

**CONFRONTING THE TERRORIST THREAT TO THE
HOMELAND: SIX YEARS AFTER 9/11**

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

—————
SEPTEMBER 10, 2007
—————

Available via <http://www.access.gpo.gov/congress/senate>

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



U.S. GOVERNMENT PRINTING OFFICE

38-842 PDF

WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TED STEVENS, Alaska
THOMAS R. CARPER, Delaware	GEORGE V. VOINOVICH, Ohio
MARK L. PRYOR, Arkansas	NORM COLEMAN, Minnesota
MARY L. LANDRIEU, Louisiana	TOM COBURN, Oklahoma
BARACK OBAMA, Illinois	PETE V. DOMENICI, New Mexico
CLAIRE McCASKILL, Missouri	JOHN WARNER, Virginia
JON TESTER, Montana	JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*

CHRISTIAN J. BECKNER, *Professional Staff Member*

BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*

LEAH Q. NASH, *Minority GAO Detailee*

TRINA DRIESSNACK TYRER, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Lieberman	1
Senator Collins	3
Senator Tester	23
Senator Warner	25
Senator Coleman	27
Senator Voinovich	30
Senator Sununu	32
Senator McCaskill	37
Senator Stevens	42
Senator Akaka	43
Senator Carper	44

WITNESSES

MONDAY, SEPTEMBER 10, 2007

Hon. Michael Chertoff, Secretary, U.S. Department of Homeland Security	5
Hon. J. Michael McConnell, Vice Admiral, U.S. Navy (Ret.), Director of National Intelligence	10
Hon. John Scott Redd, Vice Admiral, U.S. Navy (Ret.), Director, National Counterterrorism Center, Office of the Director of National Intelligence	14
Hon. Robert S. Mueller III, Director, Federal Bureau of Investigation, U.S. Department of Justice	17

ALPHABETICAL LIST OF WITNESSES

Chertoff, Hon. Michael:	
Testimony	5
Prepared statement	59
McConnell, Hon. J. Michael:	
Testimony	10
Prepared statement	73
Mueller, Hon. Robert S. III:	
Testimony	17
Prepared statement	106
Redd, Hon. John Scott:	
Testimony	14
Prepared statement	93

APPENDIX

Questions and responses for the record from:	
Secretary Chertoff	115
Admiral McConnell	137
Admiral Redd	151
Mr. Mueller	155

CONFRONTING THE TERRORIST THREAT TO THE HOMELAND: SIX YEARS AFTER 9/11

MONDAY, SEPTEMBER 10, 2007

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

The Committee met, pursuant to notice, at 9:34 a.m., in Room SD-342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Carper, Pryor, McCaskill, Tester, Collins, Stevens, Voinovich, Coleman, Warner, and Sununu.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. I thank everyone who is here, including, of course, our four witnesses.

Tomorrow—September 11, 2007—people across our Nation, and, in fact, in many places around the world, will pause to mourn and reflect on the terrorist attacks of September 11, 2001.

Today in this Committee room, we rededicate ourselves to the memories of those lost—the families and the Nation that grieve for them. Today we take time to assess the continuing Islamist terrorist threat to America and what our government is doing to protect the American people from an attack like the one that occurred 6 years ago.

Today we ask: What lessons were learned? Where do we stand in our ability to detect and deter the next attack that we know is being plotted? And is our government ready to respond effectively to mitigate the damage to our citizens and our way of life should another terrorist attack be carried out?

The “National Intelligence Estimate: The Terrorist Threat to the US Homeland,” which was issued in July 2007, makes the continuing dangers clear. “We assess that al-Qaeda’s Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the US population.”

While the core of the September 11, 2001, al-Qaeda is weaker and no longer operates under the cover of the Taliban government of Afghanistan—and its forces in Iraq are now on the run—it is clear that the leadership of al-Qaeda has regenerated itself and its hateful ideology is metastasizing across the Internet.

In his tape posted over the weekend, Osama bin Laden may sound like a rambling political candidate of the Internet fringe,

railing against American business, coming out for lower taxes, expressing concern about high mortgage interest rates, and then ultimately making clear that mass conversion to Islam is the best way for Americans to secure our future. Taken by itself, this statement might seem like the ranting of a weird but harmless person. But the fact is Osama bin Laden is a mass murderer who has the blood of tens of thousands of people on his hands. And I am speaking not just of the more than 3,000 Americans who died on September 11, 2001, or in other terrorists attacks against the West, but also in the murder of thousands and thousands of his fellow Muslims—men, women and children—innocents upon whom al-Qaeda has rained indiscriminate death in Iraq, Afghanistan, and throughout the world.

Bin Laden's tape is another shot across our bow. It is the sound of another alarm which calls us to alertness and duty and tells us that bin Laden and his ilk are out there, and so long as they are, the life of every American is endangered.

Consider the most recent plot broken up in Germany—with, I might say proudly, the help of American intelligence operatives. This plot, which German officials have said was professionally organized mostly by native Germans who were radicalized in Germany, was nonetheless carried out by these people after they traveled to al-Qaeda camps in Waziristan for training.

And then remember the actual and foiled attacks that originated in England, Scotland, Spain, Algeria, Denmark, and so many other places—all also locally plotted, some aimed at America and/or American targets.

And then come home and focus on the Fort Dix and JFK Airport plots, which demonstrated beyond any doubt that there are people right here in America who have swallowed the jihadist ideology and are prepared to kill innocent Americans. These are the evils and dangers of our age that we must live with and defend against.

Today, we are most grateful to have as witnesses the four men who are responsible for the protection of the American people from Islamist terrorism. As I look at the four of you, it is striking to me that three of you lead Federal departments or offices that did not exist on September 11, 2001, and were created in legislation that in part was initiated in this Committee, passed by Congress with the support of Members of both parties, and signed by the President, all of which have been aimed at providing better protection to the American people than they were getting from their government on this day 6 years ago.

Let me say clearly that the agencies you four administer, the Federal employees that you lead, and the work that you have done together have made our country a lot safer than it was on September 11, 2001. And, in fairness, though they are not here, of course, I would add the Department of Defense and the Department of State and all who work for them.

There is undoubtedly some luck in the fact that America—contrary to all expectations on September 11, 2001—has not suffered another terrorist attack in the last 6 years. But it is no mere accident and not just luck. It is in good measure, I believe, because of the smart, hard work that you and your agencies have done that we have not been attacked again here at home.

I say this with gratitude, but with no sense of comfort or triumph. You and I know there is more your agencies must do—and do better—and that the enemy remains strong, agile, and eager to attack us again. But on the eve of the sixth anniversary of one of the darkest days in American history, September 11, 2001, it is appropriate that we stop and thank you and your co-workers for all that you have done in the last 6 years to protect us and our homeland.

When we created the Department of Homeland Security, the Director of National Intelligence, the National Counterterrorism Center, and supported Director Mueller's transformation of the FBI, no one intended them to be static offices or organizations. We wanted them to be not just strong and capable, but as agile, flexible, and fast-moving as our enemies.

We are still in the early days of what will be a long war against Islamist extremists. Today we want to consider what we have done and still must do together to secure our homeland and win this war.

I thank you for being here, and I look forward to your testimony. Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Tomorrow is the anniversary of a day that, 6 years later, still defies understanding. The loss of nearly 3,000 innocent men, women, and children, the cruelty of the attackers, and the courage at the Twin Towers, the Pentagon, and on Flight 93 remain beyond the ability of our minds to comprehend fully or our words to express adequately.

It is appropriate that we are holding this hearing today, the eve of this somber day of remembrance. If there is one thing we fully understand about September 11, 2001, it is that the horror of that day was made possible by what has been called "September 10th thinking." What the 9/11 Commission so memorably terms as "a failure of imagination" was exploited by our enemies with devastating effectiveness.

Events in my home State of Maine on September 10, 2001, illustrate the collision course between innocence and hatred.

On that day, Robert and Jackie Norton drove from their home in Lubec, Maine, to Bangor, the first leg of a cross-country trip to the West Coast for a family wedding. Early the next morning, a commuter plane would take the beloved retired couple to Boston, where they would board Flight 11.

On that day, James Roux of Portland, an Army veteran, a devoted father, and a man known for his generosity and outgoing spirit, was packing for a business trip to California. He left Logan the next morning on Flight 175.

On that day, Robert Schlegel of Gray, Maine, was celebrating his recent promotion to the rank of Commander in the U.S. Navy. He was settling into his new office at the Pentagon. His office was believed to be the point of impact for Flight 77.

And on that day, Mohamed Atta and his fellow terrorist rented a car in Boston and drove to Portland. They checked into a motel, ate pizza, and made other preparations. When they boarded their

commuter plane for Logan the next morning to seize control of Flight 11, they left behind a trail of dots—of financing and training, of global travel and visa violations, and of known terrorism involvement—that would not be connected until it was far too late. Complacency, turf battles, and intelligence failures prevented the coordination and communication that just might have allowed the September 11, 2001 plot to be detected in time.

Nevertheless, the people of our great country responded to those attacks with determination, unity, and a sense of purpose. My concern is that our response may be in danger of flagging. If we allow ourselves to become complacent, to revert to September 10th thinking, the next attack will not be due to a failure of imagination but to a failure of resolve.

Today's hearing is held in the context of the "National Intelligence Estimate: The Terrorist Threat to the US Homeland" report. This report judged that the United States will face "a persistent and evolving terrorist threat over the next three years."

The key words are "persistent" and "evolving." This Committee has dedicated itself to anticipating the changing nature of terrorism and to addressing our vulnerabilities. One of our concerns is a central issue raised in the National Intelligence Estimates (NIEs).

That issue is homegrown terrorism. The NIE assessment is that a growing number of radical, self-generating terror cells in Western countries indicates that the radical and violent segment of the West's population is expanding. In our own country, as the Chairman indicated, the Torrance, California, case and the Fort Dix and JFK Airport plots all illustrate that we are not immune from domestic terror cells. Those homegrown terrorists, inspired by al-Qaeda's hate-filled perversion of the Muslim faith, will challenge the ability of our law enforcement and intelligence agencies to respond effectively. And they pose a challenge to all Americans to be observant and to not be afraid to report what they see.

This Committee has conducted extensive investigations of this phenomenon, in particular, the radicalization of prison inmates, the use of the Internet as a radicalizing influence, and the lessons learned by our European allies who also face this threat. I am very interested in discussing with our witnesses today how we can best counter this clear and escalating threat.

The NIE also states that al-Qaeda remains driven by an undiminished intent to attack and continues to adapt and improve its capabilities. Even more disturbing is what the report further concludes: That although worldwide counterterrorism efforts have constrained the ability of al-Qaeda to attack us again, the level of international cooperation may wane as September 11, 2001 becomes a more distant memory and perceptions of the threat diverge.

In other words, we are challenged not just by a ruthless, calculating, and determined enemy, but also by our own resolve. The names of Robert and Jackie Norton, of James Roux, of Commander Schlegel, and of so many others must not become distant memories. They must always remain a vivid reminder of the terrible price that was paid for September 10th thinking. The threat that was so fully and terribly revealed on September 11, 2001, is not a matter

of divergent perceptions. It is a persistent and evolving reality that we must continue to confront.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins, for that statement.

