel agencies to provide passengers with information on check-in and security wait times, parking situations, etc. to assist them with their trip and make it as hassle free as possible. In addition, TSA will conduct a robust summer travel public information promotion using TV, radio, and print outlets throughout the country to support the campaign. Finally, TSA will continue to update its website that is specifically designed to provide travelers with important information, to reflect any changes in security requirements and to respond to passenger input.

Data-Mining at DHS

3. In Section 201 of the bill creating the Department of Homeland Security, Congress authorized DHS to create a secure communications and information technology infrastructure that would be able to use advanced analytical tools like data-mining.

(a) What steps are you taking to ensure that Congress is informed of the development and deployment of these programs in a timely manner?

Answer: The Department's CIO works very closely with our Office of Legislative Affairs to ensure that all requests for information from Congress are responded to in a timely manner; to include our responses to any reporting requirements.

(b) What is being done to make sure that the privacy of the American people is respected as you develop systems using data-mining technology?

Answer: I believe that security and privacy are compatible goals for all DHS program initiatives and I have appointed a Chief Privacy Officer who shares this belief. DHS is committed to ensuring that the privacy of all people is respected in all our programs, including those that may use data mining technology. Consistent with federal law and policy, we require new or substantially revised programs to assess privacy impacts and to devise solutions that mitigate privacy risks. We require personal information to be handled in strict compliance with the Privacy Act and with fair information principles generally. DHS employees receive privacy training as well as training in information handling and security. And through her statutory responsibilities, the DHS Chief Privacy Officer ensures that DHS programs are established in ways that allow us to accomplish our important mission while enhancing privacy protections.

Training Centers

4. There are a number of technical colleges in Wisconsin that want to be designated as regional training centers for homeland security. Does DHS have any intention of making funding available for these schools to advance this initiative?
Answer: There are two means by which States can leverage existing training resources to address homeland security training needs. First, states may use State Homeland Security Grants to establish training programs at public safety training facilities and colleges. Allowable costs under this funding include the establishment of training programs within existing training academies, universities, or junior colleges as well as overtime and backfill costs associated with attendance at approved training courses. DHS guidance has encouraged the states to utilize existing training systems to maximize training delivery at the awareness and Performance-Defensive levels. This includes technical colleges within the state as a specific example.
Secondly, recent congressional appropriations have Competitive Training Grants to provide direct funding for to institutions such as the technical colleges cited in the question. One such institution, the Northeast Wisconsin Technical College, applied for funding under the FY 04 CTGP. This institution's application and those submitted by other applicants will be reviewed through a peer panel process based on the 5 criteria enumerated in the application. Awards will be made based on the consensus reviews performed by these peer panels and their subsequent recommendations. DHS has not requested continued funding for this program, as it lacks coordination with State efforts, and risks creating an expectation that direct Federal support will continue for an indefinite period of time.

Emergency Management Performance Grant

5. During a Budget Committee hearing earlier this year and in a follow-up letter dated

April 7, 2004,I indicated that Wisconsin emergency managers and homeland security officials are extremely concerned not only about the EMPG funding cut but also about the proposal to reduce from fifty percent to twenty-five percent the amount of EMPG funds available for personal expenses. The loss of funds for personal expenses will be especially devastating to smaller communities that may have only one or two full-time emergency management officials. In these communities, personnel costs account for almost one hundred percent of the cost of emergency management. As a result, the proposed change would force these communities to completely eliminate their emergency management capacity. Some states have told the National Emergency Management Agency that they could lose up to sixty percent of their emergency management personnel. I have not received a response to my April letter.

In your testimony at the Budget Committee hearing in February 2004, you stated that you had made the changes to the EMPG because you felt that it was the federal government's primary responsibility to help provide funding for emergency management training and exercises and that the federal government and state and local partners shared responsibility for salaries. This position underestimates the devastating impact this policy will have on local emergency management, particularly in smaller communities,

(a) What action do you propose to address the negative impact this policy change would undoubtedly have on state and local emergency management capacities in smaller communities?

Answer: The Administration's FY 2005 request for the Emergency Management Planning Grants is $170 million, which is higher than any previous request for this program. The funds will be used to assist the development, maintenance, and improvement of State and local emergency management capabilities, with a focus on homeland security, which are key components of a comprehensive national emergency management system for disasters and emergencies.

As you note, though, the request does cap the amount that states can use for salaries, thereby significantly increasing the amount of funds available for planning, training and exercises. The Administration's budget request still allows for award funds to support salaries. The request shifts the emphasis to federal support for planning while properly aligning responsibility for staffing and salaries with the states and local governments.

The Administration and Department have consistently supported the idea that homeland security is a shared responsibility between Federal and state and local governments. Additionally, it is important to remember that we are operating in a fiscal and security environment where we must ensure maximum security benefits are derived from every security dollar. To do that, we must be able to take a new look at the way in which we allocate resources, including sharing financial responsibility with our state and local partners.

(b) Should the Department's rules be adjusted to ensure that an emergency

management human resource baseline is achieved in every community?

Answer: Provision of human resources for basic emergency management is a state and local responsibility. The Department supports the flexibility that the Emergency Management Performance Grant (EMPG) program provides States to allocate funds according to risk vulnerabilities and to address the most urgent state and local needs in disaster mitigation, preparedness, response, and recovery. The EMPG program allows States and localities to use funds for personnel. There is no one-size fits all determination on the requisite number of personnel needed by local communities to handle emergency management response. The final decision rests with States and localities given their histories with emergency situations. As a general principle, DHS encourages states and localities to devote their own resources to such critical functions, and use Federal grants for building long term capabilities through planning, training, and equipment. .

(c) If the Department is not prepared to support such a baseline, what preparedness and crisis management guidance is the Department giving to small communities that may not be able to afford an emergency management official?

Answer: Provision of human resources for basic emergency management should be a state and local responsibility. Again, the Emergency Management Performance Grants program gives States and localities the flexibility to fund personnel salaries and expenses. It is up to localities to determine how best to staff their emergency management operations. In fact, many small communities have elected to use part-time personnel to manage their emergency management operations simply because their local circumstances do not require full time staff.

Establishing Standards

6. Over the last year, Senator Warren Rudman, Governor James Gilmore and other homeland security experts have made clear that establishing homeland security standards should be a top priority, Without standards, federal, state and local governments may allocate their money in ineffective and inefficient ways. I understand that the Department of Homeland Security is in the process of developing standards for first responder training and capabilities. When will these standards be made available for review and comment?

Answer: The Department of Homeland Security, under the implementation of Homeland Security Presidential Directive 8, is developing a Universal Task List (UTL), a Target Capabilities List and metrics that will be used to define and measure standards of performance for homeland security tasks. The UTL will define the tasks that must be performed at the federal, state, and local levels to prevent, respond to and recover from the incidents described in the 15 Illustrative Planning Scenarios (IPS) developed by the Homeland Security Council. The IPS define the range of threats and hazards for incidents of national significance. The UTL (version 1) will be completed by July 31, 2004.

The Target Capabilities List will define the capabilities needed at the federal, state and local levels to perform the tasks on the UTL. Building capabilities that are targeted at executing the essential tasks to standard, will provide a measurable baseline of national preparedness. The Target Capabilities List, which will be completed in the fall of 2004, will define training requirements.

Metrics will be developed to evaluate performance of the UTL as demonstrated through exercises and actual incidents. The measurement of performance will provide an objective assessment of preparedness.

The recently completed Report to Congress on the Standards and Guidelines provides additional information on standards related to training and capabilities, as well as those related to equipment, incident management, etc.

Questions of Senator Edward M. Kennedy
From the Senate Judiciary Committee Hearing
On "DHS Oversight: Terrorism and Other Topics"
June 9, 2004

I. DETENTION AND DEPORTATION OF ASYLUM SEEKERS AND HAITIANS

There have been reports of ongoing inconsistent practices and policies of Immigration and Customs Enforcement Bureau on the detention of asylum seekers. There are guidelines for the parole of asylum seekers, but parole decisions sometimes seem to be based on other factors --such as availability of bed space, and local policies. When parole is denied, there is no process for appeal. Recently, Undersecretary Hutchinson acknowledged this problem of inconsistent parole policies for asylum seekers and said that it would be addressed.

Question: What steps are you taking to make the asylum parole process uniform and fair?

There are three major routes which an alien can use to request asylum. Most aliens make their claim to asylum by filing at an Asylum Office (a part of the Bureau of Citizenship and Immigration Services). These claims are known as "affirmative asylum claims". Others arrive at Ports-of-Entry without documents or fraudulent documents and are placed into expedited removal proceedings. These aliens may make a claim to asylum and are then referred to an Asylum Officer and a credible fear determination is made. Once a positive credible fear determination has been made, the alien is then referred to the Executive Office for Immigration Review (EOIR) for adjudication of the claim. These cases are known as "credible fear claims". The third asylum route includes aliens that are already in removal proceedings that make a claim to asylum during their formal hearings before EOIR. These are referred to as "defensive asylum claims".

The detention experiences of these three groups and the ultimate outcome of the cases differ significantly. In general, only a very small number of the "affirmative" cases are ever detained. Most of the "credible fear" cases and many of the "defensive" cases are detained, at least for some time. The largest number of grants of asylum comes from the first category "affirmative asylum claims" by far.

Detention of the above categories are demonstrated by the most recent numbers available, FY 2003:

- 190 of the 56,120 affirmative asylum seekers were detained.
- 5,793 of the 5,986 credible fear asylum seekers were detained.
- 7,966 of the 11,048 defensive asylum seekers were detained.

Theses numbers taken over a year and in context of an average detention population in excess of aliens twenty thousand during FY 2003 demonstrate that ICE's Detention and Removal Operations DRO has been using discretion in cases involving asylum seekers. This fact should not be interpreted that DRO policy does not preclude the detention of asylum seekers, particularly in instances involving potential threats to our national security, aliens with criminal histories, aliens that may pose a threat to the community if released, or aliens who have significant factors indicating a high likelihood of absconding. Of those asylum seekers and credible fear cases that are detained, there are very legitimate questions of identity. However, once positive identity, sponsorship, lack of flight risk, and lack of any community safety concerns are established, the cases are eligible for parole and under our policy should be paroled.

In a national Field Directive issued by Acting Director Victor Cerda on June 10, 2004, titled Bed Space Management, Director Cerda stated, "Strong consideration shall be given to releasing aliens placed in expedited removal proceedings if the alien has established credible fear of persecution as well as identity, sponsorship and sufficient lack of flight risk."

As with any matter based on discretion, individual case factors will play significant roles. DRO will continue to monitor the current policy that allows for case-by-case discretionary parole of asylum seekers to ensure that the parole process is consistently applied.

Several months ago, in the midst of the political instability and violence in Haiti President Bush said that we would "turn back any [Haitian] refugee that attempts to reach our shore." His statement was in flagrant violation of our legal obligations under international conventions. More recently, the massive flooding in Haiti has produced many deaths and much destruction. Yet, just last week, the Department deported 78 refugees who fled Haiti and sought asylum in the United States, even as the State Department continues to warn U.S. citizens that it is to dangerous to travel to Haiti.

The Administration has also implemented a series of harsh measures on Haitian asylum seekers,

including intercepting boats from Haiti with little or no screening for asylum; prolonged and arbitrary detention of Haitians if they do reach our shores; and expedited hearings that seriously undermine their ability to claim asylum.
Many of these policies are within your jurisdiction. You could recommend granting Temporary Protected Status for Haitians currently in the U.S. The ongoing political conflict, plus the recent natural disaster, certainly meets the criteria for TPS designation.
Haitians are being returned to Haiti with no screening for asylum and no guarantee for their safety. This year we've stopped and returned more than 1000 Haitians under a ridiculous procedure called the "shout test". Only Haitians who protest their return loudly enough are asked whether they fear persecution. In contrast, all interdicted Cubans are individually interviewed about their fear of persecution and all interdicted Chinese are given a questionnaire to fill out to assess their fear of return. **Question: How can you possible justify this difference in treatment? Is It fair, or is It bigotry? Shouldn't all Haitians be interviewed individually to determine whether they fear persecution if we send them back?**

> **Answer:** While it is true that there are nationality-specific processes for identifying Cuban and Chinese migrants who may fear return, these processes are the result of the unique circumstances under which the interdiction programs for these migrants are conducted. They in no way reflect a lack of commitment to the protection of other migrants who are interdicted at sea by the U.S. Coast Guard and may fear return. It is long standing U.S. policy and practice to provide all interdicted migrants, including Haitian migrants, with a meaningful opportunity to seek and receive protection against persecution or torture.
>
> Any interdicted migrant who expresses or indicates, whether verbally or physically, a fear of return to a U.S. Coast Guardsman is interviewed by a trained U.S. Citizenship and Immigration Service (USCIS) asylum officer to determine whether the migrant has a "credible fear" of persecution or torture. These credible fear assessments are routinely reviewed and, as necessary, additional questioning is conducted to ensure that migrants have had a meaningful opportunity to express their fears regarding return and that all relevant information regarding their fear has been elicited.

Migrants who are determined to have a credible fear are then transferred for further processing by a second USCIS asylum officer who conducts an in-depth exploration of their protection concerns. Upon completion of protection screening, those migrants determined to require protection based on a well-founded fear of persecution or likelihood of torture generally will be resettled in third countries by the Department of State.

II. ASSAULT WEAPONS BAN

The Administration has been aggressively lobbying to renew the provisions of the PATRIOT Act, which expires at the end of 2005, even though we picked that date precisely so that it would not become apolitical football in this election year. But, we've heard nothing from the Administration about another essential protection against terrorism which is due to expire in

three months: the federal ban on assault weapons.

Even before 9/11, renewal of the assault weapons ban was a no-brainer. After 9/11, to even consider letting the ban expire is absurd. These weapons are killing machines. They're intentionally designed to maximize their killing power. They're no use for bunting. They're unnecessary and impractical for self-defense. They have no recreational value.

The only thing they do is facilitate crime. Before the federal ban, they were the weapon of choice for drug traffickers, gangs, and other criminal organizations. They endangered police officers and innocent bystanders.

Terrorists aren't dumb. They're exploiting any weakness or loophole in our gun laws. A terrorist training manual discovered by American soldiers in Afghanistan in 2001 told al Qaeda members to buy assault Weapons in the United States and use them against us. We'll be at much greater risk if Congress fails to renew the current ban. That's why every major law enforcement organization in the country supports renewing the ban.

President Bush says he supports it too. *As* a Congressman and a candidate for Governor of Pennsylvania, Secretary Ridge, you strongly supported a ban on assault weapons.

Question: Why hasn't the Administration made renewing the assault weapons ban a top legislative priority? Why haven't you demanded action on this issue? Given the urgency of this issue, will you call for Immediate action?

Answer: We recommend you refer this question to the Department of Justice.

III. BIOMETRICS PASSPORT DEADLINE

As you know other countries are having trouble meeting the October deadline for biometric passports. I've supported a two year extension of the deadline for countries in the Visa Waiver Program.

Question: How serious is the problem other countries are facing? How big is the gap in our own border security today? Won't some countries inevitably be slower than others in complying? Is two years sufficient time for countries to comply? Is one year sufficient time?

Answer: Implementation of biometric passports is a complex task. Only in May of this year did ICAO finalize the standards for biometric passports. Preliminary tests conducted earlier this year showed that there was no Integrated Circuit (IC) chip proposed for passports that could be read by all of the readers on the market and no reader that could read all of the types of chips. In late July, US-VISIT hosted an international meeting where chip vendors, passport manufacturers, and reader manufacturers came together to resolve problems in interoperability. In late November, US-VISIT conducted a mock port of entry test of IC passport chip readers in an operational environment. Technical problems were identified with the readers but a formal evaluation is not

yet completed.

In addition, nations preparing to issue biometric passports have had several obstacles to overcome. They must get their budgets approved for the project. They must also establish a testing and development program. Some nations, such as New Zealand, Australia, Belgium, and others have indicated that they will be able to start producing passports in early 2005. But many nations, such as Japan and the United Kingdom, have indicated that they will probably not be able to make the October 2004 deadline. The Netherlands, for instance, has an extensive testing program underway to ensure that the new passports will work in practical usage environments but will only begin issuing passports based on the results of that analysis A two-year delay would be realistic for nations to effectively implement e-passport. This would allow nations to review the "live test" to be sponsored by US-VISIT (along with Australia, New Zealand, and Germany) beginning in February 2005. That test will run several months in order to find whether these e-passports, as designed by the participating nations, work well in the inspections environment. There will be too little time between the issuance of the report and October 2005 for visa waiver nations to review and incorporate any recommended changes into their e-passport systems.

IV. COORDINATION OF IMMIGRATION FUNCTION AND POLICY

As you know, I believe that the key to the successful operation of the various immigration-related bureaus within the Department is coordination and accountability. The Homeland Security Act was supposed to bring immigration functions together from other agencies, but the Act then dispersed immigration throughout the new Department. Immigration policy is still subject to conflicting policies and interpretations. It's hard to see that much has changed.

Question: Are you satisfied with the current structure and organization of immigration functions within the Department? Shouldn't all immigration policy legal interpretation be housed in one office within DHS? How can we achieve consistent policies and application of laws among the bureaus? When conflicts over new policies arise between the two bureaus, how are they resolved?

ANSWER: I am satisfied with the current structure and organization of immigration functions within the Department. The Homeland Security Act contemplated the separation of immigration benefits and immigration enforcement policy offices, but also encouraged coordination of immigration policy issues between the enforcement (Border and Transportation Security Directorate (BTS)) and services (U.S. Citizenship and Immigration Services (USCIS)) components. I believe that, although the immigration policy offices of DHS are quite new, policy coordination between USCIS and BTS has been effective. Their efforts have been assisted by DHS' Office of General Counsel, and the Office of Civil Rights and Civil Liberties, both of which are independent of BTS and USCIS.

Question: What kinds of coordination already exist at the local and national levels between the three bureaus? Do you have formal meetings regularly?

ANSWER: The BTS organizational layer does not exist at the field office level. Therefore, USCIS, Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP) field offices work closely together on a variety of issues. Cooperation at this level, however, should be operational, rather than policy related. Field coordination varies from location to location depending on local needs and the frequency of cross-bureau issues. Some field offices have instituted regular formal liaison meetings among the bureaus. However, other offices have not found a need for a formalized structure and have addressed cross-bureau issues on a more informal basis.

V. PROGRESS REPORT ON THE BORDER SECURITY ACT

A serious security problem that became obvious after 9/11 was the failure of intelligence and law enforcement agencies to share critical information with the front-line agencies responsible for determining who is admitted into the U.S. The Border Security Act required the development and implementation of an information sharing plan. It also required the integration of data systems into a common network, the use of biometrics and machine readable passports and other documents and a report to Congress on the feasibility of a North American Security Perimeter.

Question Can you give us a progress report on the implementation of these programs and mandates? Are your agencies receiving the intelligence and law enforcement information you need from the FBI, CIA and other agencies? What progress has been made in creating the interoperable data system?

Answer: BTS is responsible for ensuring a continuing productive relationship between the intelligence arms of our BTS agencies – CBP, ICE, and TSA and the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate. BTS analysts are assigned to the Office of Information Analysis (IA) and there is a daily exchange of information between the BTS agencies and IA. This ensures that BTS has access to the information regarding threats to the homeland that IA receives by mandate from the federal government, DHS entities, State, territorial, tribal, local, and private sector partners, and Intelligence Community (IC) members, including the FBI and CIA. IA has excellent relationships with CIA, NGA, NSA, DIA, and others, and has representatives from IC members and DHS entities physically located at DHS. BTS and the Coast Guard have also exchanged personnel to enhance data sharing.

The BTS analysts primarily conduct follow-up research concerning BTS incidents of interest to IA and the intelligence community. This relationship provides a two-way street of information sharing, where the component representatives are immediately alerted to significant information received through IA channels and IA is immediately alerted to significant operational activity.

BTS intelligence representatives attend multiple, daily, meetings with IA where significant intelligence information is discussed. This includes intelligence derived from other elements of the intelligence community and law enforcement entities.

BTS agencies send daily reports to IA about significant incidents encountered by BTS agencies. These incidents are usually associated with a watch listed individual intercepted at the border, a subject on the no-fly list attempting to board an aircraft, or information alleging potential terrorist-related activity gained from an investigation.

BTS also works with IA to vet intelligence bulletins, reports, and assessments and to jointly assess relevant information. BTS ensures that intelligence is shared between intelligence analysts and operational personnel. BTS seeks to "operationalize" the intelligence we receive to ensure that the intelligence is incorporated into targeting and other decisions on an ongoing basis. For example, we may institute more targeted secondary inspections of travelers from regions that intelligence suggests warrant additional scrutiny, send priority leads based on intelligence to investigators in the field, or reassign Federal Air Marshals.

ICE has created a Threat Analysis Section (TAS) to identify and address potential vulnerabilities relative to the national security of the United States. The TAS establishes associations between individuals or groups linked to potential national security threats, develops profiles based upon relevant investigative and intelligence reporting, and produces actionable leads for field offices.

In addition, TSA's Transportation Security Intelligence Service (TSIS) produces a daily intelligence summary and a weekly suspicious incidents report that is shared with Federal Security Directors Federal Air Marshals, and state, local, and industry transportation stakeholders.

VI. LEGAL ORIENTATION PROGRAM

The Bureau of Immigration and Customs Enforcement now has the responsibility, for overseeing and implementing the Legal Orientation Program for increasing the efficiency and fairness of removal proceedings for persons detained by the Department. Near the end of fiscal year 2002, the former INS allocated $1 million to transition the program to the Executive Office for Immigration Review. The $1 million was intended to fund legal orientation programs to be transferred from the Department to the Executive Office for Immigration Review, to this day, the funds have still not been transferred.

Sen. Brownback and I wrote a letter to you in December 2003 on this issue. We received a response from Under Secretary Hutchinson just a few months ago, but the letter never indicated whether and when the $1 million appropriation is to be transferred. In fiscal year 2004, the Bureau of Immigration and Customs Enforcement transferred $1 million to the Executive Office for Immigration Review for the Legal Orientation Program.

<u>Question</u> Why have these funds still not been transferred? Does the Department continue to hold these funds? What is the status of the transfer of these funds? Do you agree that agencies must use appropriated funds for their Intended purpose?

ANSWER: The Department of Justice's Executive Office for Immigration

Review (EOIR)--not the Bureau of Immigration and Customs Enforcement (ICE)--has the responsibility for overseeing and implementing the Legal Orientation Program. While it is true that $1 million included in the Immigration and Naturalization Service's FY 2003 appropriation (which subsequently became a funding source for ICE) was not transferred to EOIR during FY 2003, ICE did transfer $1 million to EOIR pursuant to a reimbursable agreement signed on February 2, 2004. To my knowledge, this delay in funding has not been detrimental to the Legal Orientation Program.

The Department does not continue to hold these funds, as its authority to obligate or transfer remaining balances from its annual appropriation has expired and such a transfer would no longer be allowed by law.

Yes, I agree that agencies must use appropriated funds for their intended purpose. I regret that the transfer to EOIR was not made during FY 2003, and was delayed until February 2004.

VII. PROSECUTORIAL DISCRETION IN IMMIGRATION CASES

Department officials have publicly stated that a prosecutorial discretion memo on immigration matters remains in effect, but it is not clear that such discretion is being exercised in the field. Such discretion in the immigration context applies not only to the decision to issue a Notice to Appear when starting removal proceedings, but also to a broad range of other discretionary immigration-related enforcement decisions. It is an important way to encourage efficient and effective enforcement of the immigration laws and the interests of justice.

.Question: What steps have you taken to see that government immigration attorneys and field officers adhere to this guidance?

Answer: Since the breakup of INS, there are now at least three government agencies that are involved in the decisions in which prosecutorial discretion may be exercised, CBP, CIS and ICE. While ICE attorneys do not issue Notices to Appear (NTAs) or confer benefits, ICE attorneys do have a significant role in the process to assure cases are legally meritorious, to assure that sufficient evidence supports each allegation charged and to promote concepts of justice and efficiency on matters in litigation.

The Doris Meissner memorandum is available to all ICE attorneys on a program wide electronic database (DocuShare). Also the May 3, 2004 memorandum from ICE Director, Office of Investigations, John P. Clark, Operation Predator Alien Arrests, which states that law enforcement officers are often called upon to make discretionary decisions on who to investigate, who to arrest, who to charge, what to charge and when to terminate removal proceedings is available on DocuShare. The application of prosecutorial discretion to particular cases is a frequent topic of discussion between Chief Counsel and the trial attorneys, and between Chief Counsel and the HQ Components such as Field Legal Operations, Appellate Counsel and Enforcement Law Division.

Committee on the Judiciary
DHS Oversight: Terrorism and Other Topics Hearing
June 9, 2004
Senator Jeff Sessions
Written Questions for Secretary Tom Ridge

Extension of Biometric Standard Deadline

Importance of Maintaining Fingerprints as the Biometric Standard
Secretary Ridge, a few weeks ago when FBI Director Mueller was before the Committee, we discussed the importance of using fingerprints as the biometric standard for the entry-exit system at our borders and in our travel document. I believe it is incredibly important that the entry-exit system we create is Consistent with the current investments we have made in fingerprinting. Director Mueller strongly agreed with me, stating *"There has got to be interoperability and expansion of the system ourselves, working together with the Department of Homeland Security to be on the cutting edge of the use of fingerprints, and all of its various manifestations"*

In a hearing on biometrics before the House Judiciary Committee, you stated, *"The fingerprints, however, give us an added level of security and protection because we can compare it against a huge fingerprint database."*

A. Secretary Ridge, would you agree that the use of fingerprint technology is absolutely critical to our homeland security and to the identification and prosecution of terrorists and criminals who attempt to make it past our borders?

Answer: In the border and immigration management arenas, biometric identifiers are tools that help prevent the use of fraudulent identities and travel documents. The purpose of the biometric identifier is to verify a person's identity to ensure that an individual cannot apply for and/or be granted benefits under different names and to run watch list checks. Fingerprint technology is the most mature of the biometric technologies currently available. It provides the ability to verify identity and also to conduct appropriate checks. The U.S. Government, through DHS's US-VISIT and the Department of State's (DOS) BioVisa programs, has adopted an identity verification and anti-fraud strategy that uses biometric identifiers, i.e., fingerprints and digital photographs, stored in government electronic records. The DHS and DOS together have created a continuum of identity verification measures that begins overseas, when a traveler applies for a visa, and continues upon entry and exit from this country. The system stores biometric and biographic data in a secure electronic record and made available to decision makers.

B. Can you tell me why DHS waited until April 2,2004 to announce that it would include Visa Waiver travelers in the collection of fingerprints at our ports of entry through the U.S. VISIT system?