We will now go to the witnesses. Generally speaking, gentlemen, as you know, we asked you to speak to us this morning about your evaluation of the current threat environment and your own self-evaluation of the status of reform at the agencies that you lead. Obviously, we would welcome anything else you want to say this morning.

We will begin with Secretary Chertoff.

TESTIMONY OF HON. MICHAEL CHERTOFF,¹ SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary CHERTOFF. Well, thank you, Mr. Chairman, and thank you, Senator Collins, and Members of the Committee. It is a pleasure to appear before you again today as we approach the sixth anniversary of that terrible day. And it is also an appropriate time to recommit ourselves and reaffirm our determination to continue to build on the progress that this Committee made possible through its earlier rounds of legislation and that all of us have been working very hard over the past 6 years to address.

I would like to recognize, first of all, my colleagues at the table: Director McConnell, Director Mueller, and Admiral Redd. All of us meet together frequently. We confer frequently, and we all share with others—and, of course, ultimately the President—the responsibility to protect the American people and, in the words the President has used, “not to let this happen again.” All of us recognize that this is a daunting challenge and one that requires a partnership with State and local officials, with the private sector, and with our international partners.

I would also like to take this moment to thank this Committee which has really led the charge to build the institutions that can adapt to 21st Century challenges such as those posed by this war currently being waged by Islamist extremists. And once again, as bin Laden’s tape disclosed over the weekend indicates, for our enemies this war is very much a current concern and very much in the forefront of their minds. It must remain in the forefront of our mind.

Finally, of course, I have to express my gratitude not only to the 208,000 men and women who work with me at the Department of Homeland Security protecting our borders, our sea lanes, our infrastructure, and our airways, but also my colleagues all across the government in all of the agencies represented here and others who work very hard 24/7 to protect the American people.

Over the last 6 years, we have made some tremendous strides in making this country safer, and in answer to the question I often get asked, it is clear to me that we are much safer than we were prior to September 11, 2001. It is also clear to me that we have more work to be done because, as you said, Mr. Chairman, the enemy is not standing still. They are constantly revising their tac-

¹The prepared statement of Secretary Chertoff appears in the Appendix on page 59.

tics and adapting their strategy and their capabilities. And if we stand still or, worse yet, if we retreat, we are going to be handing them an advantage that we dare not see them hold.

The fact that we have not suffered another terrorist attack on our soil in the last 6 years does say something about the success of our efforts so far. Now, some people do say it is just because we are plain lucky. I do not believe "luck" is an adequate explanation for this. Others may contend that the terrorist threat has subsided or that the United States is no longer in danger, or maybe that the terrorists have lost interest. But, again, I would just commend the videotape we saw over the weekend as a refutation of that. I commend to you the arrests that we saw in Germany and Denmark. The enemy is very focused on continuing to wage this war. They have not lost interest, and if we allow ourselves to become complacent and to think that the threat has diminished, we are going to be crippling ourselves in our ability to prevent future attacks.

It is not the case that the enemy has not tried to attack us over the past several years. In December 2001, the Shoe Bomber tried to blow up an airliner coming to the United States. Last summer the British, with our help, disrupted a plot that, had it been carried out, would have resulted in multiple explosions on airliners flying from the United Kingdom to the United States. So it is not for want of trying that we have not suffered a successful attack.

Even in recent months, we have disrupted terrorist plots in our country: The plot against Fort Dix and the plot against JFK Airport. Last week German authorities thwarted a serious plot, as they themselves have acknowledged, directed in part against Americans in Europe. And Danish police also arrested terrorist suspects in their country.

These events underscore what the National Intelligence Estimates (NIEs) made clear, which is the enemy's effort to continue to focus on the West and to recruit operatives who can move in the West. And that is one of the reasons that I want to thank the Committee for the 9/11 legislation, which has now given us some additional capabilities in plugging the vulnerability through the Visa Waiver Program. Every day at our own borders we turn away dangerous people, including individuals with known ties to terrorism, as well as criminals, drug dealers, and human traffickers.

So I sum up by saying that I believe the reason that there have not been successful attacks on American soil is not because the threat is diminished; it is because we have raised our level of protection and our level of disruption, both by undertaking action overseas and undertaking action within our own borders. It is a testament to the partnership reflected in part by those at this table, the hard work of the dedicated men and women who work for the agencies of the Federal Government as well as State and local officials, and our partnerships overseas, which I think become stronger every single day.

Now, that is not to say that our efforts have been flawless or that our work is over with. On the contrary, the biggest challenge to us is not to lose the sense of urgency which animated all of us in the weeks and months after September 11, 2001. If we continue to adapt ourselves and continue to feel the need to move quickly and substantially to meet this threat, we are maximizing our ability to

protect ourselves. But if we do otherwise, we are turning around and moving in the wrong direction.

Now, I have provided the Committee with a fairly lengthy assessment of where I think we are in a number of areas.

I thought what I might take in the next couple of minutes is the opportunity to look at a few areas where I think we are now addressing gaps that have not yet been filled. Part of what we have to do, of course, is not merely plug those vulnerabilities that have been identified looking backwards, but we need to look forward. In fact, we need to look around the corners at some vulnerabilities that have not been spoken about. And we need to make sure that we are working to address those as well. So let me talk about a number of those.

The first is general aviation. As this Committee knows, we have spent a lot of time focused on the question of people smuggling in weapons of mass destruction through maritime containers or putting them on commercial aircraft, but we have not looked at the question of general aviation coming from overseas as a potential vector through which weapons of mass destruction or people who are dangerous might be smuggled into the country. We are now working to plug that threat.

Later today we will be unveiling a plan to begin the process of increasing our security for overseas general aviation coming into this country substantially. The first step of this is to move forward with earlier screening of people who are on crews and who are passengers in general aviation planes crossing the Atlantic and Pacific Oceans. We are going to use our authorities to align early reporting of crew members and passengers before take-off in the same way we now require for commercial airliners so that we can prevent people from getting on airplanes and taking off to the United States, and, as important, or more important, prevent weapons of mass destruction from getting on airplanes and coming to the United States on private aircraft. The vision of where we want to go with this moves beyond simply screening people, but ultimately looks to a process of physical screening of private aircraft overseas before they come into the United States.

We also remain mindful of the threat to our ports not only from containers in commercial cargo vessels but from small boats and privately owned oceangoing vessels which could seek to duplicate a *USS Cole*-style attack on our ports or again to smuggle dangerous weapons, materials, or people into the country. We have been working with small-vessel owners, principally through the Coast Guard and Customs and Border Protection, to assess what those risks are and to come up with a strategy that will help us efficiently but also protectively to address the risk presented by smaller boats and privately owned oceangoing vessels to our country.

We have, for example, in the last week launched a program in Seattle to work with local authorities to conduct vulnerability and risk assessments with respect to the smuggling of nuclear materials into the port of Seattle through private vessels. Part of this involves the deployment of radiation detection technology and equipment to key maritime pathways and choke points so that we can begin the process of radiological scanning of small vessels that

might bring nuclear materials into the port of Seattle. As we evaluate how this works in an operational environment, we look to expand this capability from Seattle to places like the port of San Diego and also New York City as well.

I am also committed, as are my colleagues at the table, to particularly focus on those kinds of challenges and weapons which could have a truly catastrophic effect on the United States, and that means, of course, nuclear or dirty bomb-type attacks.

We recognize that our first and most urgent priority is to prevent nuclear weapons from coming into this country and preventing dirty bombs from being constructed and detonated. And that is, of course, where we put most of our attention. But we do have to recognize that, should our actions fail, nuclear forensic and attribution capabilities would be critical in protecting against a follow-on attack, and also in making sure that we responded to anybody who launched nuclear bombs against us using terrorists as the delivery vehicle.

Therefore, even before an attack occurs, our ability to demonstrate that we have real and robust forensic and attribution capability will give us a significant measure of deterrence value, particularly against any state actor that had it in mind to use terrorists as a disguised method of delivering a nuclear bomb against the United States. That is why we have created the National Technical Nuclear Forensics Center, which is an interagency center focused on forensics and attribution, and it is housed within our Domestic Nuclear Detection Office. I had an opportunity last week to meet with the Interagency Leadership Executive Committee of that center. It is dedicated to continuing to develop and improve and to sustain a rapid and credible capability to support attribution, conclusions, and potential responses to a nuclear attack or a dirty bomb in this country. I think that is a critical element of our protection and response to a catastrophic attack.

The Nuclear Forensics Center involves partnerships all across the Federal Government, including very deep partnerships with my colleagues at the table here today—DNI, FBI, and the NCTC.

Of course, our improvements to screening, critical infrastructure protection, and intelligence fusion and sharing have to continue. We have to continue sharing intelligence horizontally and vertically. Again, I want to commend the Chairman and the Ranking Member for their leadership on information sharing in past sessions of Congress, and we are dedicated to being a full partner in the Information Sharing Environment about which more will be heard later this morning.

Finally, I would like to observe that, again, one of the cutting-edge elements of this information sharing has to do with biological threats. Providing early warning biosurveillance on human and animal health, protection, and vulnerabilities of the food and water supply, and the environment in general as it relates to biological conditions is a critical element in getting early warning and rapid response to a biological threat, whether that be a natural threat or a manmade threat.

We have recently established the National Biosurveillance Integration Center which will fuse clinical data, intelligence information, and what we get from our Biowatch sensors into a comprehen-

sive analysis of biological threats and events. While considerable work needs to be done to get this center fully deployed and fully operational, we have made some considerable progress, particularly in the last year. And, again, this is a classic example of an inter-agency effort, including not only those at this table, but the Departments of Defense, State, Interior, Agriculture, Health and Human Services, and Transportation.

Let me conclude by saying that as we honor the victims of September 11, 2001, tomorrow, I hope that the anniversary of that day is not merely an opportunity to commemorate the loss of life or to celebrate heroism, but also an opportunity to rededicate ourselves to the struggle and to recognize the most important lesson is “Never again,” at least to the limit of our human abilities.

I would like to thank the Committee for your ongoing support and for the opportunity to testify at the hearing. I look forward to continuing our important work in protecting the American people.

Chairman LIEBERMAN. Thank you very much, Secretary Chertoff, for an excellent statement. I particularly want to thank you for those announcements toward the end of your statement about what you are doing to try to raise the security with regard to private aviation and boats coming into the country, as well as the development of a center to make sure that we have the forensic capability to consider rapidly the aftereffects of a nuclear attack. This is a gruesome business, but as Senator Collins said and the 9/11 Commission said, it was a failure of imagination, which is to say a failure to imagine that anyone could possibly do what the terrorists did on September 11, 2001, that created part of the vulnerability we had on that day. And I think you are imagining now what our enemies might do to attack us, and you are attempting to close those vulnerabilities. So I appreciate it very much.

The Department of Homeland Security, as we know, was created out of Congress. The next two agencies we are going to hear from are the Office of the Director of National Intelligence (ODNI) and the National Counterterrorism Center (NCTC), who were the two leading recommendations of the 9/11 Commission, the so-called Kean-Hamilton Commission. It strikes me that since they are both headed now by retired admirals, we may have to revise MacArthur’s old statement and say that “Old sailors not only do not die; they do not even fade away.”