Answer: US-VISIT was established to respond to several Congressional mandates and the desire to improve the security of our citizens and visitors. When DHS was formed, I challenged the US-VISIT program office to design, develop, and deploy an automated entry and exit system that can better account for those who come to visit the United States. Because I believe that an entry and exit system without biometrics is not a secure system, I also challenged US-VISIT to deploy, in advance of the Congressional mandate, an entry and exit system that uses biometrics.

Border inspectors process over 500,000,000 border crossing transactions per year through air, land, and sea ports of entry. This necessitates implementing US-VISIT in phases or increments. The first increment of US-VISIT was launched on 5 January 2004 at 115 airports and 14 seaports. We also began testing a biometric departure confirmation system or exit process in two places in the country. On 3 August 2004, US-VISIT announced that it will expand exit pilots to 13 additional airports. By 30 September 2004, we were ready to expand enrollment to visitors traveling under the Visa Waiver Program who enter through an air or sea port. And by 31 December 2004, US-VISIT will be deployed to the 50 busiest land border ports of entry.

These steps are the just beginning of our long-term vision – to create a virtual border by tying together the threads of our immigration system, increasing the integrity of information by uniting disparate sources, and managing data on a timely basis.

C. Is this announcement a permanent announcement of that policy, will visa waiver travelers always be fingerprinted at the border, along with visa travelers, through US VISIT?

Answer: Yes. The 30 September 2004 inclusion of VWP travelers into the US-VISIT program is the next step in the implementation of the program. There is an important security interest in including VWP travelers in the program as the biometric checks ensure that the person carrying the passport is not an imposter.

D, Does the Administration believe it has the power to carve visa waiver travelers out of the US VISIT system once the deadline for inclusion of an ICAO selected biometric in Visa Waiver country passports is met?

Answer: As the requirements of section 110 Of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (as amended by the Data

Management Information Act of 2000), which requires the implementation of an entry-exit system, does not differentiate between VWP aliens and aliens with visas. The Border Security Act of 2002 deadline in section 303(c) of that law deals only with the requirement to have biometric technology in the passports themselves. Regardless of legal authority, DHS believes that the inclusion of VWP travelers in US-VISIT meets a valuable security need and ensures our ability to facilitate legitimate travel.

2. Visa Waiver Program In General/IG Report

At the end of April, the DHS Inspector General issued a report entitled *An Evaluation of the Security Implications of the Visa Waiver Program* (VWP), which concluded that the security in the VWP is lax.

A. Review of Visa Waiver Countries

The report highlights the fact that DHS Border and Transportation Security is legislatively required to, at least once every two years, evaluate each of the Visa Waiver Program countries so that we can decide if each country's designation should be continued. The one review that has been conducted was done in November of 2001 and evaluated only 5 of the 27 countries — it resulted in the Visa Waiver status of Argentina and Uruguay being terminated and Belgium being put on provisional status,

When will the full reviews of all 27 visa waiver countries be complete? Whencan we expect to hear the designation recommendations for each of the 27 countries?

Answer: A. Six of the VWP countries were reviewed 2002 – 2003. As a result of that review cycle, two of the original 29 countries, Argentina and Chile, were removed from the program. The results of the Belgium, Italy and Portugal reviews, with Italy and Portugal remaining in the program and Belgium being placed in a provisional status, were published in the Federal Register on March 3, 2003. The report on Slovenia was never published. DHS has begun the review of the 23 unreviewed countries, as well as Belgium, and Slovenia and is committed to completing the reviews in November and submitting the required reports to Congress.

B. Additional Steps Taken Due to Report Recommendations

1)DHS has taken one significant step toward improving the security of the Visa Waiver Program that did not exist when the IG report was written. On April 2, 2004, DHS announced that Visa Waiver travelers will be fingerprinted upon entering the US. as part of US. VISIT.

Please report on all the steps DHS has taken to follow the other recommendations in the IG report for improving the security of the Visa Waiver Program.

Answer: BTS has taken steps to follow all the recommendations in the IG report and is providing the OIG with a detailed response. For example, with regard to the first recommendation, the BTS Under Secretary designated an acting VWP program manager with clearly defined responsibilities and authorities on July 1, 2004. OIE has been assigned formal responsibility for conducting the required country reviews and developing formal protocols for those reviews, per recommendation 3. Sufficient funding has been provided for the current country reviews, per recommendation 4. With reference to recommendation 2, the BTS Office of International Enforcement's (OIE) VWP Oversight Unit participates in the US-VISIT Congressional Report Working Group that is developing a plan to ensure the accurate and timely submission of required VWP annual reports. The Bureau of Customs and Border Protection (CBP) is developing procedures that are responsive to recommendations 6, 7, 9, 10, 11 and 14 and, as appropriate, is coordinating with Immigration and Customs Enforcement (ICE). The draft protocol already contains the provisions referenced in recommendation 8. Note that recommendations 5 and 13 were closed by the OIG. (See attachment)

3. Information Sharing

A. NCIC

As you know, I remain deeply concerned by the lack of immigration related information contained in the NCIC, the database that state and local law enforcement officers across the country access everyday to catch criminal suspects and individuals that have evaded warrants for their arrest,

In February, I received a letter from Undersecretary Asa Hutchinson which detailed the number of entries in the Immigration Violators File (IVF) of the NCIC. The letter committed to an accelerated pace of placing alien absconders into the NCIC. At the time of that letter, Undersecretary Hutchison estimated that new absconders records were being entered at a rate of 200 per day.

Can you tell me what progress has been made since February on the entry of alien absconders into the NCIC? Are we still entering them at the rate of 200 a day, a rate I consider to be too slow?

Answer: Since February 1, 2004, the Law Enforcement Service Center has entered 17,495 new absconder records into the NCIC. The LESC enters approximately 1000 records into NCIC each month. In September of 2004, ICE input more than 4400 records or approximately 1100 per week for all NCIC entries including absconders, new deported felons, new criminal fugitives, and

NSEERS. It is important to note, however, that In addition to the initial entry, each record must be re-validated 90 days after the initial entry and again on an annual basis long as the entry is valid. ICE increased the number the total number of records entered by more than 100% from FY03 to FY04 and is currently the largest contributor with more than 157,000 records to date.

B. IDENT/IAFIS Merger

Another urgent issue in immigration information sharing is the merger of the INS and FBI fingerprint databases as recently highlighted in the March Department of Justice IG report titled, *IDENT/IAFIS: The .Batres Case and the Status of the Integration Project.* The report concluded, through the illustration of the Batres case, that there is still an urgent need to integrate the IDENT and IAFIS databases as soon as possible.

What progress has been made on IDENT/IAFIS integration since the March IG report?

Answer: The integration of the IDENT and IAFIS systems is progressing on schedule. Prior to FY 2004, the responsibility for the integration of IDENT and IAFIS resided with the Department of Justice (DOJ). In FY 2004 responsibility for the acquisition and field deployment of IDENT/IAFIS workstations was transferred to DHS from DOJ. DHS saw the need to continue to deploy this capability and assumed the project management and fiduciary responsibilities for the rollout. DHS/US-VISIT expects to spend $4 million in FY 2004 to continue to deploy to Border Patrol and Inspections locations, and potentially more than $3 million in FY2005 to deploy to the remainder of the DHS locations.

During an apprehension, DHS agents use the integrated IDENT/IAFIS terminals to collect fingerprints and send them to both the IDENT and IAFIS systems. These terminals account for approximately 50 percent of the total apprehensions of aliens within DHS . In 2004, DHS completed deployment of the integrated terminal to all Border Patrol stations, all air and sea ports of entry, and the 50 busiest land border ports of entry. In 2005, DHS will complete deployment to the remaining ports of entry and ICE field offices.

Secretary Ridge
QFRs for Judiciary Hearing
June 16, 2004

As referenced in National Security Presidential Directive-25, how does the Department of Homeland Security envision the role of U.S. Immigration and Customs Enforcement in the counter-narcotics strategy?

Answer: The means and methods used by narcotics smuggling organizations represent a significant vulnerability to the security of our nation. The goals and objectives set by the Administration in both the creation of DHS and the issuance of the counter-drug strategy through National Security Presidential Directive-25 (NSPD-25) clearly establish ICE as a critical component in efforts to counter the threat posed by terrorism and drug trafficking. NSPD-25 states that international drug trafficking organizations and their linkages to international terrorist organizations constitute a serious threat to the national security of the United States, which requires a concerted effort by all appropriate departments and agencies.

A primary goal in the establishment of DHS was to improve the ability to identify and interdict suspect persons and illegal contraband entering the United States by combining into one Department the separate activities and assets of agencies such as the U.S. Customs Service, Coast Guard, Border Patrol, and the Immigration and Naturalization Service.

As the investigative arm of BTS, ICE is responsible for conducting investigations related to smuggling and other violations of U.S. border integrity and our financial system. ICE's very broad authorities to pursue investigations are not limited to any specific region or criminal activity, and they provide the flexibility to fully pursue vulnerabilities pertaining to our nation's borders – to include illicit drug trafficking. ICE has a distinct but complementary mission to those agencies charged with solely narcotics enforcement.

ICE has become proficient in identifying the vulnerabilities of smuggling and transportation organizations. Working together with agencies internal and external to BTS, ICE employs numerous national programs and initiatives designed to identify, target, disrupt, and ultimately dismantle smuggling organizations that pose a threat to our nation.

Do criminal investigators assigned to the U.S Immigration and Customs Enforcement have the unimpeded authority necessary to fully enforce violations of all types related to border security and vulnerabilities? If not, what additional authority is necessary to fulfill that mandate?

Answer: Yes, with the following exception: Since the creation of ICE in March 2003, our increased resources (material and personnel), statutory authority and technical

expertise have dramatically improved our ability to target and disrupt criminal organizations engaged in human smuggling and trafficking. However, some technical legislative omissions remain with the Immigration and Naturalization Act (as amended) which permit human smugglers to escape apprehension and removal by ICE. We will work within the Administration to provide you the necessary legislative changes in the near future.

My bill, S. 1837, will extend the National Money Laundering Strategy for another three years. The Department of Homeland Security has significant expertise in money laundering investigations but didn't exist when the law was passed. What should be DHS's role in developing a national strategy and in our efforts to combat terrorist financing?

Answer: Previous legislation directed development of the NMLS by DOJ and Treasury in recognition of the statutory responsibilities of their respective component law enforcement agencies. This included Treasury's U.S. Customs Service and Secret Service - now part of DHS. Customs' Office of Investigations - one of the largest investigators of money laundering and financial crimes - became part of DHS' Immigration and Customs Enforcement (ICE).

ICE and its predecessor organizations have been instrumental in the conduct of complex and high-impact financial investigations for over 30 years. To cite a few examples: the Bank of Commerce and Credit International (BCCI) in Tampa; Operation Greenback in South Florida; Operation Casablanca in Los Angeles; and Operation Green Mile in Phoenix. ICE leads New York's El Dorado Task Force and Miami's Foreign Political Corruption Task Force. These operations and task forces alone have resulted in the seizure of almost one billion dollars in criminal proceeds.

The National Money Laundering Strategy (NMLS) was recently reauthorized through the intelligence reform bill using the text from the original legislation without recognizing the creation of DHS and its money laundering programs. As described above, DHS has extensive investigative authority and plays a major role in protecting the economic security of the nation, and should have significant involvement in the development, drafting, and implementation of the NMLS. DHS participation is essential to the United States Government's efforts to identify, disrupt and dismantle organizations and systems used to launder proceeds of criminal activities, including terrorism.

It's my understanding that the DEA and ICE are currently in discussions over how they should coordinate narcotics investigations. Can you please state what role you think ICE should play in investigating international narcotics smuggling organizations, and what overall role the Department of Homeland Security should have in disrupting the economic basis of the drug trade?

Answer: ICE's investment of equipment and human capital in counter narcotics work has

been significant and continues to serve a critical role in our nation's counter narcotics and homeland security efforts.

As the investigative arm of BTS, ICE works in partnership with agencies internal and external to BTS. ICE employs numerous national programs and initiatives designed to identify, target, disrupt, and ultimately dismantle smuggling organizations that pose a threat to our nation. These programs are numerous and cover a wide range of subjects, including maritime and border security, the national drug control strategy, liaison to external agencies, cross-designation programs, and future initiatives.

ICE routinely conducts investigations to dismantle criminal organizations that use internal conspiracies to facilitate their smuggling operations. The majority of internal conspiracies occur in the airport and seaport environments. The ICE Maritime Port Security Program was formally initiated on June 24, 2003 with the introduction of Operation Safe Harbor. This initiative combines both personnel and technology to secure our seaports by addressing the threats posed by internal conspiracies and smuggling operations. Operation Safe Harbor focuses on investigative initiatives in the maritime port environment as well as non-investigative initiatives involving cooperative programs with CBP, Coast Guard, TSA, and other agencies. Special agents are currently deployed within seaports to target criminal organizations using internal conspiracies.

It is well established that the lifeblood of any criminal enterprise is money. Depriving narcotics traffickers of their profits through aggressive financial investigations is imperative to the national narcotics enforcement strategy. ICE, in cooperation with other federal agencies, has played a longstanding role in the execution of that strategy by conducting investigations of money laundering and other complex international financial crimes, in particular narcotics money laundering." ICE presently has in place several longstanding programs and strategies targeting narcotic money laundering, including the Cornerstone Unit, bulk cash smuggling strategy, the Black Market Peso Exchange Program, the Money Laundering Coordination Center (MLCC), and the Trade Transparency Unit (TTU). These programs and strategies further represent the active and important role that DHS plays in the overall disruption of the economic basis of the drug trade.

Cornerstone is DHS/ICE's investigative initiative that protects the economic security of the U.S. by targeting and eliminating vulnerabilities in the financial and trade sectors susceptible to exploitation by drug traffickers and other criminal organizations. This program helps to identify the ways in which drug traffickers and money laundering organizations exploit financial systems.

ICE bulk cash smuggling initiatives focus on identifying various methods of transporting bulk currency and negotiable instruments that represent the profits from illicit drug smuggling into the United States. The passage of the USA PATRIOT Act provided an important tool to ICE to enforce bulk cash smuggling. ICE agents have successfully utilized this authority by conducting enforcement initiatives at border crossings, international airports, and express mail courier hubs.

Trade-based money laundering and the use of legitimate trade transactions to launder, disguise, and move proceeds of illicit crimes play a significant part in supporting the economic bases of the drug trade. ICE can identify and combat trade-based money laundering, of which the Black Market Peso Exchange (BMPE) system has been identified as the most pervasive. ICE's access and experience in analyzing trade data, and its close working relationship with our inspectors at the border, establishes ICE's role in combating trade-based money laundering. ICE has in place the Numerically Integrated Profiling System (NIPS), an analytical program to exploit this trade data. ICE's Trade Transparency Unit (TTU), an outgrowth of NIPS, shares U.S. and participating foreign governments trade data. This allows both countries to see both sides of an import/export transaction. Anomalies that are identified in transactions may be indicative of trade-based money laundering.

ICE's MLCC serves as a clearinghouse and de-confliction center for international narcotics money laundering operations within ICE. The MLCC provides crossover bank account relationships, and provides strategic and tactical analyses of trends and patterns that develop from historical and current money laundering investigations. The MLCC is ICE's repository for all Black Market Peso Exchange (BMPE) investigative data gathered from various financial investigations. As part of the U.S. Government's overall plan to assist Colombia in the battle against the drug trade, ICE has an active role in combating trade- based money laundering and the BMPE. Special Agents assigned to the ICE Attaché in Bogota, Colombia facilitate ICE's initiatives under Plan Colombia.

SUBMISSIONS FOR THE RECORD

Border Trade Alliance
Alianza del Comercio Fronterizo
Alliance du Commerce Transfrontalier

October 1, 2003

The Hon. Tom Ridge
Secretary of Homeland Security
3801 Nebraska Ave., NW
Washington, D.C. 20393

Dear Secretary Ridge:

It was with great interest that we read the recent Memorandum of Understanding (MOU) between the Secretaries of State and Homeland Security concerning implementation of Section 428 of the Homeland Security Act of 2002. The Border Trade Alliance (BTA) wholeheartedly endorses the MOU's stated intent of creating a system in which both departments "work cooperatively to create and maintain an effective, efficient visa process that secures America's borders from external threats and ensures that our borders remain open to legitimate travel to the United States." It is in that spirit that we write to you today.

As you know, residents of our neighbor to the south, Mexico, must secure a B1/B2 "laser visa" Border Crossing Card (BCC) in order to travel into the United States. While the BCC is good for 10 years, the holder may only remain in the U.S. for up to 72 hours at a time. If a Mexican traveler with a BCC seeks to travel 25 miles beyond the border, that traveler must obtain form I-94 and pay a fee of $6 U.S. (except for those travelers who entered the U.S. at certain ports of entry on the Arizona-Mexico border).

The BTA advocates extending the permissible period of entry for Mexican citizens from the current 72 hours so as to more accurately reflect the economic and social realities of the U.S.–Mexico border region. Furthermore, the BTA believes that the permissible geographic entry area into the U.S. should be extended for travel without an I-94.

The economies of the U.S. communities of the U.S.-Mexico border depend on the ability of legitimate Mexican travelers to cross the border with minimal hassle. Consider these facts:

- According to a survey conducted by VISA, McAllen, Texas is the number one city in the United States as a spending destination by Mexican VISA credit card holders.
- In San Diego, California, annual sales tax receipts totaling $1.5 - $2 billion can be attributed to Mexican shoppers. (Source: Crossborder Business Associates)
- Mexican tourists spent approximately $1.6 billion in Arizona last year and support some 35,200 jobs. (Source: Economic Impact of the Mexico-Arizona Relationship, American Graduate School of International Management)

The above is just a sampling of the inextricable links between the U.S. southern border and our neighbor to the south.

Address: 111 W Monroe, Suite 510, Phoenix, AZ 85003 Toll-Free: (800)333-5523 Tel: (602) 266-7427 Fax: (602) 266-9826
Web: www.thebta.org

Border Trade Alliance letter to DHS seeking changes to BCC regulations, page 2

As we celebrate the 10th anniversary of the implementation of the North American Free Trade Agreement, let us remember NAFTA's vision of bringing our three signatory nations closer together. In today's environment of heightened security awareness, we should strive to enhance our relationships with our friends and allies in Canada and Mexico so that we may focus our precious enforcement resources on those travelers who may require more thorough focus from our border personnel. By amending the rules governing use of the Border Crossing Card and the I-94, the U.S. government would send the message that our country welcomes legitimate travel and commerce and would be taking a needed step to greatly improve the processing of legitimate travelers at our ports of entry.

The Border Trade Alliance has worked with policymakers in all three NAFTA countries for the past 17 years in an effort to facilitate legitimate cross-border trade and travel. We hope you will agree that the integration of the North American economies and today's security environment necessitates looking for ways in which we can facilitate legitimate border crossings while stamping out the scourge of terrorism and contraband trafficking. We look forward to working with your department to affect this needed change in our nation's immigration policy.

Sincerely,

Richard Cortez
Chair

CC: Secretary of State Colin Powell

Senator Dianne Feinstein
Senator Barbara Boxer
Senator John McCain
Senator Jon Kyl
Senator Pete Domenici
Senator Jeff Bingaman
Senator Kay Bailey Hutchison
Senator John Cornyn

U.S.-Mexico Border Caucus
U.S.-Mexico Caucus

Governor Gray Davis
Governor Janet Napolitano
Governor Rick Perry
Governor Bill Richardson

Ambassador Antonio Garza
Ambassador Juan Jose Bremer

Border Facts and Talking Points

- Each year, the INS inspects more than **half a billion entries into the U.S.** (This number includes all categories of temporary visitors, green card holders, and U.S. citizens, and multiple crossings by the same individual.)

- More than 80% of all inspections are done at land borders (more than 400 million). Air inspections are second with just under 80 million annually. (Source: INS Inspections Statistics). 80% of land border inspections are same-day trips. (Source: North American Trade and Travel Trends).

- Approximately 800,000 border crossings are made daily between U.S. and Mexico; approximately 260,000 cross each day between U.S. and Canada. (Source: North American Trade and Travel Trends.)

- In 1998, the last year for which data is available, **more than 30 million of those entrants were temporary visitors (nonimmigrant visas)**, and of those, **more than 23 million were tourists,** and more than **4 million were business visitors**. (*Source:* 1998 Statistical Yearbook of the Immigration and Naturalization Service.) **195 million temporary nonimmigrants were admitted at land borders in FY2001**. (*Source:* DOJ OIG Report I-2002-006, April 2002).

- Between 15 and 18 million visitors entered under the Visa Waiver Program last year, which allows nationals of some 25 countries (mostly European) to travel here as tourists or to conduct business.

- In 2000, international travelers spent **$82 billion in the U.S.**, not including passenger fares and this supports 1 million U.S. jobs in the tourism industry. (*Source:* Tourism Industries/International Trade Administration, U.S. Dept. of Commerce, via Travel Industry Association web site, www.tia.org/ivis.)

- U.S. Consulates around the world reviewed **8,222,451 visa applications** for temporary visitors in 1999. They also process **over 700,000 green card applications each year**. Depending on the country of nationality and the type of visa, several different types of background and security checks may be done during this process, as well as, usually, an in-person interview. The review process can take anywhere from a day to several months

- Last year **127 million cars and 211,000 boats** passed through our inspection ports.

- Trade between U.S. and Canada in 2000 was over $400 billion, averaging over $1 billion **each day.** Trade between the U.S. and Mexico in 2000 was over $248 billion. Canada and Mexico are now our #1 and #2 trading partners, representing more than 30% of U.S. international trade. **(Source: *North American Travel & Trends, U.S. Dept. of Transportation, Bureau of Transportation Statistics, 2001).***

- Two-thirds of all NAFTA Trade is transported by trucks, at $429 billion in 2000, with Detroit/Windsor and Laredo/Nuevo Laredo seeing the highest volume on each border.

A coalition of Americans concerned about trade, business, and border management
1615 H Street, NW, Washington, DC 20062-2000 202-463-5522 *Fax* 202-463-5901
www.abbcoalition.org

Statement
United States Senate Committee on the Judiciary
DHS Oversight: Terrorism and Other Topics
June 9, 2004

The Honorable Orrin Hatch
United States Senator , Utah

"DHS Oversight: Terrorism and Other Topics"

We are here today to hold our eighth hearing since last fall to oversee our government's attempts to protect against and respond to acts of terrorism. We heard from Attorney General Ashcroft yesterday.

Today we are pleased to have Secretary Tom Ridge, the leader of the Department of Homeland Security.

In the aftermath of September 11th, the new Department of Homeland Security was created. This was a massive undertaking the likes of which this country has not seen since 1947, when President Truman reorganized our defense and security agencies.

I personally want to thank Secretary Ridge and his colleagues at DHS for your efforts to improve our nation's security.

You are to be commended for your leadership and the initiatives that you have implemented—initiatives to increase our nation's ability to respond to emergencies, to enhance the security of our borders, to increase our ability to defend against bioterrorism, to improve our intelligence-gathering and information-sharing, and to integrate our local communities within our nation's homeland defense efforts.

Despite the daunting nature of your charge, in just over a year your department has:

-successfully merged 22 agencies and 180,000 employees into a single department;

-developed and implemented aviation security procedures—including explosives detection systems;

-issued new security directives requiring enhanced rail operator protocols;

-tailored the student visit program to ensure that students who pose no threat to our country are permitted entry;

-streamlined the information sharing process;

-established a homeland security operations center aimed at coordinating the efforts of federal, state, and local authorities;

-enhanced port security;

-And, provided substantial assistance to those on the frontlines, our nation's first responders.

By no means is this a comprehensive list of your accomplishments. And, all would agree, there is much more to be done in order to ensure the security of our homeland.

Most recently, however, you have proven that you are a leader willing to take the constructive criticism and recommendations of others when it comes to safeguarding this country. By way of example, the Office of Inspector General recently issued a report recommending a number of changes to the Visa Waiver Program.

In response, the Department of Homeland Security announced that by the end of September this year, it will extend US-VISIT requirements to travelers who visit the United States from Visa Waiver Countries.

We have had 93 million visitors from these countries over the past five years, so this will not be an easy task. I commend you for taking this bold step forward to improve our visa waiver system, and for working to secure this country against the threat of terrorists.

I do want to take a few moments to challenge the Administration in an area in which I think we can do much better: bioterrorism.

First off, let me recognize that our country is in many ways much better off to respond to a bioterrorism attacks than we were in the Fall of 2001.

Our first responders are much better equipped.

There is much better coordination among the federal, state, and local governments – we in Utah saw this first hand during the Winter Olympics.

I want to commend the Administration and my colleagues in Congress for the work on the Bioshield legislation.

Senators Gregg, Frist and Kennedy have consistently moved the ball forward on this issue.

Vice President Cheney and Secretary Thompson have provided leadership in this area. Dr. Tony Fauci at NIH is coordinating government, academic, and private sector scientists and, as always, is pushing the envelope of scientific knowledge forward.

Unfortunately, the results to date are simply inadequate.

We know that there is a list of some 57 known bioterrorism threat agents. It is my understanding that

there are only two FDA-approved countermeasures to these known threats. That is correct – just two of the 57 threats have responses.

And the truth of the matter is that the r&d pipeline is less than robust.

That is one reason why Senator Lieberman and I have proposed bi-partisan legislation whose goal is to provide a variety of incentives designed to stimulate private sector biotechnology firms to develop new research tools, diagnostics, therapeutics and vaccines.

Our legislation includes tax incentives, intellectual property incentives such as patent term restoration and extension of current marketing exclusivity periods, and up-front liability negotiations.

We must not let any politically expedient anti-drug company antipathy with the attempt of the Lieberman-Hatch bill to unleash the creative genius of the private sector because that is where treatments and cures will come from.

In short, we need to create a well-capitalized bio-defense industry that will respond to our needs as this threat evolves. That is the goal of the Lieberman-Hatch bill.

I commend my partner, Senator Lieberman, for his vision in this critically important area.

Although the year is moving along, I hope in the weeks ahead to hold a hearing on some of the novel IP and liability provisions of the Lieberman-Hatch bioterrorism bill.

Mr. Secretary, I hope that the Administration will carefully review our bill and provide experts to participate in this hearing.

Let me close by saying that I know that everyone on this Committee shares the common goal of protecting our country from additional terrorist attacks. And I believe we are all committed to achieving that goal with complete respect for the fundamental freedoms of the American people.

This Committee has a historical tradition of examining, debating, and resolving some of the most important legal and policy issues that have been presented to Congress. We are once again faced with an important task that will have a profound impact on our country's security and liberty. I am confident we are up to the task.

Statement of Senator Patrick Leahy,
Ranking Member, Senate Judiciary Committee
Hearing On
"DHS Oversight: Terrorism and Other Topics"
Secretary Tom Ridge
June 9, 2004

Mixed Messages: Who's In Charge?