[Laughter.]

They come back and serve their country, and for that we are extremely grateful.

Admiral McConnell, the Director of National Intelligence——

Senator WARNER. Add me to the list.

Chairman LIEBERMAN. Senator Warner is added to the list as well. You are not calling yourself an “old sailor” are you?

Senator WARNER. You better believe it. I am older than these guys.

[Laughter.]

Chairman LIEBERMAN. Admiral McConnell, go ahead.

TESTIMONY OF HON. J. MICHAEL MCCONNELL,¹ VICE ADMIRAL, U.S. NAVY (RET.), DIRECTOR OF NATIONAL INTELLIGENCE

Admiral MCCONNELL. Sir, Senator Warner was the Secretary of the Navy when I was briefing him as a young lieutenant, so thank you, sir.

Mr. Chairman, Senator Collins, and Members of the Committee, thank you very much for the opportunity to appear before the Committee to provide a status of our efforts to confront terrorist threats to the Nation. I also appreciate the opportunity to describe the implementation of the reforms mandated by the Congress and the President since September 11, 2001, and, as has been mentioned, 6 years ago tomorrow.

My biggest concern, as mentioned by Senator Collins, is going back to September 10th thinking by many in our country. As stated in our July National Intelligence Estimate, the level of focus and commitment may wane in time. The threat is real, and we must remain vigilant.

As noted, in July my office released the National Intelligence Estimate, the intelligence community's most authoritative judgment on a particular subject, and this was on the terrorist threat to the U.S. homeland. In our key judgments, an unclassified version of which has been mentioned here and is posted on our website, for the 3-year period of the estimate, we assess that our Nation faces and will continue to face a persistent and evolving threat, mainly from Islamic terrorist groups and cells, and most especially al-Qaeda.

The terrorist threat without question is real. I will share with you today how we in the intelligence community are working to counter these threats. I also have submitted a more comprehensive overview in my statement for the record, and I ask that it be submitted to the record.

Chairman LIEBERMAN. Without objection.

Admiral MCCONNELL. To confront today's threats, we have made many changes in the way we conduct intelligence, law enforcement, homeland security, and diplomatic and defense activities. Our greatest progress can be concentrated, I believe, in four areas: First, by improving our organizational structures to meet the new threats of this century; next, by fostering greater information sharing to provide the right information to the right people at the right time, largely driven by this Committee; third, strengthening our intelligence analysis; and, fourth, implementing the necessary reforms that allow us to build a dynamic intelligence enterprise that promotes diversity to gain insight and to sustain a competitive advantage against our adversaries.

First let me touch on the structural improvements in the intelligence community. One of our challenges was integrating foreign and domestic intelligence, that is, foreign intelligence collected inside the United States. We are ensuring that we collect the right information to most accurately and objectively reflect the threats inside the United States. We are better able to do this with the establishment of the FBI's National Security Branch (NSB). The NSB

¹The prepared statement of Admiral McConnell appears in the Appendix on page 73.

integrates the FBI's counterterrorism, counterintelligence, weapons of mass destruction, and intelligence programs, allowing for a coordinated focus on collecting foreign intelligence within the United States. And, of course, as mentioned, the National Counterterrorism Center (NCTC) uses all that information with foreign collected information to provide a more comprehensive picture.

Second, with regard to our structure, creation of the National Clandestine Service at CIA to guide all clandestine human operations across the community with the most effective leadership allows for better oversight and coordination we did not have before.

Third, we are working to dismantle stovepipes, the stovepipe mentality inside the intelligence community. This mind-set is where an agency can produce, and limit within its walls, vital national intelligence. One way we promote greater collaboration is by using cross-community mission managers to identify intelligence priorities, gaps, and requirements. Mission managers engage in strategic planning and collection management against our hardest targets. Today we have mission managers for North Korea, Iran, Cuba, and Venezuela, counterterrorism, counterproliferation, and counterintelligence.

Finally, with the support of this Committee, we have established a Program Manager for the Information Sharing Environment to enhance our sharing of terrorism information not only among Federal but also among State, local, tribal governments, as well as the private sector.

Let me turn now more specifically to information sharing. Our efforts to improve information sharing mechanisms are of special significance, given that the failure to do so contributed to our inability or our failure to prevent the September 11, 2001 attacks. In our July National Intelligence Estimate, we assess that al-Qaeda is planning to attack the homeland, is likely to continue to focus on prominent political, economic, and infrastructure targets, with a goal of producing mass casualties, visually dramatic destruction, and significant economic shocks. And, of course, as mentioned by the Chairman, the intent is to create fear among our population.

To counter this, we must depend not only on the 16 agencies of the intelligence community, but also on the eyes and ears of our State and local partners across the country. And more than depending on them, we must be willing to share threat information and work with them to protect our Nation. We believe that State and local partners can no longer be treated only as first responders, but also as the first lines of prevention. In the past 6 years, the Program Manager for the Information Sharing Environment has led the charge to transform our policies, processes, procedures, and, most important, workforce or workplace cultures to reinforce sharing terrorist threat information as the rule, not the exception. I have also made improved information sharing a centerpiece of the DNI's strategic planning going forward.

Although the effort to implement the Information Sharing Environment is well underway, it is essential that the implementation activities take place within a broader strategic context of enhancing our Nation's ability to combat terrorism. The ultimate goal is not simply information sharing for the sake of sharing. The objective

is to improve our national capacity to protect our Nation from future attack. We are working very hard to do just that.

Let me now turn to analysis. We are in the process to fundamentally reform our analytical process. In addition to focusing on improved formal training and analytical rigor, we are moving the intelligence community toward implementing a community-wide information technology architecture that allows, among other things, analysts to better share and to collaborate. This means community-wide computer connectivity and standardized information-sharing policies. So whether you are an analyst in Hoboken or Honolulu, a special agent in the FBI, or a soldier on the front lines, we will be able to contribute to and benefit from accurate and timely intelligence. This is balanced, of course, so that we do not compromise operational security, consistent with our responsibilities to protect sources and methods.

The Office of the Director of National Intelligence is also developing virtual communities for analysts who can securely exchange ideas and expertise across organizational boundaries, to find, access, and share information to make their analytical judgments. We are better engaging with outside professionals who can challenge our analytical assumptions, provide deep knowledge, insights, and new ways of thinking. We conduct red-teaming and alternative analysis to ensure we have examined all possibilities in our analytical process.

We also have taken steps to ensure the impartiality of our analysis and our analytical products. As mandated by the Intelligence Reform Act, we established an Assistant Deputy Director for Analytical Integrity and Standards. This person serves as a focal point for analysts who wish to raise concerns regarding politicization, bias, lack of objectivity, appropriate alternative analysis, or dissenting views.

We also have made qualitative improvements to our analysis, specifically our National Intelligence Estimates. Key judgments are written to explore more thoroughly the implications of our critical underlying conclusions. Appendices and annexes now provide full transparency in our analytical judgments by describing the analytical train of reasoning we used to arrive at our conclusions. And the main text now highlights the full range of analytical judgments and their implications, bringing dissenting opinions to the fore so policymakers, such as Members of this Committee, can have the benefit of the full analytic picture.

Let me move now to implementing necessary changes in our policy and our practices. I will turn to the policies we have enacted across the intelligence community as well as policies we are currently pursuing through our recently completed 100-day plan and the upcoming 500-day plan. These reforms will allow us to better confront threats to the Nation as we go forward.

In June, I signed a directive mandating civilian joint duty for intelligence officers across the intelligence community. This initiative was started by Ambassador Negroponte as far back as 2005. It was difficult to get agreement, but it is now passed. Now it is up and running. If an up-and-coming officer aspires to be serving at the senior reaches of the community, he or she will have to serve a tour of duty at a different agency outside their parent agency dur-

ing their career. The experience provides the officer with broader perspective and brings the community towards a higher level of collaborative behavior. Our approach was patterned after the successful Goldwater-Nichols bill of 1986 that moved DOD to military jointness.

We also have been working to recruit intelligence officers with the needed background and skills that will strengthen our abilities. We are developing programs to recruit young people from all walks of life, including first-generation and second-generation Americans and members of traditionally underrepresented groups with language skills and cultural understanding that we need for the insights and for our analysis. Recruiting new and talented employees means little, however, if we are unable to get them through our security process. Therefore, we have a pilot project with the Department of Defense to see if we can go much faster using an automated process, commercial best practices, and then a new approach for life-cycle monitoring once you are on the inside.

We have accomplished a great deal, but we still have a lot more to go. To better integrate the intelligence community, we initiated a deliberate planning process based on the principles of transparency, accountability, deadlines, and deliverables. The first phase of these efforts was spelled out in our 100-day plan. They were designed to jump-start the necessary reforms in the community to build momentum. The next phase, our 500-day plan, started in August. It is intended to sustain and accelerate the momentum with an expanded set of initiatives and greater level of participation. Our plan was developed through a community-wide effort through the use of working groups, blogs, and wikis to solicit inputs from the community.

I am happy to report that enthusiastic participation by the community allowed us to put together what we think is a comprehensive plan. This plan will be executed through cross-organizational and community-wide engagement. Our primary emphasis is improved collaboration across the community. Working groups from each of the areas will focus on the key issues and engage the key stakeholders. Our intent is to integrate the intelligence community and enable cross-organizational collaboration across critical mission areas to serve our customers better but, more importantly, to better protect the Nation. We must continue to accelerate our efforts.

In closing, we have come a long way over the past 6 years developing a more integrated, more collaborative community. I believe the result is a stronger community better able to protect the Nation. I think the Nation is better protected today than it was 6 years ago, but we must remain vigilant, and we must remain engaged.

Mr. Chairman, that concludes my prepared remarks. I look forward to your questions.

Chairman LIEBERMAN. Thanks very much, Admiral McConnell. I have a few questions that I hope we can build on during the Q&A period. Particularly, I appreciate your last thoughts there, which is that you are moving toward an integrated, collaborative intelligence community, which is part of what we did not have on September 11, 2001.

Admiral Redd, thanks for being here. Thanks for your service. I will just say in introducing you that more than a year ago, Senator Collins and I went out and spent a good part of a day at the National Counterterrorism Center, and it was one of those occasions when you have the satisfaction of actually seeing something that was called for in legislation, enacted and carried out. And I remember we said to each other—I went home that night and said to my family, “I was at the NCTC today, and you all have reason to feel more secure tonight as a result of what is happening out there.” So I thank you for that, and we welcome your testimony now.

TESTIMONY OF HON. JOHN SCOTT REDD,¹ VICE ADMIRAL, U.S. NAVY (RET.), DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Admiral REDD. Thank you, Mr. Chairman, and that is a very good point, that words do eventually mean something, and they do translate into tangible things, and NCTC is a very tangible example of that.

Chairman Lieberman, Senator Collins, distinguished Members of the Committee, thank you for the opportunity to testify before you today on our Nation’s efforts to confront the terrorist threat to the homeland since September 11, 2001. I also have a short oral statement and would ask that my longer written statement be submitted for the record.