Thank you, Mr. Chairman, and thank you, Secretary Ridge, for appearing before the Committee to discuss the state of our homeland security efforts. If the American people are uneasy about their security as we enter the summer traveling season, that may be because of the conflicting signals they are receiving from their Government. Yesterday we heard from the Attorney General, who two weeks ago took to the nation's television screens to warn them of an impending Al Qaeda attack. It had the appearance of the unilateralism that has come to characterize the Attorney General's handling of his job. Earlier the same day, Mr. Secretary, you appeared on many of those same television screens and encouraged Americans to "go out and have some fun" this summer. The American people are left to wonder whether they should be summering in fallout shelters or living the lives to which they had become accustomed before the September 11 attacks.

These doubts stem in part from the Administration's failure to follow the process Congress mandated in the Homeland Security Act of 2002. Under the Act, the Secretary of the Homeland Security Department is the only person authorized to issue public threat warnings. In broadcasting his own independent warnings, the Attorney General disregarded that law. I agree with the words of Christopher Cox, the Republican Chairman of the House Select Committee on Homeland Security: "In the Homeland Security Act, DHS was assigned the central coordinating role in this process. The absence of Secretary Ridge from [the] news conference held by the attorney general and the FBI director, and the conflicting public messages their separate public appearances delivered to the nation, suggests that the broad and close interagency consultation we expect, and which the law requires, did not take place in this case. The American public, state and local law enforcement, governors and mayors, and private sector officials with responsibility for critical infrastructure all deserve crystal clarity when it comes to terrorism threat advisories."

White House's Ambivalence And Partisanship About DHS

The Administration's lingering ambivalence about the Department of Homeland Security seems to be a residual byproduct from the process that created the Department. And as we review the Administration's failure to hew to the charter of the Homeland Security Act, it is instructive to consider the history of the Department's founding. Of course, the President initially opposed the efforts of Democrats, joined by some Republicans in Congress, to create a Department of Homeland Security in the first place. He then flip-flopped on the issue, embracing the creation of a new agency in an announcement timed to deflect attention from this Committee's oversight hearing with Coleen Rowley, the FBI agent who accused the Administration of negligence in its reaction to the arrest of Zacarias Moussaoui the month before the September 11 attacks. After the President's conversion, he then barnstormed the nation and campaigned against Democratic Senators like Max Cleland, who agreed with the President's newfound goal of creating a new Department but wanted one that would respect the rights of the men and women who were working to keep our nation safe. And well before the Department was established, the White House for more than a year ignored outright – without even the courtesy of a dialogue, or even an acknowledgement – the appeals many of us had made for implementing the provisions of the USA PATRIOT Act that authorized help to our partners in homeland security, our state and local first responders. In the critical year after September 11th, the Administration also casually disregarded our appeals to implement other homeland security provisions Congress had included in the PATRIOT Act, such as the section on Northern Border security and the provisions to improve our translator capabilities.

It would be comforting if we could at least tell Americans that – despite the conflicting guidance from their leaders and the President's history of playing politics with homeland security – that their Government was doing everything possible and practical to keep them safe. Unfortunately, we cannot truthfully tell them that. As we sit here today, there is much left undone in securing our nation. And we have recently learned that a White House budget memorandum circulated within the Administration last month states that if there were to be a second Bush Administration, the President actually intends to *cut* spending for homeland security by $1 billion in his next budget – the first budget he will submit once he knows he will not have to face American voters again. In other words, we should expect that whatever security gaps are present today will only worsen in coming years. Although such news may be shocking, it is the logical consequence of the obsession of the President and the Republican-controlled Congress with cutting taxes for the wealthiest Americans, regardless of the fiscal consequences. The top 1 percent may have benefited, but the nation as a whole is and will continue to be less secure because of the reckless fiscal policies of this Administration.

Broken Promises To First Responders

I look forward to hearing Secretary Ridge's view as to our most pressing security needs. First, however, I would like to share some of my most serious homeland security concerns, starting with the Bush Administration's failure to provide the necessary

assistance for first responders throughout our nation. As the costs borne by law enforcement agencies across the country continue to rise, we need to increase funding for our nation's first responders. Instead, the President has proposed cutting overall funding for our nation's first responders by $800 million. These cuts target vital emergency services affecting every State, regardless of size or population.

The Hart-Rudman report on domestic preparedness argued that the U.S. will fall approximately $98.4 billion short of meeting critical emergency responder needs over the next five years if current funding levels are maintained. Clearly, the domestic preparedness funds available are insufficient to protect our people and prepare for and respond to future domestic terrorist attacks anywhere on American soil.

Indeed, a 2003 report by the Council on Foreign Relations found a number of serious flaws in the preparedness of our first responders. For example, the Council found that only 10 percent of fire departments in the nation have the personnel and equipment to respond to a building collapse. The Council also wrote that most cities do not have the necessary equipment even to determine the kind of hazardous materials their emergency responders may be facing.

In February 2003, I introduced S.315, the First Responders Partnership Grant Act. I have repeatedly asked the Chairman to mark up this bill, but he has declined to do so. The bill would provide $4 billion annually to support our State and local public safety officers in the war against terrorism. Grants will be made directly to state and local governments and Indian tribes for equipment, training and facilities to support public safety officers in their efforts to protect homeland security and prevent and respond to acts of terrorism. This is essential Federal support that our law enforcement officers, firefighters and emergency medical service providers need and deserve. Unfortunately, this Committee has refused even to consider it.

Vulnerable Ports

I believe that our approach to port security is also insufficient, and I know that many of my colleagues on this Committee share that view. Senators Biden and Specter have introduced legislation to strengthen the security of our ports, as has Senator Feinstein. I hope to hear today whether the Secretary supports those bills.

More than 90 percent of the world's trade is moved in cargo containers. As CBS "60 Minutes" reported last summer, fewer than 2 percent of the 16,000 containers coming into the U.S. every day are inspected. Stephen Flynn, a senior fellow at the Council on Foreign Relations and a noted expert on seaport security, told "60 Minutes" last summer that the information provided by shippers is frequently unreliable and vague, and said, "The fact of the matter is criminals have been operating in seaports a long time. The bad guys know how open the system is. The good guys don't seem to have a real command on it here because we haven't paid as much attention to this problem as we need to."

The General Accounting Office has found that that the information that the Bureau of Customs and Border Patrol uses to determine which cargo should be searched is "one of the least reliable or useful for targeting purposes." In addition, the U.S. has been slow to install radiation detection portals at our ports, leaving us vulnerable to the smuggling of a nuclear or radiological weapon. I would appreciate an update from the Secretary on the installation of such devices.

Mass Transit Measures Idle

Our mass transit systems are similarly at risk, as this Committee discussed in an April hearing. While we will spend about $4.5 billion on aviation security this year, we will devote only $65 million to rail security, even though five times as many people take trains as planes every day. The Madrid bombing vividly demonstrated the potential vulnerability of mass transit, and I am concerned that the Administration is not responding forcefully enough to this threat. Last year, a survey of transit agencies by the American Public Transportation Association identified some $6 billion in unmet security needs. These needs remain unmet today, and yet we have not received a plan from the Transportation Security Administration to address them.

There are a number of bills pending in the Senate by Senators Hollings, Schumer, Feinstein and others, including S.22, the Justice Enhancement and Domestic Security Act introduced in January 2003, that address rail security and funding issues. I hope the Secretary will tell us the Department's position on those bills.

Air Security Concerns Linger

While we have devoted substantial resources to our air security, problems remain. There have been several reorganizations of the TSA's airport screeners program, and I begin to wonder if and when we are going to get it right. Reports from the GAO and the DHS Inspector General's office suggest that the screening of baggage and passengers at our nation's airports remains lax, nearly three years after the September 11 attacks. Meanwhile, some Congressional Republicans are calling for yet another reorganization, in which the airport screeners would be returned to the private sector. On top of all this, the TSA has been slow in developing security procedures at port and rail facilities around the country. I would like to hear today what steps are being taken to correct the problems the GAO and the IG have found, and what continuing role and structure the Secretary envisions for the TSA.

Outsourcing And Unmet Immigration Responsibilities

Finally, I would like to say a few words about the immigration functions at DHS. Just last week, the Department awarded a contract worth up to $10 billion to Accenture LLP to oversee and expand the US VISIT program, which Congress has approved to track the entry and exit of foreign visitors. Accenture's parent company – Accenture Ltd. -- could itself be considered a foreign visitor to the United States, as it has moved offshore to

Bermuda. I am concerned that a contract this lucrative has been awarded to a company whose parent has chosen to leave the United States, while wholly American companies also submitted bids. I think this sends exactly the wrong message to corporations deciding whether they should continue to be headquartered here.

I think it also sends the wrong message when the President makes a splashy announcement in January promising to liberalize our immigration policies, and then does nothing to advance his own plan in the following five months. I still await the legislative proposal I sought from him in January. It appears that the President has abandoned his efforts in the face of harsh criticism from the right wing of his party. Our immigration problems, however, will not simply go away because the President's base opposes any realistic effort to deal with them.

At the very least, we should pass those bills that have strong bipartisan support, such as the DREAM Act – which continues to languish on the Senate floor – and the AgJOBS bill, which would help farmers and farm workers throughout the nation. I hope that the Secretary can shed light on his and the President's positions on those bills, and the President's plans for immigration reform during the remainder of his term.

Conclusion

I have raised a number of concerns in my remarks today, and I do not mean to imply that this is an easy job. These are trying times, these are major challenges, this is a new Department, and you confront these dangers and uncertainties every moment of every day. We do appreciate your willingness to testify before the Committee. You have made yourself far more available than the Attorney General ever has. I believe that the Administration as a whole should take these concerns to heart and work with Congress to get the funding needed to address our security vulnerabilities, even at the cost of forsaking some of the President's tax cuts. We simply cannot meet our needs with the resources that we have available. I would urge the Secretary to convey this message to the White House.

We thank you for your testimony today.

#####

WRITTEN TESTIMONY FOR SECRETARY TOM RIDGE
U.S. DEPARTMENT OF HOMELAND SECURITY
to the
Senate Judiciary Committee
June 9, 2004

Good morning, Chairman Hatch, Senator Leahy, and members of the Committee. I am pleased to have the opportunity to address you today on our progress at the Department of Homeland Security and our efforts in leading the national effort to help secure our country.

As we know too well, despite our nation's successes in the global war on terror, our enemies are still dangerous and more determined than ever to attack us here at home. We must be equally determined to stop them, to protect Americans and the American way of life.

In the aftermath of September 11th, President Bush and the Congress worked together to prepare our country for the future. They created the Department of Homeland Security to provide a central point of command for the protection of our country and citizens. On March 1, 2003, we opened our doors with the combined efforts of 180,000 people and 22 agencies, together under a common mission and focused on the President's vision for a safe and secure America.

In order to accomplish our goals for this new Department, we built bridges to one another, ones that interconnected capabilities and people, ones that invited, rather than impeded, two-way channels of communication. We knew from the outset that our vast scope of protective measures had to build upon our existing strengths but, more importantly, be reconstructed in a way that unified and facilitated speed, openness, and easy access for all those involved in the hard work of securing this country every day.

Presidential initiatives, like the USA PATRIOT Act and others, began tearing down the walls that prevented our policy makers from having the benefit of intelligence analyses that were based on all available information. That's just one of the Patriot Act provisions that are so vital to the continued ability of the Department of Homeland Security to work to prevent terrorist attacks and of the reasons why I so strongly support the President's call for Congress to renew those provisions of the Patriot Act that will otherwise expire next year. These tools are important as we build more integrated and coordinated homeland security, intelligence, and law enforcement communities.

We began eliminating roadblocks that once prevented communication between the Federal government and our partners in states, cities, counties and towns across America. Now, we are replacing them with an active, multi-layered communication system between all levels of government.

We began to connect once disjointed pathways between preparation and prevention. Now, we are establishing a cohesive strategy that combines vulnerability and threat assessment with infrastructure protection.

We began to confront old obstacles that divided the tremendous capabilities of thousands of security professionals from policemen to sheriffs and firemen to EMTs. Now, we are enhancing the abilities of first responders with interoperable standards for communications and equipment.

We began to fully integrate and coordinate our efforts at the national level, paving the way for the Department of Homeland Security as the national focal point for security and protection.

***

The President created the Department of Homeland Security not only to tackle existing tasks, but to recognize and develop new and better methods for accomplishing the job of homeland security and to develop initiatives and systems that we have never taken – or needed to take – to protect our country.

One of the most important "new measures" we have deployed is the integration of the Department into the new homeland security, intelligence, and law enforcement communities that the President has developed in the post-September 11th world.

The establishment of the Department of Homeland Security has created a new analytic capacity, combining specific threat information and actionable intelligence. This new capability allows us to share important information with those who need it most, individuals at the state and local levels.

Let me be clear, the Department of Homeland Security is not specifically in the traditional intelligence collection business – although many of our components collect significant amounts of information – but we are in the analysis and application business. We turn this information into actionable intelligence, which we then disseminate to those who need it most – at the state and local levels.

We interface with all components of the Intelligence Community, including the Terrorist Threat Integration Center (or TTIC), in order to synthesize, analyze and apply information collected from thousands of sources, from electronic surveillance to human reporting.