Chairman LIEBERMAN. Without objection.

Admiral REDD. And before we leave the old sailors analogy, I would note that Director Mueller, as a former Marine, is a member of the Department of the Navy, which is probably about as far as we can take that discussion without getting into trouble here.

[Laughter.]

Chairman LIEBERMAN. Remember, we are looking for collaboration.

Admiral REDD. Yes, sir.

Mr. MUELLER. Our liaison just broke down.

Admiral REDD. In the 6 years since September 11, 2001, the U.S. Government has taken significant steps to improve our understanding of the terrorist threat and our ability to combat it, and many of those steps are indeed the result of the Intelligence Reform and Terrorism Prevention Act, which was championed by this Committee. And for that, sir and madam, we are in your debt.

While I am going to focus today on the progress we have made, I would just start with a comment that none of what I say should obscure the real and significant challenges that we continue to face. We are in a long war, and our enemy is determined and dangerous. Our counterterrorism efforts have disrupted many of the enemy’s plans and diminished certain capabilities. But the events of the last days and the last weeks clearly demonstrate the clear and present danger which continues to exist.

With that in mind, let me turn briefly to the role the National Counterterrorism Center (NCTC) plays and continues to play in the war on terror. Today, as directed by the legislation, NCTC has

¹The prepared statement of Admiral Redd appears in the Appendix on page 93.

two roles, two fundamental roles. In military terms, I wear two hats. The first is a very familiar one to everyone, and that is intelligence, and in that hat I report to Admiral McConnell, the Director of National Intelligence. The second hat is to do with a thing called "strategic operational planning," which is a new and I believe revolutionary capability in our government. And in that hat, I report to the President.

Let me first turn to NCTC's role in counterterrorism intelligence. As envisioned in the legislation, analysis is the heart and soul of NCTC's intelligence mission. More than half of our government workforce, which is about 400 people, is devoted to this effort. I would submit that today NCTC provides the best example of all-source, integrated analysis in the intelligence community. There are two primary reasons for that, some of which have been alluded to here.

First, NCTC is the only place in the U.S. Government where all intelligence, both foreign and domestic, comes together.

Second, we are, as indicated and directed in legislation, a truly joint organization. Virtually all of our analysts come from other Federal agencies, and this allows them to leverage the diverse skills and backgrounds of their co-workers in reaching their analytic conclusions.

In addition to producing analysis, NCTC also has a mandate to integrate analysis across the intelligence community. The net result of this effort is a full spectrum of intelligence product for policymakers and operators. These range from raw intelligence products, such as our threat matrix, which is designed to provide immediate situational awareness of an impending threat, to more in-depth types of analytic products, which, for example, the President's Daily Brief (PDB).

Significantly, virtually all of the reports for senior policymakers are coordinated through NCTC as the DNI's mission manager. The purpose of that is to ensure that differing views are not only represented but that they are also put in context.

So how was all this played out in the real world? Perhaps one of the best examples occurred a year ago during the U.K. aviation threat. In this, the most significant threat to the homeland since September 11, 2001, NCTC worked hand in glove with DHS, FBI, CIA, NSA, and others to share intelligence and provide integrated analysis in a very dynamic environment. When the President and the National Security Council met, NCTC gave the intelligence briefing, combining both foreign and domestic information. In my view, and in the view of others, that is exactly what the legislation had in mind when you established NCTC.

Another key function of NCTC is information sharing. Let me give you three examples now of how we have improved information sharing, I believe dramatically so, since September 11, 2001.

The first is NCTC Online. Simply put, this is the Nation's premier classified website for counterterrorism intelligence. Maintained by NCTC, this highly classified electronic library contains over 7 million counterterrorism documents—or terrorism documents. These reports come into NCTC on over 30 networks from over 60 organizations, and it is instantly available to around 8,000 analysts around the world.

The second example of information sharing is what we call the Terrorist Identities Datamart Environment. You have to have a good acronym, so it is TIDE. Today, the U.S. Government has one central knowledge base of all known and suspected terrorists. It is maintained by NCTC and is based on all-source classified information. Every day we distribute a sensitive but unclassified extract, which is the basis of various screening activities. We send that to Bob Mueller's folks at the Terrorist Screening Center, and that becomes the information which provides for entry checks at borders, Secretary Chertoff's business, consular checks for visa applications in the State Department, and TSA's no-fly list.

The third example of information sharing deals with situational awareness. Every day NCTC chairs three secure video teleconferences—8 o'clock in the morning, 3 o'clock in the afternoon, and 1 o'clock in the morning. There are participants from across the community to make sure everybody is on the same page. Our Watch Center is open 24/7, passing information as events occur, again, around the intelligence community. Also, significantly, we are physically collocated with the FBI and CIA's Watch Centers for Counterterrorism. And of great significance to those who have been in the intelligence business, there are no doors between those Watch Centers.

Let me now turn briefly to NCTC's second role in the war on terror: Strategic operational planning. In this role, we lead an inter-agency planning effort that brings all elements of national power to bear in the war on terror. This effort also involves a spectrum of activities from deliberate, long-range strategic planning to more dynamic, short-range operational planning efforts. An example of the former is the National Implementation Plan (NIP), which was approved by the President last year. NIP serves as the Nation's strategic blueprint for the war on terror and it integrates the full weight of our diplomatic, homeland security, law enforcement, financial, and military activities, as well as intelligence. At the other end of the planning spectrum are more operational planning efforts, including those established to address specific threats. The interagency task force, which deals with the current heightened threat environment, is an ongoing example.

So where does all this leave us? Despite continuing and significant challenges, I believe that today, 6 years after September 11, 2001, the United States is better prepared to fight the war on terror than at any time in our history. Let me give you seven reasons why I say that.

First, our intelligence is better. Terrorists are a tough target, but our collection, our analysis, and our production are significantly improved.

Second, we have made major strides in information sharing and getting intelligence to the people who need it to take action.

Third, we are taking the fight to the enemy and have achieved significant successes in the field. Thousands of terrorists have been taken off the field of battle, and dozens of plots have been disrupted.

Fourth, we are attacking every element of the terrorist's life cycle, including terrorist travel and terrorist finance.

Fifth, and very importantly, this is not only an American effort. We are working more closely and more effectively with a greater number of allies around the world to defeat the terrorists.

Sixth, and of special interest to this Committee, we have taken significant steps to make the homeland a hostile place for terrorists to enter and operate.

Finally, through a new strategic planning effort, we are laying the groundwork to take the efforts already underway to a new level of integration and effectiveness.

All of this means to me that we are safer today than we were on September 11, 2001. But we are not safe, and nor are we likely to be for a generation or more. We are in a long war. We face an enemy that is adaptable, dangerous, and persistent, and who always has a vote. While we have won many battles since September 11, 2001, there are many battles yet to be fought, and we must anticipate that there will be setbacks along the way. Thank you, sir.

Chairman LIEBERMAN. Thank you, Admiral Redd, for that excellent testimony.

Director Mueller, obviously the FBI is the senior institution at the table, pre-existing September 11, 2001, but under your leadership it has gone through quite a significant internal transformation to meet this new threat to our homeland. So I thank you for being here, thank you for what you have done, and look forward to your testimony now.

**TESTIMONY OF HON. ROBERT S. MUELLER III,¹ DIRECTOR,
FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT
OF JUSTICE**

Mr. MUELLER. Thank you, Mr. Chairman, and good morning, Senator Collins and Members of the Committee. I also appreciate the opportunity to be here today to discuss the terrorist threats facing our Nation, as well as those steps, measures the FBI has taken to confront those threats.

After September 11, 2001, the FBI's priorities shifted dramatically. The FBI's top priority is and will continue to be the prevention of another terrorist attack. By joining our traditional collection expertise with our expanding intelligence capabilities, we have had a number of successes in the war against terror. Several have been mentioned here today, from Portland, Oregon; Torrance, California; to Chicago; to the recent Fort Dix and JFK plots. Indeed, the development of a mature intelligence and national security infrastructure is and will continue to be a key to our success.

We have established the National Security Branch, and the Directorate of Intelligence has dedicated and integrated intelligence services within the Bureau. And beginning immediately after September 11, 2001, we have made significant strides in reshaping the way we meet our mission. We have doubled the number of intelligence analysts on board, tripled the number of linguists, set up field intelligence groups comprised of FBI, Federal, State, and local partners in each of our 56 field offices. And today intelligence is woven throughout every FBI program and every operation.

¹The prepared statement of Mr. Mueller appears in the Appendix on page 106.

While much of the U.S. Government's attention is focused on—and rightfully so—al-Qaeda's reach from abroad into the United States, homegrown radicalization also exists. The role of our law enforcement partners is absolutely critical to identifying individuals and groups presenting this threat, especially through the FBI's Joint Terrorism Task Forces, of which there are over 100 today. And, moreover, outreach to Muslim and South Asian communities plays an essential role in helping the FBI to identify violent extremists within those communities. To that end, I periodically meet with members of major Muslim and Arab community-based organizations, civil rights groups, as do senior executives at FBI headquarters.

Special agents in charge of all of our 56 field offices conduct town meetings with members of Arab and Muslim communities, and members of the Arab American community attend the FBI's Citizens' Academy, an 8-week program designed to give community leaders an overview of the FBI and the Department of Justice procedures and operations.

And while the FBI and other members of the intelligence community, several sitting here today, and State and local law enforcement partners have been successful to date in preventing another major terrorist event within the homeland, we cannot rest easy. al-Qaeda and other extremist groups continue to have the will and the ability to attack us, and we must all continue our vigilance, commitment, and efforts to keep America safe.

The FBI was created nearly 100 years ago to address crime crossing State boundaries. The threats we now face are global, and technology is moving more quickly than we could have foreseen just 10 years ago. And we together, those of us at the table and in the FBI, must continue to protect the security of our Nation while upholding the civil rights guaranteed by the Constitution.

Mr. Chairman, Senator Collins, Members of the Committee, I appreciate the opportunity to testify this morning, and I look forward to answering your questions.

Chairman LIEBERMAN. Thanks very much, Director Mueller.

Gentlemen, I would say that my impression, as I listened to the four of you—and I hope that others across the country will be able to do so—is the picture of a great Nation that was attacked on September 11, 2001 in a way that we simply did not anticipate, now marshaling our enormous resources and patriotism to defend against another such attack. So, again, no one at the table, no one up here is feeling comfortable because the enemy is out there. But I think the composite picture is of enormous progress that has been made to close the vulnerabilities that existed on September 11, 2001, and again for that I thank you.

We are going to have a 6-minute round here at the beginning. Votes will go off at 11 o'clock, but I am going to keep the hearing going and just ask us to take turns going over to vote and coming back.

I want to talk in specifics about the collaboration. The 9/11 Commission and others, in looking back at September 11, 2001, pointed to the gaps particularly between the CIA and the FBI in sharing information, some of which came from a historic pre-September 11, 2001 mind-set about where the responsibility of each was and how

you could not have anybody involved in foreign intelligence work with domestic law enforcement.

Obviously, we are in a different kind of war now where the lines between foreign and domestic are effectively blurred, if not eliminated, and I wanted to ask both Director Mueller and Director McConnell if you would just address briefly whether you think that the gaps that existed between the two communities have been effectively closed since September 11, 2001. Admiral Redd, sometimes a picture is worth a thousand words. When we were out at the NCTC, we noted that there was no door between the CIA desk and the FBI desk. But beyond that, are you sharing information, Admiral McConnell?

Admiral MCCONNELL. Sir, I think the gap is significantly less than it was. I think we are still closing it. It is the process of transforming cultural—or human behavior. As you mentioned, the wall between us that was generated in a period of the 1970s, 1980s, the difference between foreign intelligence and domestic activity, was significant. In my view, that was one of the things that contributed to our failings at September 11, 2001. So while legislation has changed so we can now talk to each other, as opposed to going one way, it can go back and forth. We have created the National Security Branch in the FBI to actually have an intelligence mission more focused on this sort of thing.

So I think we are significantly better, but I would not want you to take away from this that we have done everything that we need to do. It is truly cultural transformation. This means human behavior. That is one of the reasons we pushed the joint duty approach to get people to serve in the other person's organization.

Chairman LIEBERMAN. Fair enough. Director Mueller.

Mr. MUELLER. I would support what the Admiral said. I had mentioned three things. The impediments to sharing that there were before September 11, 2001, have been removed. The PATRIOT Act is in some large part attributable or responsible for breaking down those walls. Second, the NCTC as a mechanism for sharing has worked exceptionally well. There are no doors, there are no walls in terms of the exchange of information, the quality and caliber of the analysis that is done there. And, third, the exchange of personnel. Now that the wall has been broken down, the ability to trade personnel and information, we have established the National Security Branch, the No. 2 person in the National Security Branch, Phil Mudd, is from the CIA, as an example of the exchange of personnel and the importance we all recognize of sharing information, exchanging information, integrating information, whether it be collected overseas or collected domestically.

And, finally, I would say that I would agree that we have made substantial strides, but we have a ways to go.

Chairman LIEBERMAN. Thanks. The other respect is that intelligence gathered overseas may directly relate to intelligence that we need here at home to protect against an attack on our homeland. We are, as we have all said, at war, and in this war, even more than in traditional wars, intelligence is critically important to prevent enemy attacks. Part of what we are trying to do is adjust our intelligence-gathering system and our technologies to that new reality.

Admiral, before we broke for the August recess, we had quite a go-round about FISA, and we adopted legislation. I wanted to ask you to speak for a moment about that, and if you can in this open setting—there have been some press suggestions, media suggestions that the United States through your office, was able to assist the German Government in the apprehension of those plotting terrorist attacks against American targets in Germany. Could you comment on that specifically and more generally on how the system we adopted in July, early August, is going?

Admiral MCCONNELL. Yes, thank you, Senator. With the Foreign Intelligence Surveillance Act under consideration for updating, we found ourselves in a position of actually going backwards, losing capability because of the interpretations of the law.

Chairman LIEBERMAN. By courts.

Admiral MCCONNELL. Yes, sir, by the FISA Court. Looking at the requests, it was actually taking us too much time, and because of the interpretations we were losing ground. So the approach we took was to ask for basically three things: First of all, do not require the intelligence community to obtain a warrant when we are targeting a foreigner, a terrorist, in a foreign country. We had found ourselves in the position where, based on the interpretation of the law, we were being asked to get warrants against terrorists operating in a foreign country. So we asked for relief for that.

The second thing, for those private entities that assisted us, we needed to have some protection for them with regard to liability.

And the third thing, quite frankly, was in the interest of protecting civil liberties and the privacy of Americans, we felt it was appropriate to be required, as we were in the old FISA legislation, to have a warrant anytime we targeted a U.S. person. That would include even a foreigner in this country suspected of being a terrorist. So we thought it had the right balance.

It was passed, as you well know, and we are very pleased with that, and we are better prepared now to continue our mission—specifically Germany, it made significant contributions. It allowed us to see and understand all the connections with regard—

Chairman LIEBERMAN. The newly adopted law facilitated that during August?

Admiral MCCONNELL. Yes, sir, it did. The connections to al-Qaeda, the connections specifically to what is referred to as the Islamic Jihad Union (IJU), an affiliate of al-Qaeda. Because we could understand it, we could help our partners, and through a long process of monitoring and observation, realizing that the perpetrators had actually obtained explosive liquids, hydrogen peroxide which they would condense or try to condense to an explosive. And so at the right time when Americans and German facilities were being targeted, the German authorities decided to move.

[Information provided for the Record from Admiral McConnell follows:]

INFORMATION SUBMITTED FOR THE RECORD

During the Senate Committee on Homeland Security and Governmental Affairs hearing on September 10, 2007, I discussed the critical importance to our national security of the Foreign Intelligence Surveillance Act (FISA), and the recent amendments to FISA made by the Protect America Act. The Protect America Act was urgently needed by our intelligence professionals to close critical gaps in our capabili-

ties and permit them to more readily follow terrorist threats, such as the plot uncovered in Germany. However, information contributing to the recent arrests was not collected under authorities provided by the Protect America Act.

Chairman LIEBERMAN. Thank you. Senator Collins.

Senator COLLINS. Admiral Redd, you recently said in an interview with *Newsweek*, "We are going to get hit again." Secretary Chertoff talked today about some of the possible lines of attack that he is working on, for example, general aviation, small boats.

When you look at the intelligence, what kind of attack do you believe we should be preparing for?

Admiral REDD. Thank you, Senator. First of all, there were two parts of that interview, which, as you know, sometimes get conflated. One is the heightened awareness or the heightened threat environment in which we are right now. And the second is the statement, which I also made in my oral statement, that over time, over a 40-year generational period, just statistically batting a thousand would be very difficult, and that is why I said we may get hit again.

The short answer is you cannot focus on any one of those. We watch very carefully what al-Qaeda is saying. We watch their planning. There is a certain sense at which they tend to come back and be persistent and try the same things again. As was indicated in the NIE, they are focused on large elements or large reaction to things like our transportation system, particularly aviation. But we cannot just look at one of those. We have to look across the board.

Senator COLLINS. Secretary Chertoff, if you look at the recent plots that were thwarted in this country, if you look at Germany just last week, at Scotland, London, the JFK plot, it appears that terrorists still are looking at bombs and that they are looking at IEDs as the weapon of choice.

What is DHS doing in the area of IEDs?

Secretary CHERTOFF. Well, Senator, I think you are correct that the attack weapon of choice still is the IED, and we are doing a number of different things, all of which I think will soon be captured in a strategic document directed both by Congress and the President. But let me go through some of the major elements of what we are doing.

Of course, we begin with detection. We want to detect and prevent something from going off. One element of that, of course, is technology. Through our Science and Technology Directorate, we are doing research in such things as technology that will enable us to detect liquid explosives even when they are in a container, and to detect those liquid explosives rapidly and accurately in an operational environment.

With respect to other kinds of technological issues, of course, the Defense Department is doing a lot of work based on what they are seeing in Iraq and other places overseas. We get the benefit of that.

And then through our Office for Bombing Prevention, which is part of the Directorate of Infrastructure Protection, we actually educate State and local bomb detection and bomb prevention units in what they ought to look for and how they can deal with these threats.

A second element, of course, is detecting someone who is trying to bring a bomb onto an airplane or into transit or some other part

of infrastructure. Part of the process of doing that, of course, is deploying the existing technology. Part of it is an enhanced use of what we call VIPR Teams, which are teams with canines and other hand-held detection equipment that we can surge into mass transit. We do that in response to a particular threat. We do it in response to a high-profile event, like the Super Bowl or something of that sort. And we do it on a random basis.

A third element is the use of behavioral observation. This is a technique which we see overseas sometimes at airports. The Israelis use a version of this. We actually use it at the border. We train people in how to observe a behavior in a way that tips off somebody who might be planning to do us harm. And so as we have increased training and deployment of behavioral units at our airports and other locations, that has given us another element.

So we use the whole spectrum of tools, whether it be advanced scientific research, widespread deployment of existing technology, use of dogs, and training of our screeners and of State and local officials in how to detect different kinds of components and suspicious behavior.

Senator COLLINS. Director Mueller, there was a report last week by the Inspector General of the Department of Justice that was very critical of the terrorist watch list that is maintained under your direction. On the one hand, the IG found that there were several known or suspected terrorists who were not listed appropriately, and the IG was also critical that there were innocent people on the list and that it was very difficult for them to be removed from the list. All of us have had examples of constituents who have been on the list because their name is similar to someone who should be on the list.

What is your response to the DOJ IG's criticism of the watch list? This obviously is an important tool, but its usefulness is lessened if it is not as accurate and complete as possible.

Mr. MUELLER. Well, we absolutely agree with that, that it has to be as up-to-date as possible with the latest information. The IG's report gave us some credit for having made substantial strides since his previous report, but still focused on two areas in which we have still got a great deal of work to do. The first is in terms of redress. Since his last report, we have established an Office of Redress. It is operating. I think both the IG as well as ourselves would like it to operate faster. But it is operating successfully.

The second area is in the quality assurance of the information that we get, assuring that it is updated so that persons who may have been on the list at some point in time when we have additional information are removed from the list. And, again, as is often the case, it is a question of money and personnel, and we are putting money and personnel into assuring and upgrading our quality assurance.

The IG made 18 recommendations. We are following up on every one of those recommendations. I pointed to a computer glitch—I will call it a computer glitch—writ large in terms of the individuals that in a particular instance, but it was over a period of time, did not make it on the list, and that has been remedied. So we have taken each one of the recommendations from the IG and are working on those recommendations.

One more recent example is we have been able to go through and scrub the no-fly list and cut it in half. And so we are making progress in terms of the goals that we share with the IG in assuring the quality assurance on the list. But it is and has been exceptionally successful in terms of doing what it was established to do, and that is, identifying persons whom we do not want to let into the country, identifying persons who may be in the country, and giving us some indication as to where they are and what they are doing.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thank you, Senator Collins.

As is the custom of the Committee, we call in order of appearance, so the next three Senators are Senator Tester, Senator Warner, and Senator Coleman.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Thank you, Mr. Chairman, and I appreciate the panel's coming here today and testifying before us.

I want to add my voice to the many colleagues and witnesses in remembering the horrors of September 11, 2001. They are real stories of bravery, cops, firefighters, regular folks who performed acts of heroism that inspired us then and inspire us now. We should truly give thanks to those folks whose actions represented the best of what this Nation is truly about.

Six years ago today, I was a regular farmer in Montana, unprepared for what was going to be happening the next day. And today I am still a farmer, although I spend a little less time on the farm. But it is interesting to hear today about how our Nation has made advances, but still needs to strive for better preparedness.

In listening to the testimony this morning, we have made some progress, most impressively in first responders and sharing of information to deal with potential threats and actual emergencies. In other areas, we still need improvement. Some of it is due to new agencies. Secretary Chertoff as well as your predecessor have built a new agency, and I understand, Admiral McConnell, that the DNI has only existed for 2 years.

But in too many areas, we have seen a real lack of urgency. The fact that there appears to be no real effort to track individuals who overstay their visas, for example, is particularly shocking and troubling to me, especially when we try to address the immigration problems we face, as well as the homeland security problems we face.