For instance, our National Targeting Center looks at information from both internal and external sources – such as passenger information and cargo manifests – and combines it with intelligence and threat information. To this end, I am happy to report that DHS has just signed an important agreement with the European Union that permits the legal transfer to DHS of advanced passenger name record (PNR) data from airlines flying between EU countries and the United States. The National Targeting Center uses PNR data in combination with a host of other passenger, cargo intelligence and threat information to conduct a risk analysis that helps to identify potential terrorists and terrorist targets for additional scrutiny. During the period of heightened alert last December, the targeting center played a pivotal role in analyzing passenger manifest information related to several international flights that were determined to be at risk, in order to ensure that passengers on board did not pose risks to the flights.

Information from the Intelligence Community is not the only kind of information with which we deal. Every day, the Department is sharing important information with homeland security partners across the Federal government and throughout the country at the state and local level. For example, we coordinate our visa and foreign traveler policies with the Department of State; through the FBI, we alert law enforcement personnel and homeland security directors to threat information; we work with fire chiefs and emergency managers on procedures and potential forms of attack; and combat computer viruses with Chief Information Officers in the private sector and governments at all levels.

The Department has made information sharing the hallmark of our new approach to homeland security – and we have developed new tools for communication that reach horizontally across Federal departments and agencies and vertically to our partners at the state, local, territorial, and tribal levels as well as the private sector.

Under the umbrella of the Homeland Security Advisory System, the Department is working to improve coordination and communication among all levels of government, the private sector, and the American people.

This communication tool includes the color-coded Threat Condition, as well as several products that allow us to tailor specific information for specific recipients – a part of the country or an individual sector.

The Department issues Threat Advisories, which contain actionable information about an incident or threat to critical infrastructures, networks, or resources; and Information Bulletins, which impart less-specific information about terrorists' general tendencies, tactics, or strategies and are usually not specific about time or place. This communications process – which represents the first ever centralized effort of its kind in the Federal government rather than relying on the fragmented system that existed before – not only outlines threats, but also recommends specific steps that can be taken to heighten readiness or improve physical protections.

Let me share with you a couple of examples of bulletins that were sent to the front lines – issued to first responders across the country that can use the information to secure our hometowns. A recent bulletin titled "Potential Terrorist Use of Official Identification, Uniforms, or Vehicles" noted that "al-Qaida and other terrorist groups likely view the theft or other illegal acquisition of [these items] as an effective way to increase access and decrease scrutiny in furtherance of planning and operations."

And another bulletin last year regarding "July 4th General Awareness" recommended that facilities heighten security forces, maintain irregularly timed security sweeps, and conduct thorough identity checks.

Of course, this is just a sampling of the information we make available to security professionals across the country. Over the course of our first 14 months, the Department has issued more than 90 alerts and advisories to the American public, Federal, state, and local governments, or the private sector. Together with the response from our partners across the country, they are constantly helping to improve our security posture.

It is important to note that communication is a two-way process – not an information blast, but a true exchange. We collect information from the field and listen to what our partners need from us in order to do their jobs better. This means heightened awareness, better intelligence, wiser decisions, and improved coordination at every level. To that end, we have created several new two-way channels of communication, including the National Infrastructure Coordination Center (or NICC) – created for the private sector – and the Homeland Security Information Network (or HSIN) – created for use by government entities.

The NICC provides a centralized mechanism for the private sector, industry representatives, individual companies and the Information Sharing and Analysis Centers – or ISACs – to share and receive situational information about a threat, event, or crisis. The NICC also supports the Homeland Security Operations Center – a 24-hour, 7-days-a-week nerve center that enables the Department to monitor activity across the country. Obviously, this tool would not be effective without the participation of our partners across America.

One of the ways we receive this input is through the recently launched Homeland Security Information Network (HSIN). This real-time collaboration system is already used by more than one

thousand first responders, mainly from the law enforcement community, to report incidents, crimes and potential terrorist acts to one another and to the Department through our 24-hour Operations Center.

It was developed by state and local officials in partnership with the Federal government. It allows multiple jurisdictions, disciplines and emergency operation centers to receive and share the same intelligence and tactical information - so that those who need to act on information have the same overall situational awareness.

Through the Homeland Security Information Network, we are expanding our connectivity and counterterrorism capabilities to two new communities – senior decision makers such as Governors and Homeland Security Advisors and Emergency Operations Centers.

In addition, the information network will eventually provide these collaborative and analytic capabilities to all 50 states, territories, tribal governments and major urban areas. By the end of the year we will achieve real-time nationwide connectivity.

In fact, by this fall more than 5,000 officials will be linked through the Homeland Security Information Network. Every homeland security advisor will have access to the information network, as will Governors, Adjutants Generals, state and urban Police Departments, and Emergency Operations Centers across the country. And by year's end, we will be able to share classified information up to the "Secret" level, and provide training for sensitive information management and use. Over time, the full suite of applications on the information network will be available on the robust national classified information sharing system that we are developing.

In the future, with our state and local partners, we will expand this information sharing environment - while continuing to safeguard classified information - to an ever-widening circle of first responders for ever-increasing layers of coordination and communication between those tasked with protecting our homeland. In short, the Homeland Security Information Network will be both user-friendly and used by more of our partners.

It's important to note – this is a tool of prevention. The main goal of this network is to stop an attack before it ever comes to fruition. Through this system, states will be able to immediately communicate to their county and local partners – creating their own communications networks. And in the future, the private sector will be able to access the system so they can coordinate their preparedness efforts with ours.

During last year's blackout we concluded early on through local reporting to this information network that terrorism was not a likely cause. And more recently, we were able to dispel rumors of evacuations from government offices in Washington, D.C. This capability saves cities countless man hours and precious dollars.

The Homeland Security Information Network communities have also been the cornerstone of our efforts to protect our national monuments and secure holiday celebrations and special events such as the Super Bowl and this past New Year's Eve celebrations. I have watched first hand as state, county and city Operations Centers from across the country went on-line, sharing information and viewing the same operational picture in real time.

Just as important, improvements in our communication – and cooperation – are not limited to the domestic front. During last year's Christmas holiday period, we were able to communicate quickly and effectively with security officials on the ground in England, France and Mexico to recommend and implement plans to mitigate terrorist threats to airline passengers traveling to the United States.

This is an example of the tangible results we have produced by focusing our efforts on effective two-way communications. Here at home, for instance, field agents guarding our Nation's borders stop individuals when necessary based on information provided by the Department and, in return, report back to headquarters with information that can be analyzed for helpful intelligence. The head of my intelligence analysis unit even spoke directly with a state trooper in Wyoming after a routine traffic stop – in order to clarify potential threat information.

***

Some of the most important pieces of intelligence or information that we receive have to do with potential targets. Once we take into account all of the information that is available, we are using a risk management strategy to anticipate threats, protect our infrastructure, and prevent attacks.

The responsibility is great, and the practical challenge is even greater. We share nearly 7,500 miles of land border with Canada and Mexico, across which more than 500 million people, 130 million motor vehicles, and 2.5 million rail cars pass every year. We patrol almost 95,000 miles of shoreline and navigable waters, and 361 ports that see 8,000 foreign flag vessels, 9 million containers of cargo, and nearly 200 million cruise and ferry passengers every year.

We have some 445 primary airports and another 124 commercial service airports that see 30,000 flights and 1.8 million passengers every day. There are approximately 110,000 miles of highway and 220,000 miles of rail track that cut across our nation, and 590,000 bridges dotting America's biggest cities and smallest towns.

That is just a thumbnail of the vast infrastructure that supports the largest and most efficient economy in the world – with more than $11 trillion in Gross Domestic Product.

Of course, we cannot protect all of it, every single day, against every form of attack. We must find a way to strike the right balance between protection and progress. As a result, for the first time, we are employing a risk management methodology to prioritize our efforts. It doesn't mean that we are giving up on one area in favor of another. It means that we are trying to be as analytic and efficient as possible to keep ahead of our terrorist enemies.

We are employing our improved two-way communications as an integral aspect of the first of five steps in our new risk management methodology. In the first step, we determine which targets might be most attractive to terrorists, including key resources and sectors such as the Internet, telecommunications, nuclear and chemical facilities, water, energy, and transportation systems, banks and financial centers, and national – or natural – monuments, icons, and treasures. We do this, as I mentioned, by collecting vast amounts of data from our partners.

Next, we assess the vulnerabilities of these sites – whether they have good security systems, effective counter measures in place, or strong defenses against entry and infiltration. Third, this information is analyzed according to the threat environment that exists – including information from the intelligence community – and prioritized to determine which sites or sectors pose the greatest risk.

We then use this information to strategically build or bolster protective measures and, lastly, evaluate our progress.

The threat environment surrounding our critical infrastructure changes by the hour – even the minute. We recognize that our enemies are nimble, clever, and extremely persistent. They are able to evaluate our security measures and develop new methods of attack, on new sectors and assets, and in new areas of the country. As a result, our priorities can – and must – change quickly. Today's highest risk sector might be tomorrow's lowest priority – and vice versa.

That is why we are developing a National Infrastructure Protection Plan (NIPP) in coordination with our partners across the public and private sectors, as mandated by President Bush in his Homeland Security Presidential Directive Seven (HSPD-7). By the end of this year, the final NIPP plan will outline a consistent baseline for protection standards and protective measures for each sector of critical infrastructure. This will guide the actions of Federal agencies, state and local governments, and private sector owners and operators, helping them move toward prioritized and consistent levels of protection against terrorist attacks across all of our critical infrastructure sectors.

This process of integrating widespread protection efforts with a dynamic, real-time map of vulnerable critical infrastructure has never been done before on the national level. We are working to make it an effective tool throughout the Department of Homeland Security.

***

The combination of new abilities in information sharing, improved two-way communications, and our unique infrastructure protection plan has given the Department capabilities that the Federal government has never had before. Most importantly, it means we can act to prevent terrorist attacks and protect Americans. We have emerged from a static security environment into a dynamic, real-time, action-oriented system of layered protections…on air, land, and sea.

Before the Department was created, America's homeland security functions focused largely on law enforcement and interdiction. Today, strong action and decisive leadership dictate the steps we take to implement protective measures or respond to various threats. We have greatly enhanced our overall capability to *act* – and we do so at three strategic levels: operational, tactical, and incident driven.

Every day, our job is to work to make our country more secure, so during our normal operations, we protect infrastructures or geographic areas as a result of non-specific strategic threats. I would like to emphasize that our normal operations mode still represents a higher level of alert and a greater commitment to vigilance than has ever existed in the Federal government. We are constantly evaluating our intelligence, our inventory of infrastructure, and a threat environment that literally changes by the hour and day.

Even in this ever-changing environment, however, we believe that terrorists will consistently target certain sectors and consistently look to use certain types of attack. That knowledge allows us to operate at a high level of awareness, even in our normal mode. As a result, we place special emphasis on these sectors in our daily operations, and by the end of this year we will have increased security in many of the highest risk areas.

We also think that terrorists will continue to attempt to utilize airplanes and other transportation systems as weapons of mass destruction, so we integrate this knowledge into our ongoing efforts to shore up vulnerabilities in our transportation sector. Earlier this year, we worked closely with metropolitan transit police departments to raise awareness of the threat of attack on transporters of "toxic inhalation hazard" materials, which could expose populations to hazardous chemicals carried in rail cars, and worked closely with other federal agencies to recommend and begin implementing protective actions to reduce this vulnerability. In a separate effort during the Holiday alert period, we have worked closely with industry and the Department of Transportation to study all existing security gaps and are currently designing a risk mitigation strategy to reduce these risks. We have issued security directives to metropolitan transit agencies, commuter and passenger rail operators requiring that they implement protective measures to counter the threat of attack to the passenger rail system. And for the long term, we have begun to work with the private sector to design and develop more secure rail cars for carrying toxic chemicals.

If we receive threat information for specific cities or sectors, information on which we can take action, we move from our normal stance into the tactical operation mode – a new dimension of protection unique to the operations of the Department. At this point, we increase or accelerate protective measures at the site of these targets.

Lastly, as we saw during the period over the holidays when the threat level was raised to Orange, we have the ability to operate in an incident-driven mode. In this case, we act quickly on reliable intelligence about a specific city, building, event, or type of attack. For example, just last month, we discovered a critical vulnerability in some of the routers that control much of the global Internet infrastructure. If exploited, this security gap could have caused a large-scale disruption to the operation of the Internet, impacting the economy and security of the United States and nations around the world. However, DHS, in cooperation with several private sector firms and government agencies, was able to quickly disseminate a warning and patch for this vulnerability through the U.S. Computer Emergency Readiness Team – or U.S. CERT. In this case, we reduced a global security risk in a matter of hours.

In this situational mode, the Department draws on all of the new capabilities I have just outlined for you – heightened DHS involvement in analyzing intelligence, widespread coordination at the Federal level, and intense two-way communications. This is when the hard work of early preparation and active engagement pays dividends.

Let me give you a sense of what this actually looks like.

On December 21, 2003, I announced to the public that we had raised the Threat Condition from an Elevated to High risk of terrorist attack – or from Code Yellow to Code Orange.

Before the decision was made to raise the level, the Intelligence Community received a substantial increase in the volume of threat-related intelligence reports. Credible intelligence sources suggested that there was the possibility of attacks against the homeland around the holiday season, a possibility that appeared to be greater at that point in time than at any moment since September 11th. The information we received indicated that extremists abroad were anticipating near-term attacks that would rival – or exceed – the scope and impact of those we experienced in New York, at the Pentagon, and in Pennsylvania on September 11th.

This collection of information and intelligence was enough to warrant a nationwide alert, and that is what we did by raising the Threat Condition to Orange – which is designed to trigger a series of protective actions by homeland security professionals across the country. We briefed the nation's Governors, Homeland Security Advisors, Mayors, and other local officials and asked them to review the security measures they had in place, and advised them to increase protections to thwart terrorist attacks.