The fact is there are still gaps, huge gaps. The security of our food supply needs to be addressed. Director Mueller and others, I think that you folks have got it absolutely right when you talk about the threat of complacency in this world post-September 11, 2001.

I would like to also talk a little bit about the men and women of our Customs and Border Patrol. I have had a chance over the years to visit with many of them who work the Northern Border that Montana shares with Canada. They work very hard, but too often many of them are overwhelmed with staff shortages and other personnel matters that can limit their ability to do their job.

As you gentlemen point out, they need to be right every time, while a terrorist only needs to be lucky once.

We have seen the GAO investigators that have been able to bring certain radiological materials across the Northern border, and we have seen potential terrorists attempt to cross into the United States through the Northern border. And as I understand it, we are about 1,722 Customs officers and 488 Border Patrol officers short on the Canadian line. I can tell you, my staff and I have heard a lot of complaints from folks trying to cross the border, DHS employees, from constituents traveling through these border crossings.

I will start my questioning with Secretary Chertoff, and that is, from your perspective as head of the Department of Homeland Security, what is the plan for getting staffed up at the Northern border?

Secretary CHERTOFF. Well, first let me say, Senator, that we—I guess when the President started his term, we had about 9,000 Border Patrol agents. As of last week, we are at about 14,400, and we are on track to being at 18,300 by the end of next year. So we are going to be doubling it.

Obviously, the largest element of the Border Patrol has gone to the Southern border, and that is because between the ports of entry 98 to 99 percent of the illegal crossings are the Southern border rather than the Northern border.

What we try to do on the Northern border is use air asset sensors and high-tech equipment as a way of getting a broader sense of who is crossing the border so we can deploy assets more efficiently.

I think we are on the way to having several air wings stood up along the Northern border, which will give us better coverage in terms of airframes.

I do envision some number of the new Border Patrol agents who are being added will be going to the Northern border, although I will tell you that the lion's share of those will be going to the Southern border.

What is particularly promising is as we work on what we call our SBInet, which is a combination of ground-based radar and cameras, we are currently operationally testing down at the Southern border. That will eventually be a tool that we use at the Northern border as well.

Senator TESTER. And I appreciate those efforts. I can just tell you that—and I know the focus is on the Southern border and for good reason. But I live 100 miles south of Medicine Hat, which is about 70 miles south of the Canadian border, 60 miles south, and I can tell you that it is fairly common knowledge, I mean, there is work that needs to be done there. So I really appreciate your efforts in that.

You talked a little bit about general aviation. You talked a little bit about containers. There has been some conversation about that. Can you give me any sort of idea on the containers that are coming in, commercial containers? What percentage of those are being tested? And do we need to put more emphasis on that?

Secretary CHERTOFF. By the end of this year, we will be scanning virtually every container that comes into the United States by sea, at least at the port at which it enters the United States. Also, pur-

suant to the SAFE Port Act, we have agreements with seven overseas ports to do the radiation scanning over there. We are operational in three of them, including one in Pakistan. And pursuant to the new legislation, we are going to try to put as much of this offshore as possible. But first things first. We are at a minimum going to get it done, as I said, virtually 100 percent by the end of this year. I should say by the end of next year we will be scanning virtually 100 percent of all the containers coming in through the land ports of entry, including from Canada as well.

Senator TESTER. That is good. I appreciate those efforts. My time has expired. Hopefully I will not get waylaid and I will be able to get back here.

Chairman LIEBERMAN. I hope so. Thanks, Senator Tester.

We are going to go to Senator Warner and then to Senator Coleman.

OPENING STATEMENT OF SENATOR WARNER

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

First, I would like to say that all of us remember September 11, 2001 but I remember it particularly because I remained on Capitol Hill with a small group of Senators, and this fine gentleman, Robert Mueller, came up with the Attorney General to brief us. My recollection was it was early afternoon, and you shared with us everything you knew at that time. And I look back on what few facts you were able to convey, and I see before us today a team of four of the finest public servants, most of whom have come in from other positions to serve once again in public office. And I have a great deal of confidence in this team and their ability to protect America.

I, for one, think we are going a long way towards protecting this country, certainly much beyond what you were able to convey on the morning of September 11, 2001. Am I not correct, Mr. Mueller?

Mr. MUELLER. Yes, and thank you for your comments, sir.

Senator WARNER. Thank you.

Gentlemen, I hold up here two cards: One is my Virginia driver's license and the other is my Senate ID. Now, this license is not unlike those in all the other States, and it was skillfully fabricated by several of the September 11, 2001 perpetrators. This Senate ID involves high-tech and, as far as I know, cannot be fabricated.

Now, the question comes about the REAL ID program. I consider it one of the highest priorities. I join with my colleagues Senator Collins, Senator Voinovich, and others to try to get the funding necessary to help the States begin this program.

We lost by only six votes. A swing of four votes could have made that difference. I hope that we repeat that effort in the near future, but I would like to ask each of you, given your dramatic statements here this morning, particularly about al-Qaeda and the threat to this country, where you ranked the REAL ID Act as a priority program. And do you fully or equivocally endorse it? Secretary Chertoff.

Secretary CHERTOFF. Well, Senator, as you know, under the REAL ID Act, we are bound and we are pushing very hard to get a nationally secure identification. We also have a similar complementary program for travel within the Western Hemisphere

called the Western Hemisphere Travel Initiative. I think this is one of the three or four really big items I want to get well launched before the end of this President's term. I think it is at the highest rank of priority, and—

Senator WARNER. That will help me. I want to try and get each one's opinion here. Admiral McConnell.

Admiral MCCONNELL. Sir, fully endorse. It is absolutely needed.

Senator WARNER. High priority?

Admiral MCCONNELL. Yes, sir.

Senator WARNER. Admiral Redd.

Admiral REDD. Same thing. Fully endorse. We need to get to the point where we can tell yes or no, this is the individual.

Senator WARNER. Director Mueller.

Mr. MUELLER. Anyone who has read the 9/11 Commission report understands the utility that the hijackers put to use these IDs, would understand the necessity and the importance of this program. I absolutely support it.

Senator WARNER. Highest priority?

Mr. MUELLER. High priority.

Senator WARNER. We have discussed al-Qaeda here this morning, and several of us serve on the military intelligence committees. We have a lot of discussion about that organization, and you have mentioned it, certainly, each of you today. Can each of you tell us what you can so that the American public has a little better understanding to what extent they are making efforts to take actions here in this country, and to what extent, if any, they have, should we say, chapters or splinter groups or self-appointed al-Qaeda in the United States? Let's start with you, Secretary Chertoff.

Secretary CHERTOFF. To be brief, Senator, they are still intent on carrying out acts against the United States, preferably in the homeland; if not, against American interests elsewhere. I think they are looking both to develop operatives so that they can launch from overseas. They are also, I think, hoping to radicalize those within this country. They have been less successful in the latter respect here than they have in Europe, but it is a growing issue.

Senator WARNER. Fine. Admiral McConnell.

Admiral MCCONNELL. Sir, they have committed leadership that can adapt. They have safe haven for training. They have middle management for organization, training, and preparation. The thing they need the most are operations personnel. We watched them recruit. We watched them bring them to Pakistan, that border area between Pakistan and Afghanistan, to train them in things like liquid explosives and so on.

So the intent is clear. They have not yet been successful infiltrating back in the United States.

Senator WARNER. As an organization, do you think they are as strong as they were on September 11, 2001, or much stronger?

Admiral MCCONNELL. They have regained a significant level of their capability. I do not think they are as strong because they commanded so much and were so much larger before the invasion of Afghanistan, and they had a country to operate freely in. So they are in an area that makes them difficult to get to, so I would say significant capability but not as strong as September 11, 2001.

Senator WARNER. And due to the successful efforts of our military and many others.

Admiral MCCONNELL. Yes, sir. Our military, and collaboration also with the Pakistani military.

Senator WARNER. Admiral Redd.

Admiral REDD. I would just agree that this strategic intent is unchanged, and in terms of the homeland or groups here inside the homeland, obviously that is what we spend every day looking at. If we know they were here, obviously they wouldn't be here, they wouldn't be effective. But we work extremely close with the FBI and across the intelligence community to make sure that any piece of information—and it may come from somewhere well outside our borders, which could indicate that.

Senator WARNER. In the domestic arena, Director Mueller, what can you share with us?

Mr. MUELLER. I look at it in three tiers: Core al-Qaeda in Waziristan, the border area, Afghanistan, and between Afghanistan and Pakistan where individuals were being trained; and the desire of al-Qaeda to insert such individuals in the United States as being a tremendous concern.

Second, you have loosely affiliated groups who may get some training but do not have the planning necessarily, orchestration from core al-Qaeda. The takedown in Germany, Denmark most recently, London, and Madrid are examples to a certain extent of loosely affiliated groups, of which we have got concern.

With those two groups, the biggest concern we have is those coming in from Europe who may have been trained and be inserted either by core al-Qaeda or undertake attacks in the United States without the planning or financial backing of core al-Qaeda.

And the last tier is those who are self-radicalized, those in the United States who do not have ties overseas with al-Qaeda, but adherence to that ideology. Miami and the Fort Dix plot are just a couple of examples of that.

We do have individuals in the United States who adhere to that ideology, that extremist ideology, and we work with our counterparts to make certain that we identify. We, after identification, determine to what extent there are other participants either here or overseas, and then work to disrupt those plots, and we mentioned some examples of that.

Senator WARNER. I thank the panel. I thank the Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Warner. Senator Coleman.

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. Thank you, Mr. Chairman. I want to associate myself with the comments of my colleague from Virginia, and thank you, gentlemen, for your service.

We have clearly gotten past the silo mentality, and I think it should raise the level of confidence, understanding that this is a race without a finish line. I remember, Secretary Chertoff, in your confirmation when you said you have got to be right 100 percent of the time, and a single failure is something we cannot afford.

Let me follow up on the question that my colleague from Virginia talked about, the level of the threat. Director Mueller, you kind of

broke it into three parts. When we look at homegrown, which is I think what we were seeing in Germany, first let me step back. Do we have the tools, do you have the tools that you need to identify the threats early on? Is there anything that you need in terms of the ability to surveil, the ability to respond, that you do not have today that this Congress should offer you? Secretary Chertoff.

Secretary CHERTOFF. I think at this point, from the standpoint of my agency—and I think Director Mueller can maybe talk a little bit more specifically about the Bureau—we do have the tools we need, including information and our ability to screen. I worry, however, that those tools not get taken away from us. I worry that people not start to degrade what we have spent time building up.

Senator COLEMAN. Is that in particular the PATRIOT Act?

Secretary CHERTOFF. Well, I am thinking particularly about some of our capabilities with respect to screening people as they come to the border, our ability to move to more biometric, fingerprint-based screening, and what Senator Warner said about identification cards. I mean, we are moving to get more secure identification. If we move backwards, that is going to make it harder rather than easier to detect problems.

Senator COLEMAN. Admiral McConnell, we just dealt with FISA, which is a temporary piece. That is not a final fix. Do you have the tools? And if not, what else do you need?

Admiral MCCONNELL. Sir, that is what I was going to mention, FISA, and it was a temporary fix. Some are of the belief that this community is spying on Americans, doing data mining and so on; that is simply not true. And so the debate with FISA gave us partially what we needed. So that debate is going to continue over the next few months, and if we lose FISA, we will lose, my estimate, 50 percent of our ability to track, understand, and know about these terrorists, what they are doing to train, what they are doing to recruit, and what they are doing to try to get into this country.

Senator COLEMAN. Admiral Redd.

Admiral REDD. I would agree, obviously, with all these comments. I would just mention there is another way that we can lose tools, and that is through leaks. These are methods which are extremely sensitive, and we have to be very careful, particularly when we have had a success somewhere, that people do not start thinking that it is okay to talk about how we did it because those are very sensitive and very fragile in some cases.

Senator COLEMAN. Director Mueller.

Mr. MUELLER. I would not talk so much in the way of tools as such, but in terms of understanding the importance of State and local law enforcement to our success, it is often overlooked because it is perceived in some way as being quintessentially a Federal problem. But every one of the cases we have made have been made by Joint Terrorism Task Forces where State and local law enforcement are absolutely essential participants.

To the extent that we develop sources in communities, it is State and local law enforcement that assist us developing those resources.

Senator COLEMAN. I was going to follow up with that question. By the way, let me ask you, are those efforts adequately funded?

Mr. MUELLER. I would say that we have to keep an eye that they continue to be adequately funded, particularly with the uptick around the country for violent crime. If you talk to a police chief or a sheriff, their concern is responsiveness to their community on violent crime, but it is absolutely essential to our success to harness the 700,000-plus State and local law enforcement around the country through the Joint Terrorism Task Forces or other mechanisms. And so I do believe as there is momentum to provide funding to address violent crime, we should not forget the necessity of utilizing and funding efforts by State and local law enforcement to continue to address the terrorism threat.

Senator COLEMAN. In addition to the State and local law enforcement focusing on the homegrown or even loosely affiliated—my background is as a former prosecutor—prisons are breeding grounds for gang violence. Are we looking at prison grounds as a breeding for terrorist activity? And do we have the tools to deal with that? Secretary Chertoff.

Secretary CHERTOFF. Actually, that is one of the first areas that we did look at because we had exactly the same insight that you did, that has traditionally been an area where you bring together people who are predisposed to break the law, many of whom are violent. They have time on their hands, and this can be a dangerous mixture.

We have done a lot of work with the Bureau jointly in places like California and New York, which are also doing a lot of work themselves, and we are working also with correctional systems not only at the Federal level, but in other States to talk about first of all identifying the problem, figuring out ways to reduce the problem, making sure there is adequate screening of people who are coming into prisons claiming to be religious leaders, to make sure they are not there actually promoting a brand of indoctrination that would create a danger. And I think this is an area of continued concern for all of us.

Senator COLEMAN. Anybody else want to respond to that? Director Mueller, is that an area you are looking at?

Mr. MUELLER. Yes. We, for several years, have had an initiative that looks not just at the Federal system, which is fairly easy to take care of, since they are also in the Department of Justice, but in the various prison systems at the State and local level. And in several of our Joint Terrorism Task Forces, we have representatives of the State prison systems that participate on a daily basis to address that ongoing concern.

Senator COLEMAN. Mr. Chairman, my time is up. I have a whole other area of inquiry on smuggling nuclear material. We are going to have at least a second round here?

Chairman LIEBERMAN. I hope so. Yes, indeed.

Senator COLEMAN. Thank you.

Chairman LIEBERMAN. Please come back. Thanks, Senator Coleman.

Admiral McConnell, at the risk of editorializing, which is a risk I will assume, I just want to come back and say by way of punctuating what you have said this morning, you said in response to my question earlier that the authority that the FISA reform law gave

you helped you—us—assist the Germans in breaking up that terrorist group in Germany.

Second, you have just testified in response to Senator Coleman's question that if you lost the FISA authority, you would lose 50 percent of the information capacity you have to gather about what terrorists are doing and planning to do to us. That is very compelling testimony.

I want to yield to Senator Voinovich because we are on the clock, but I want to thank you for it. Senator Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Mr. Chairman.

As Woody Hayes once said, "You win with people." In my mind, the real issue is having the right people with the right knowledge and skills at the right place and at the right time. And I think anybody listening to the four of you this morning has to be impressed with what we have heard.

During consideration of the Intelligence Reform and Terrorism Prevention Act of 2004, I underscored my belief that the interpersonal skills and the relationships between the leadership within the intelligence community was just as important as the organizational structure.

I want to commend all of you for working together. I am concerned about the continuity our intelligence community will have over the next several years as we transition to a new administration. I think this is something that all of us should give a great deal of consideration to.

Several years ago, we had testimony from State and local enforcement representatives who observed poor information sharing between Federal, State, and local government. I want to tell you there has been considerable improvements in this area. The Joint Terrorism Task Forces in Cincinnati and Cleveland are examples of this improvement, and you all ought to feel very good about that, Director Mueller.

Even with the increased resources and better information, I think that we must remember that in 1998 Osama bin Laden made a fatwa, or a religious decree, effectively declaring war on the United States. He declared war on us in 1998, stating "The ruling to kill Americans and their allies—both civilian and military—is an individual duty for every Muslim who is able, in any country where this is possible."

After reading the National Intelligence Estimate, we know the threat continues. I sometimes look back and wonder if we had taken the resources that we put into Iraq and had sent them to Afghanistan how far ahead we would be today from where we were then—although we have made, according to what you have said to us, some real progress.

My concern is how our Federal agencies are working together to reduce radicalization in the United States while at the same time ensures our democratic principles are upheld. Director Mueller, I have spent a lot of time talking to Muslims in Ohio, and one of their big complaints is on that. They feel that they are being unfairly profiled. I think that this is something from a dignity we must continue to work on.

[The prepared statement of Senator Voinovich follows:]

PREPARED STATEMENT OF SENATOR VOINOVICH

Mr. Chairman and Ranking Member Collins, I commend you both for convening today's hearing regarding our national security and the threats posed by terrorism to the U.S. homeland. On the eve of the sixth anniversary of the tragic and violent terrorist attacks of September 11, 2001, I know the question on many Americans' minds is: "Are we safer?" Although security is difficult to measure or quantify, the American public should be reassured that we are indeed safer.

The United States is at war against a transnational terrorist movement fueled by radical extremists who seek to harm us and our way of life. These individuals will continue to adapt and attempt to find new ways to disrupt our security. It is our responsibility as Members of Congress to thwart their efforts by providing the necessary tools to our national security personnel for mission success. This investment will continue to yield great dividends, as I strongly believe that strengthening our intelligence gathering capabilities is the first and best line of defense against potential terrorist activity.

Woody Hayes often said that, "you win with people." If you do not have the right people, with the right skills, in the right job, at the right time, no organization will meet its goal. The men and women of our law enforcement and intelligence communities have made great strides in cooperation in pooling resources to better counter threats posed by terrorists. The public is aware of at least several recent instances of intelligence and law enforcement personnel successfully disrupting terrorism plots including at John F. Kennedy Airport in New York and at Fort Dix in New Jersey. The U.S. homeland has been free from attack for six years; a fact we surely owe in part or in its entirety to the men and women working for the agencies represented today.

While we can enact legislation and authorize funding to minimize risk, it is an uncomfortable truth that we can never fully eliminate it. Thus, we must use common sense in developing future legislation to ensure our limited resources are allocated based upon risk assessments grounded in credible intelligence and analysis.

Several years ago, this Committee heard testimony from state and local law enforcement representatives who observed poor information sharing between the Federal, State and local government. Since that time, we have witnessed the positive development of State and local fusion centers throughout the country, with Federal agencies engaged in counterterrorism activities working together on a larger and more productive scale than ever seen before. For example, in my home State, the Ohio Strategic Analysis and Information Center, which partners with DHS and the FBI, has been positively regarded as a "one stop shop" for terrorism-related law enforcement information.

Even with increased resources, better information sharing and cooperation among agencies and across all levels of government, the threat remains real, and we must remain vigilant. In 1998, Osama bin Laden made a fatwa, or religious decree, effectively declaring war on the United States. He said: "The ruling to kill Americans and their allies—both civilian and military—is an individual duty for every Muslim who is able, in any country where this is possible." Almost a decade later, the threat from Osama bin Laden and al-Qaeda is still very real.

A significant challenge that remains is improving the Federal Government's ability to recruit and train skilled translators and linguists to meet our national security needs. Significant progress has been made in this area, but we need to do more to raise the proficiency of our intelligence and law enforcement personnel in critical foreign languages and cultures. Earlier this year, the Subcommittee on Oversight of Government held a hearing to examine our national level of foreign language proficiency. Unfortunately, the hearing revealed a shortage of Federal employees with proficiency in critical languages. Thus, I am anxious to hear from our witnesses about progress in this area.

In addition, our clearance processing system remains broken, limiting the ability of our national security agencies to meet their heightened mission requirements. The Subcommittee on Oversight of Government Management began its oversight work on the security clearance process during the 109th Congress because of our concern with the long standing backlog of security clearances and the cumbersome process that hampered the Federal Government's ability to clear highly skilled employees in a timely manner. I would remind my colleagues that this program has been on the Government Accountability Office's High-Risk List since 1990. The first timeliness milestones set forth in the Intelligence Reform and Terrorism Prevention Act for security clearance reform are behind us, but we still have a long way to go if we are to make meaningful improvements in this critical area. Accordingly, I look

forward to learning when the new process outlined in Director McConnell's 100 Day Plan will be operational.

I would like to thank our distinguished panel for sharing their thoughts and time with the Committee.

Senator VOINOVICH. I would like to hear more about what other things are we doing to try and eliminate this receptivity to Muslims in various parts of the world to Osama bin Laden's extremism.

Admiral REDD. Senator, I could give you sort of a top-down view, if that would help. I mentioned, too, in my remarks the National Implementation Plan, which is, for all intents and purposes, the Nation's war plan, if you will, for the war on terror. As you expect, it has stuff like protect and defend the homeland and go after the terrorists, but one of the key pillars in there is countering violent Islamic extremism. And so, that is recognized as one of the strategic musts or imperatives, for us as a government. If you go through that plan and you look at all the tasks that are assigned to the various Cabinet officers, almost 30 percent of them or a third of them are assigned to the State Department for exactly that reason.

So the short answer is yes, it is recognized. It is, as you understand, a very difficult problem. We have an analytic group at NCTC which works with the rest of the community in terms of what the messaging is. And as you indicated, there is no surprise in al-Qaeda's ideology. They have been very clear about it and very public about it from the very beginning. But in terms of how you message that and how that is broken down, I would say the State Department in fairly recent times has stood up a group called the Counterterrorism Communications Center whose job is, on a more tactical basis, to take a look at what is going on around the world and to start to get our side of the message out.

But as you well understand, this is not just a U.S. effort. You and I cannot do very well in terms of countering a fatwa by Osama bin Laden. It has to come from Muslim clerics who have that capability in other parts of the world. I think that we are starting to see in many cases a resurgence—not a resurgence, but the emergence of an understanding of that and effects beginning, but this is going to be the generational part of the war, in my view. This is why this is going to be like the Cold War in really only two respects: One, it is going to last a long time; and, two, it has a strong ideological component.