This was the beginning of three weeks of consistent two-way communications between the Department and our partners throughout the country. Our Office of State and Local Government Coordination was in constant contact with homeland security officials in states, cities and counties across America and received routine periodic updates from higher risk areas on the protective measures they were implementing to keep citizens and infrastructure safe from attack. Our Office of Private Sector Liaison reached out to several thousand companies and organizations with the Department's instructions for heightened alert and increased vigilance. And our 24-hour Homeland Security Operations Center – and Interagency Incident Management Group – fielded thousands of calls during this period and shared vital information with our national and international partners.

The response around the country to this call to action was exceptional. There was an increased police presence at shopping malls, train stations, power plants, and large gatherings such as sporting events and holiday celebrations. Emergency communications plans were implemented and watch centers were activated. We increased our detection capabilities by deploying sensor equipment in different parts of the country, including expanding our BioWatch program. We took important steps to ensure coordination at every level, such as placing local law enforcement personnel in our headquarters command center, providing air marine assets to several major events, and sending DHS personnel to monitor actions on the ground in areas of special attention across the country. And we encouraged individual citizens to review – or develop – their family emergency plans or Ready Kits. We implemented broad security measures and, when the situation warranted, we recommended and, in some cases, carried out ourselves, targeted actions such as grounding high-risk flights headed for the United States from overseas.

We know that greater security plus added vigilance is a deterrent; and, thankfully, this time of heightened alert passed safely and without incident. Each time we raise the Threat Condition, which we have now done five times since August 2002, we learn more about the process and improve our abilities to communicate and coordinate effectively with the public, with the private sector, and with our partners at every level of government.

As these examples show, the Department of Homeland Security operates at the strategic, tactical, and situational level every day – moving seamlessly between them as the situation dictates. By having a single integrated department, we have leveraged tremendous resources and created capabilities that never existed before September 11th.

***

Another area where major changes have been implemented is in the way we welcome people to our country. The experience of traveling to the United States has changed for millions of foreign visitors over the past two years. The U.S. government has created new procedures, laws and travel regulations, stepped up the enforcement of existing laws and processes, and – in creating the Department of Homeland Security – restructured many travel processes, functions, requirements and

responsibilities. And more changes are coming. Over the next several years, Homeland Security will continue to enhance its systems and introduce new elements to the international travel experience.

As a result, the challenge of creating awareness, understanding and support for U.S. travel policies among diverse publics has increased substantially. The United States today finds itself struggling to catch up with these changes and, in many cases, to ameliorate unfavorable attitudes and perceptions about traveling to the United States.

Our policies have been designed to keep our borders closed to terrorists but open to legitimate, law-abiding visitors. They deserve to travel on secure airlines and vessels; to be processed efficiently through our ports and border crossings; and to have their privacy respected and protected from abuse. And once here, they deserve to live in safety -- not in fear of terrorists, criminals and fugitives from the law. That is the charge of our open, welcoming nation -- a champion of freedom at home and abroad. I believe the changes we favor will help us preserve those freedoms and protect all individuals from harm.

Currently, 27 nations are members of the Visa Waiver Program, or VWP. Under the program, citizens of participating countries are allowed to travel to the United States for tourism or business for 90 days or less without obtaining a visa.

The policy encourages travel and trade between the United States and our allies. However, one unintended consequence of the policy is a potentially significant gap in security as those wishing to avoid visa security checks conducted at U.S. consulates abroad attempt to take advantage of the program.

One of the responsibilities of the Department of Homeland Security, in consultation with the Department of State and other relevant agencies, is to determine whether the continued participation of a particular nation in the VWP poses a threat to the national security or law enforcement interests of the United States, and therefore should be ended.

The Enhanced Border Security and Visa Entry Reform Act requires that beginning on October 26th, 2004, Visa Waiver Program countries have a program in place to issue their nationals machine-readable passports. They must be tamper-resistant and incorporate biometric and document authentication identifiers that comply with International Civil Aviation Organization (ICAO) standards.

The law also requires that visitors coming to the United States under the VWP present these new biometric and machine-readable passports if they were issued on or after that date. VWP travelers with non-biometric passports issued after 10-26-04 will need a visa to enter the United States.

Extension of the Deadline

We have learned that while most Visa Waiver Program countries will be able to certify that they have a program in place to issue biometric passports by the October 26th deadline, few, if any, of these countries will actually be able to produce biometric passports by that date.

Under the current deadline, millions of visitors from Visa Waiver Program countries who do not have ICAO-compliant passports will have to obtain visas prior to traveling to the United States.

As my colleague Secretary Powell has indicated in a hearing last month, this sweeping change will place a great burden on our consulates and have significant negative implications on tourism, travel and commerce. So relief is critical. Secretary Powell and I are extremely encouraged by the progress that has already been made by Visa Waiver Program countries to meet the emerging ICAO

standards. We will continue to work with them to help them meet the mandatory deadlines. It must be noted that the reason these countries cannot meet the October 26th deadline is not a lack of will or commitment, but rather challenging scientific and technical issues.

For those same technical reasons, the Department of Homeland Security is not currently in a position to acquire and deploy equipment and software to biometrically compare and authenticate those documents. Further, adhering to the original deadline also would likely prevent us from creating a system that is interoperable for all nations. Like the foundation of a house, interoperability must be built into the system from the very beginning. To do otherwise would prove extremely expensive, time-consuming and difficult.

Acknowledging the current limited state of technology and the potential for harm to our relations with our closest allies, the Department, as stated earlier, requests that the October 26th, 2004, deadline under the relevant sections of the Enhanced Border Security and Visa Entry Reform Act be extended to November 30th, 2006.

The US-VISIT Program

Despite these challenges, we have identified a partial solution that we believe will allow us to improve the nation's security and the integrity of the Visa Waiver Program. This involves enrolling Visa Waiver Program travelers in the US-VISIT system, beginning this fall.

US-VISIT represents the greatest single advance in border technology in three decades. The Department has established US-VISIT to:

- Enhance the safety of our citizens and visitors;
- Facilitate legitimate travel and trade;
- Ensure the integrity of our immigration system; and
- Protect the privacy of travelers to the United States.

US-VISIT represents a continuum of security measures that uses biometrics as a key element. Biometrics such as digital, inkless fingerscans and digital photographs enable the Department to determine whether the person applying for entry to the United States is the same person who was issued the visa by State. Both State and our Department use biometric and biographic data to check against appropriate "lookout" data.

The Department deployed the first increment of US-VISIT on time and within budget. And, as it includes biometrics ahead of schedule, we have exceeded the mandate established by Congress.

On January 5th, 2004, US-VISIT entry procedures were operational at 115 airports and 14 seaports. By the end of the year, US-VISIT will be in operation at our 50 busiest land ports of entry. We have also begun pilot-testing biometric exit procedures at one airport and one seaport and will expand to additional pilot locations later this summer.

US-VISIT procedures are clear, simple, and fast for visitors. On average, US-VISIT procedures take less than 15 seconds per person during the inspection process. As of the beginning of May, more than 4 million foreign visitors have been processed.

As impressive as its speed is already US-VISIT has matched more than 300 persons against criminal databases, preventing more than 100 known or suspected criminals from entering the country. More than 200 were matched while applying for a visa at a State Department post overseas.

As noted earlier, we are also dedicated to safeguarding travelers' privacy. We have extended the principles and protections of the 1974 Privacy Act to all individuals processed through US-VISIT. And US-VISIT features a three-stage process for redress if an individual has a complaint.

Visitors to this nation have a right to be secure from criminals and predators. US-VISIT has helped to make that right a reality.

One example: on December 28th, 2003, an international traveler appeared for inspection at Newark International Airport. Standard biographic record checks using a name and date of birth would likely have cleared the individual. However, when his fingerprints were scanned and checked against the US-VISIT biometric database, it was revealed that he was a convicted felon who had been previously deported from the United States. He had used multiple aliases to disguise from authorities his record of rape, assault, criminal possession of a weapon, and the making of terrorist threats.

Similar examples abound. A fugitive drug trafficker was captured after two decades on the run. A traveler sporting three Social Security numbers and a 14-year criminal history was nabbed. And just weeks ago, an airline crewmember was biometrically identified as having been convicted for forgery and violation of electronic funds transfer accounts. Crewmembers are not exempt from US-VISIT. She was sent home and her visa was cancelled.

Through US-VISIT, our two Departments have identified numerous criminal and immigration-law violators who otherwise would have disappeared. Every day the system highlights the importance of using accurate, timely information to protect our nation from terrorists and criminals – and, I would add, to protect innocent non-citizens and their families from being tarred with a broad brush or targeted by mistake. By focusing on individual behavior, US-VISIT and programs like it help reduce our reliance on more arbitrary and unfair standards such as nationality.

VWP and US-VISIT

In FY 2003, the Department of Homeland Security recorded the admission of approximately 13 million Visa Waiver Program traveler visits through air and sea ports of entry.

By expanding US-VISIT to include processing of Visa Waiver Program travelers, the Department expects to double the number of admissions processed through US-VISIT, thus enhancing the integrity of our borders.

I would add that there are some travelers from Visa Waiver countries who are required to obtain nonimmigrant visas, and so have already been successfully processed through US-VISIT. Since its implementation, approximately 400,000 nonimmigrant visa holders from Visa Waiver Program countries have been processed.

Earlier this month we briefed ambassadors of Visa Waiver countries on this change, and overall they are supportive. A European Commission spokesperson told the Wall Street Journal that, "We [will] work closely with the U.S., with whom we share counterterrorism goals, to ensure that any new measures are introduced with minimum disruption and maximum safety."

These Visa Waiver Program countries appreciate our interest in increasing security as well as our support for the deadline extension to enable them to follow our lead.

Many of them, including Australia, the Netherlands, and Singapore, are actively engaged in developing programs that will allow them to collect biometrics and match the data upon a visitor's entry. We are working with many of these countries to share information about terrorism and other security threats, in addition to opportunities for improvements in immigration and border management.

And we are working with Secretary Powell to get the word out that the United States remains an open and welcoming nation to those who wish to live, work or study here.

Yes, this new era demands new security requirements, such as mandatory interviews for visa-holders, small processing fees, and the verification of a student's enrollment status through our Student and Exchange Visitor Information System, or SEVIS, which serves nearly 10,000 campuses across the country.

But it also demands that we extend a helping hand. Our SEVIS "Tiger Teams," for instance, show up at airports as foreign students arrive to help them navigate the process. They serve as on-scene ombudsmen, contacting the universities and trouble-shooting so that legitimate students are not left behind.

US-VISIT is critical to our national security as well as our economic freedom. It is already making a significant contribution to the Department's efforts to provide a safer and more secure America.

We recognize that we have a long way to go. We will build upon this initial framework and solid foundation to ensure that we continue to meet our goals of enhancing our security while facilitating travel for the millions of visitors we welcome each year.

We are committed to a program that enhances the integrity of our immigration system, that catches the few and expedites the many – and, above all, that keeps our doors open and our nation secure.

Countries in the Visa Waiver Program are our closest allies and economic partners. A two-year extension of the October 26th, 2004 biometrics deadline will permit these allies to remain in the Visa Waiver Program. And processing Visa Waiver Program travelers through US-VISIT will help our two Departments – and nation -- achieve our security objectives.

***

The tools we have developed have now become a formidable force multiplier in the effort to secure and protect America. The first year's accomplishments have provided an excellent foundation for future work – and there remains plenty to do. That is why we have recently completed the Department's first high-level Strategic Plan – which includes vision and mission statements, and a set of strategic goals and objectives that provide the framework for our daily operations into the future.

I'd like to discuss the Department's seven key priorities for the coming year. I think they will provide the Committee with some insight into where our collective homeland security efforts have been and where they are going in the future.

1. Stronger Information Sharing and Infrastructure Protection

Our first goal is to further improve information sharing and infrastructure protection. I have already provided many of the details of our efforts, but suffice to say that we will dig deeper into our efforts – specifically, work in greater tandem with the private sector to strengthen vertical communication

systems and significantly increase permanent protections around our nation's most vital assets. The goal is to maximize real-time sharing of situational information – without delay, and with full throttle distribution of intelligence to those in the field who need to act on it.

By the end of this year, we intend to complete vulnerability assessment guidelines for three critical infrastructures: chemical, petroleum and nuclear The Department has been working with industry through the American Society of Mechanical Engineers(ASME) to develop guidelines for each of the eight critical infrastructure subsectors: chemical facilities, nuclear power plants, nuclear spent fuel storage facilities, petroleum facilities, liquefied natural gas storage locations, railroad bridges, subway systems, and highway tunnels. The Department with the assistance of ASME will work to standardize these guidelines as they are vetted through the various infrastructures.

We are building the National Assets Database, a national inventory of physical critical infrastructure that contains thousands of sites and is growing literally every day. This is a dynamic document that is constantly updated to include additional sites based upon the ever-changing threat environment in which we operate.

2. Standards for Interoperable Communications and Equipment

Part of the tragedy of September 11th was that equipment didn't work across jurisdictions and disciplines. Fire department radios couldn't transmit to police department radios. Firefighters rushing in from other cities and even neighborhoods were, in some cases, unable to assist because the couplings that attach "hoses to hydrants" simply wouldn't fit; they weren't compatible. Our first responders are first on the scene and their ability to communicate and work with each other in the event of a crisis is paramount – and their inability to do so is a long-standing, complex and critical issue facing this Nation.

We are employing a two-track strategy as we work to solve this problem. There are immediate steps the Department can take in the short term, while we focus everyone's attention on a long-term, integrated solution to overall interoperability. Already, for example, the Department has identified technical specifications for a baseline incident interoperable communication system. If adopted at the state and local level, by the end of 2004, most first responders will have a way to communicate with each other during a crisis, regardless of frequency or mode of communication.

The Department also recently announced the first comprehensive Statement of Requirements for communications throughout the first responder community. This set of standards marks the first time in history that 50,000 public safety agencies across the country will have a common standard for wireless communications and interoperability. This will serve as an important tool that will bring governments, public safety officials, the communications industry, and future research and development efforts together under a common mission.

We have also adopted the first set of standards regarding personal protective equipment developed to protect first responders against chemical, biological, radiological and nuclear incidents.

These standards, which will assist state and local procurement officials and manufacturers, are intended to provide emergency personnel with the best available protective gear – allowing them to protect themselves, as they work to protect others.

I am pleased to report that all of the Department's efforts in this area will be coordinated by a new Office of Interoperability and Compatibility. Much of their work has already begun, and they will continue to coordinate and leverage the vast efforts spread across the Federal government to reduce unnecessary duplication in programs and spending, identify and promote best practices, and conduct research and development, testing and evaluation, develop standards, provide technical assistance, training, and develop grant guidance for interoperability between local, state, and federal agencies.

This office will focus not just on interoperable communications, but also on the gear that will be used by multiple jurisdictions – firefighters and police officers from different neighborhoods – as they join together to respond to a major event. In addition, this Office has initiated a program aimed at providing communications interoperability at disaster sites in the near term, and we expect multiple cities to achieve this goal sometime this fall.

These immediate steps at the Federal level will begin to build a foundation for longer-term efforts and a truly national solution.

This second track will require actionable results at the state and local level – in other words, a resolve not to let an incompatible radio frequency or a too-small/too-large piece of safety equipment impede the ability of brave men and women to save the lives of citizens...as well as their own. A truly nationwide interoperable system demands commitment from leaders at all levels – and we are already beginning to see a commitment to this important principle.

3. Integrated Border and Port Security Systems

The President quickly acted to strengthen security at our borders – welcoming the free flow of trade and travelers, while keeping terrorists out. We unified the inspection process – presenting "one face" at the border – and in doing so, nurtured better morale, improved service, and reduced delays. One face at the border streamlines our personnel and our processes, joining customs, immigration, and agriculture inspectors together under one chain of command, one set of rules and guidelines, and one multi-faceted training program. Today, our Customs and Border Protection Officers are being prepared for all three elements of border enforcement.

The President took immediate and extensive measures to enhance aviation security. In less than a year, America deployed newly trained screeners and thousands of Federal air marshals, hardened cockpit doors on aircraft, and introduced state-of-the-art technologies, which, from the curb to the cockpit, have made airline travel safer.

We launched the US-VISIT program at 115 airports and 14 seaports across the country. Now, the "smart technology" of biometrics is speeding the entry of millions of travelers, and stopping criminals before they enter our country. To date, more than 4 million passengers have been processed through US-VISIT, and more than 400 passengers have been apprehended or prevented from entering the country, including one prison escapee who had been on the run for more than 20 years and another man with 8 aliases who managed to enter the country in December, but was stopped by US-VISIT when he tried to enter again just two months later.

With the help of the FBI and other federal partners, together we also stood up the Terrorist Screening Center to give law enforcement a one-stop shop for information on terrorist watch lists. The screening center continues to make great strides toward total watch list consolidation; and already we are able

to share lists with our border officials at all ports of entry – land, air, and sea – and with state and local law enforcement through the National Crime Information Center – or NCIC.

We also looked at our system for welcoming foreign students, retooled it, and by last fall had a new system in place that ensures that legitimate foreign students are not delayed upon entry – and that those posing as students, seeking fraudulent entry to schools, are stopped in their tracks. Last fall almost 300,000 students were successfully cleared for study at our institutions of higher education. Those two hundred who attempted entry, but were not registered at any school, were sent home.

We significantly expanded the nation's container security initiative, known as CSI. The result: there are DHS inspectors in Rotterdam, in Singapore, in Hong Kong, and 14 other international ports of trade, working alongside our allies to target and screen the nearly 20,000 containers of cargo that arrive from these ports at our shores every day.

To further improve upon the base of border and port security protective measures which we have already established, we will expand the US-VISIT program to our 50 busiest land ports of entry by the end of this year, and add an additional seven Free and Secure Trade lanes, bringing the total to 18 locations.

We will expand the NEXUS and SENTRI trusted traveler programs to expedite the passage of frequent, low risk border crossers that undergo a background check.

We will strengthen the critical partnership with private sector owners and operators of the supply chain through expansion of the Customs Trade Partnership Against Terrorism, which provides business incentives to companies that voluntarily meet a set of government-approved security standards. More than 6,000 importers, carriers, and brokers, including 186 foreign manufacturers, are now enrolled in C-TPAT.

With private sector involvement and support, we will also enhance air cargo security by investing in new research and technology, and expanding pre-screening and known-shipper programs.

We also will deploy aerial surveillance and sensor technology, increase manpower and interagency coordination at specific points along the border, expand the Container Security Initiative to 10 additional high-volume ports, and work with the private sector to facilitate compliance and assessment of new maritime security regulations.

4. Create More Prepared Communities

Since March 1 of last year, we have allocated or awarded a record $8 billion to states, regions and cities to help train and equip our Nation's dedicated first responders.

Now, we want to examine as many ways as possible to broaden communication and coordinate actions, so that when people show up at an incident; they're not meeting for the first time; they're not confused about the chain of command; and they're not lacking for help in their communities as they scramble to aid and assist our citizens in the midst of a crisis.

As part of this effort, we introduced the National Incident Management System – or NIMS – so that those with responsibility for protection at all levels of government and the private sector understand what their role will be – and will have the tools they need to be effective.

NIMS is the Nation's first-ever standardized approach to incident management and response – and it unifies Federal, state, and local lines of government into one coordinated effort.

NIMS makes America safer – across our entire Nation and throughout every neighborhood – by establishing a uniform set of processes, protocols, and procedures that all emergency responders, at every level of government, will use to conduct response actions.

For the first time, all of the Nation's emergency teams and authorities will use a common language, and a common set of procedures when working individually – and together – to keep America safe.

The Department is also developing the National Response Plan to integrate all of the current Federal response capabilities under a single "all hazards" system for prevention, preparedness, response and recovery.

The plan is being developed with guidance from all stakeholders – Federal government agencies, state, local, and tribal officials, as well as first responders. This working blueprint will enhance current Federal capabilities and will unify the team that will be charged with responding to potential attacks or disasters.

We are also building a foundation on which the private sector can take important steps to improve their readiness. The ANSI/NFPA 1600 – a set of voluntary standards developed by the American National Standards Institute and the National Fire Protection Association – empower the private sector to examine their own readiness and take part in the shared responsibility of homeland security. These standards encourage mutual respect, cooperation, and open communication – essential elements of our national approach to readiness. Voluntary standards like these – and the process used to develop them – help make us smarter about how to perform our duties better, and give us direction and guidance in the areas we need them most. They are just one tool – but an important one – in our effort to make our country more secure.

Citizens are just as integral to combating terrorism as any state and local government or private company. Terrorism is insidious. Terrorists seek to infiltrate our society, scope out targets, and wage war in our streets and cities.

And so, to achieve a national movement toward an integrated and seamless degree of protection, it's vital that we continue to reach out to our citizens and empower them to play a direct role in securing their families and their communities.

The Department of Homeland Security will focus its efforts on raising the baseline level of preparedness across the Nation.

We will continue to educate the public about the importance of being prepared for all emergencies, whether wrought by disaster or design. Our goal over the next year will be to accelerate the basic level of citizen preparedness across the Nation. Current research suggests that between 20 to 30 percent of Americans have an emergency supply kit and that 15 percent have a communications plan.

Our desire is that nearly half of all Americans, in some form or combination, will be better prepared by the end of 2004 – whether that's by preparing family Ready kits and emergency plans; volunteering to

aid in disaster planning; or engaging in CPR and training exercises to help someone in a life-threatening situation.

To help push this forward-leaning agenda, by the end of 2004, we will add to the strength of our existing Ready campaign by launching two new citizen preparedness endeavors -- Ready for Business and Ready for Schools. We will also continue to work with third party organizations, such as The American Red Cross and America Prepared – and, of course, Citizen Corps. Citizen Corps' mission is to encourage everyone to participate in making America safer; their councils, which have grown to more than 1,100, have helped us deliver the Ready message at the grassroots level – the level where it's needed most.

5. New Technologies and Tools

Every day we must operate with the knowledge that our enemies are changing based on how we change. As we shore up one vulnerability, they work to uncover another. This is why science and technology is key to winning this new kind of war. The work we do at Homeland Security, in partnership with the private sector, national laboratories, universities and research centers, helps us push the scientific envelope. It helps drive the development and use of high technology to combat the weapons of high consequence. New tools of analysis, information sharing and detection can help us counter terrorist attacks -- before they can happen -- and if they happen, minimize their impact.

For instance, we are developing new capabilities for detecting the presence of nuclear materials in shipping containers and vehicles. We are also developing the next generation of biological and chemical detectors, ones uniquely sensitive enough to not only alert people to the presence of dangerous pathogens, but allow for evacuation by redirecting air flow.

We also established our first three Centers of Excellence and our first class of Homeland Security Scholars and Fellows -- to foster new thinking, new capabilities and new career paths that are so essential to the fight against terrorism.

These capabilities are critical to a war where speed of knowledge and action is vital to the protection of the public. Homeland Security can't drive these advances, only science can, but together with our partners we are taking up the charge to secure our country using the latest technologies available.

6. Improved Customer Service at Immigration Services

Another key priority of this department will be to improve and protect immigration practices, and at the same time improve homeland security. Again, it is part of our mission to ensure that we remain a welcoming nation for people who want a better way of life and who want to make a contribution to the great American story – but also to keep our borders and communities closed to terrorists.

Citizenship has long been among the most important privileges this Nation can bestow. And, as the Department that oversees this critical function, we are committed to making the immigration and naturalization process a welcoming and timely one. Our four new pilot programs – two in the Los Angeles area, Dallas and New York City – are aimed at reducing the backlog of pending cases and streamlining the citizenship process, while strictly protecting the privacy and civil liberties of everyone involved. Already in Dallas, the project called the I-130 Pilot has been a proven success. This

customer service initiative aims to complete the "adjustment of status" process within 90 days. In Los Angeles, the I-90 pilot aims to reduce the wait time to replace or renew a permanent resident card or green card from a year to less than a week.

We will soon expand our E-Filing initiative, allowing applicants to complete several of the most popular forms online. Last year E-Filing began with two forms – an application to replace a green card and an application for employment authorization. Soon this customer service initiative will support eight forms that account for more than 50% of the applications for benefits filed each year. The new forms will include the application for Temporary Protected Status, employment based petitions and change of status. By the end of fiscal year 2006, E-Filing will include a total of 12 forms that will account for more than 90% of the applications for benefits filed yearly. We have also posted processing times – updated monthly – for forms on the United States Citizenship and Immigration Services website.

CIS is also creating an orientation guide to help immigrants better integrate into American society. This guide will introduce local community resources, emergency service providers, and a host of critical information to new residents in our country.

7. Build a 21st Century Department

We're working to build a department that strives to create the model government agency for the 21st century. In a 21st century threat environment, nothing less will do. Of course, just getting up and running operationally was a challenge unto itself – merging 180,000 people, 22 Federal entities, 22 different human resources servicing offices, 8 different payroll systems, 19 financial management centers, and 13 procurement systems.

We have proposed a new human resource system – called MAX HR – which will allow the Department to act swiftly and decisively in response to our mission needs, quickly adapt to the changing nature of our work, and attract, maintain, and motivate a highly skilled workforce.

New provisions include pay for performance and performance management, while preserving labor relations, appeals processes, and protecting the rights and responsibilities of all workers.

The Department has undertaken a resource transformation initiative entitled *eMerge2* which is a business-focused program that seeks to consolidate and integrate the Department's budget, accounting and reporting, cost management, asset management, and acquisitions and grants functions.

We have also instituted a Leadership Development Curriculum that includes "One-DHS" training and candidate development to ensure that our workforce is marked by outstanding leadership and guided by a singular commitment to success.

Today, we operate as a single unit – one team, one mission, one fight. And our management philosophy and leadership development reflect that.

***

The entire Department, in fact, reflects this shared responsibility. We are committed to leading the unified national effort to secure America. We have done so – and will continue to do so – by

developing new and innovative methodologies to prevent and deter terrorist attacks, and protect against and respond to threats and hazards. All the while, we will ensure that we maintain safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce.

Homeland security is not one department or one organization. Homeland security is about building bridges between the people tasked with our Nation's protection, and giving them the tools they need to do their jobs well.

Homeland security is about the integration of a nation, the integration of people and technology to make us smarter, more sophisticated, and better protected.

The entire Department, in fact, reflects this shared responsibility. We are committed to leading the unified national effort to secure America. We have done so - and will continue to do so - by developing new and innovative methodologies to prevent and deter terrorist attacks, and protect against and respond to threats and hazards. All the while, we will ensure that we maintain safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce, and accomplish these goals in a way that is respectful of the civil liberties and personal privacy of our citizens and our visitors.