So I would say we recognize it, working to go in that direction, but this is a fairly new beast for us.

Senator VOINOVICH. Thank you.

Senator COLLINS [presiding]. First let me say it is wonderful to be Chairman again.

[Laughter.]

However briefly. Senator Sununu.

OPENING STATEMENT OF SENATOR SUNUNU

Senator SUNUNU. Thank you, Madam Chairman.

Director Mueller, there was an earlier question about the terrorist watch list, and I wanted to follow up on that a little bit to get a little bit more specific information about the recommenda-

tions of the IG and objectives for implementing their recommendations.

They made 18 suggestions. You indicated that you are already underway in implementing some of those suggestions. Could you speak to the two or three that you think are the most significant and describe the way that you think they will improve the integrity and usefulness of the watch lists?

Mr. MUELLER. Well, the two that I have mentioned before, I think, areas where we need to spend more effort, and that is in the area of quality assurance of the information. We have information coming through from a number of agencies that results in an individual's name being put on the watch list. What we have accomplished over the last several years, I guess, is put into place a quality assurance program that scrubs that information. It was pointed out by the Inspector General, and that was not working as well as it should. What we are looking at is adding personnel, improving training, and assuring that scrub is more effective and efficient than it has been in the past.

The second area is in redress, giving those who are stopped and believe that is as a result of their name being improperly placed on this watch list, is to give those individuals an Office of Redress where you can go and determine—and ask the questions about whether or not your name is on it and get some redress. We established that office—

Senator SUNUNU. How often does that happen?

Mr. MUELLER. I would have to get back to you, but I believe it is several hundred, the last figures I saw.

Senator SUNUNU. Over a one-year period, several hundred times?

Mr. MUELLER. I believe it was over a one-year period. And what the IG focused on, it is good that you set up an Office of Redress. What is happening is it takes too long to get that accomplished. And that is an area that, again, with resources, personnel, and training we hope to do better at.

Senator SUNUNU. Is there any particular area of law enforcement or particular source of information where names are being provided to the watch list that really should not be? In other words, any specific areas where the quality of the information provided has been especially poor?

Mr. MUELLER. No. I cannot pick any particular entity that contributes to the watch list and say this is more problematic. The problem comes in identifiers, and the problem comes if the name can be identifiers, dates of birth can be identifiers, and you can have with one individual a number of names; you can have a number of dates of birth associated with that particular name. And sorting out the information that may come in from overseas or may come in domestically and identifying it with a particular person with particular identifiers is a substantial challenge.

I will tell you, I believe the latest figure I saw, approximately 90 percent of the names on the watch list are individuals outside the United States.

Senator SUNUNU. You mentioned increased staffing a couple of times. How many more people do you expect to add to this task? And what is your timeline for implementation of the majority of the 18 recommendations?

Mr. MUELLER. I would have to get back to you on that, sir.

Senator SUNUNU. OK. Please do.

Secretary Chertoff, Senator Collins and others on this Committee have been very concerned about the process of implementing the REAL ID program. As you well know, my personal preference would be to have pursued aggressively the negotiated rulemaking, the collaborative rulemaking that was underway back in 2004 and 2005 prior to the passage of the REAL ID mandate.

At the moment, however, the proposal is to publish the final rule in October, and October is also the deadline for States to file for an extension for implementation. That would not seem to give the States a fair amount of time to really assess the scope, the costs, and the changes that are necessary for compliance in implementation. How are you going to address that administrative train wreck?

Secretary CHERTOFF. Well, first of all, we did put a preliminary rule out, and we did indicate that we would be quite reasonable in terms of granting extensions. The current plan would be in theory to have next spring be the point at which the process of people signing up for REAL ID licenses would begin. But we have indicated that we anticipate extending that to the end of 2009 upon a request and indication that States want to move forward and do that. And I think, frankly, a lot of States have now begun the process and have been seriously engaged with us in talking about what their plans are, including many of the major States—States like California, Arizona, and I think Virginia.

So I envision that this is not going to be a problem. I do think if a State does not want to participate, obviously, and they give us notice about that, that is not so much an implementation issue as it is a resolve issue.

Senator SUNUNU. As I understand, one of the requirements of the preliminary rule is that the data fields that are collected through the ID process would have to be made available in a database to all other States. That naturally raises privacy concerns, and I would like you to describe the way in which at the Federal level you intend to protect the private information, which I think everyone would understand needs to be protected in a very aggressive way.

Secretary CHERTOFF. Well, first, let me make clear that we have tried to design this so as to maximize privacy. We specifically avoided creating a new Federal database that would accumulate information that is otherwise not there. And we have also worked very closely with the Association of Motor Vehicle Administrators. There is a model for doing this kind of sharing with respect to commercial driver's licenses where there is cross-checking among States. So we envision using that model. It is basically a distributed model in which States would be able to have access to other States' databases for purposes of checking, but we would not create a new database.

I might add that one of the positive privacy benefits of the new rules is the requirement of background checks in DMVs. That is going to elevate the level of privacy. I can tell you historically as a prosecutor, I remember cases where people abused their access to existing systems for criminal reasons or because they saw an at-

tractive woman going down the highway and they wanted to get her phone number. So we are actually curing that problem by putting these background check requirements in place.

Senator SUNUNU. I appreciate your candor, and I would underscore that the privacy issues are issues that need to be a very high priority. I believe that they are with the work that you are doing, but it is always worth underscoring that we need to continue to maintain that priority status.

Second is dealing with the cost. This is a Federal mandate. You mentioned a new database is not being created, but there is a requirement that the information be shared, and that costs money and carries with it risks. So we have got to recognize the costs associated with the program and do everything possible to minimize those costs. There are some people that would like to use the fact that it is a mandate as an excuse to simply increase the size of the role or the responsibility at the Federal level. I think that the focus should be on minimizing the costs, and I hope you take that to heart.

And the third is the concern of unintended consequences, and that is probably my biggest concern with a program like this: Not that it cannot be implemented in a reasonable way, but that it will provide a foundation for others to use the program at a later date in ways in which it just was not intended. And it is very difficult to sit here today and to look 2, 3, or 4 years, or 10 or 20 years down the road and try to come up with ways that the program might be misused or misapplied or expanded in an inappropriate way. But I think that is something we all need to be conscious of, most of all those who are working to structure the program today. Thank you.

Thank you, Madam Chairman.

Secretary CHERTOFF. I think that is reasonable. If I might just for one moment.

Senator COLLINS. Yes.

Secretary CHERTOFF. The actual deadline for requesting extensions is going to be February 2008, so there will be some time to assimilate—

Senator SUNUNU. There will not be an October deadline to request an extension, but a February deadline?

Secretary CHERTOFF. Correct.

Senator SUNUNU. Thank you.

Senator COLLINS. Thank you. Thank you, Senator Sununu, for bringing up that very important issue. That is a major issue in both Maine and New Hampshire, as the Secretary is well aware. I think the Department went a long ways by setting up the new process, but I also hope that the Department is following through on a more collaborative approach, bringing in State officials, privacy experts, and technological experts to make sure this is being done in a way that will minimize privacy concerns as well as the rather extraordinary costs.

Is that process underway as well, sort of a negotiated rulemaking after the fact before you get to a final rule?

Secretary CHERTOFF. Well, we have done a lot of consultation in the run-up to the final rule that is going to be issued in the fall,

and that includes with State officials, the Motor Vehicle Association, and privacy people.

I might add as well, this kind of complements the Western Hemisphere Travel Initiative, and in particular, our efforts to get States to come up with enhanced driver's licenses that would satisfy that. I have myself in the last few months dealt with the governors of Arizona, California, New York, Michigan, Minnesota, and Vermont on all these issues, and States are increasingly signing up for enhanced driver's licenses, which will actually operate along a system that is very similar and scalable to REAL ID.

So what I think we are now beginning to see is not only do we have increased engagement with the States, but we have increased enthusiasm on behalf of most States for biting the bullet to get involved with this process.

Senator COLLINS. Thank you.

Director McConnell, I want to bring up the issue of information sharing further with you. I think you have made real progress, but this was a major recommendation of the 9/11 Commission. And when the Commission did its report card, it gave the government's efforts only a D as far as improving information sharing. Now, that obviously was before your time.

Recently, several technology companies have told my staff that there are technological solutions to the barriers that prevent intelligence agencies from more easily sharing information, and there have been recent reports that the NSA, for example, is linking databases to encourage information sharing.

But, unfortunately, we have also heard from the Program Manager for the Information Sharing Environment that the barrier is not really technological, that it is cultural; and that although a lot of progress has been made, that there still is a hesitation to share information particularly with State and local law enforcement.

Do you still believe that there are significant cultural barriers to be overcome before we have the kind of seamless system that will encourage the sharing of information that could be absolutely vital to thwarting and uncovering a terrorist attack?

Admiral MCCONNELL. Yes, ma'am, there are still significant cultural issues, and where we find ourselves is attempting to create a situation that would adapt to the current needs. By that we have a responsibility to protect sources and methods. We have a responsibility to protect those who have agreed to cooperate with us in spying on someone else, whose lives would be at risk if the information were compromised.

So the way I try to describe it when we are having this dialogue and debate in the community is we are committed to information sharing, but we also have a responsibility to protect sources and methods. So we want to try to create a situation where there is tension in the system. We cannot be prescriptive to get the perfect answer for every situation, but if we can create a culture where the analytical community is not thinking about—I have information, you have to demonstrate a need to know it, but my attitude as an analyst is I have a responsibility to provide—that puts tension in the system to share.

Now, for those who recruit spies or operate very sensitive systems or capabilities that, if compromised, we would have a loss of

life or lose a capability, there are people who want to not be as willing to share. So it is managing that cultural dynamic that is the big challenge. We recognize it, we are addressing it, and we are being very aggressive in attempting to transform this culture to get us to the right place.

Senator COLLINS. Thank you.

Chairman LIEBERMAN [presiding]. Thanks very much, Senator Collins. Do you want to finish the time or are you okay?

Senator COLLINS. I thought that since Senator McCaskill had not questioned—

Chairman LIEBERMAN. That is good of you. The remaining Senators who have not asked questions are Senators Akaka, Carper, Pryor, and McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL

Senator MCCASKILL. Thank you, Mr. Chairman.

First, thank you all. I listened to all of your testimony at a different location, even though I was not physically here, and I do want to congratulate all of you for putting in the effort and the time that you do every day to try to do the very best job we can in terms of making this country safe.

Unfortunately, the issue of whether or not we are safer or not has become colored with the brush of politics, as so often happens in our government, and that is unfortunate. And as I said the other day in a hearing, we cannot really say that we have not been attacked because of what we have done, because that is not true. Because if we were attacked tomorrow, the people who say that we were attacked because we failed, that would not be true either.

The truth is somewhere in between. We are safer, but there are still gaping holes. There are still major problems, whether it is communication, whether it is technology, whether it is the struggle for ideas that we seem to be failing at around the world, whether it is our image in the moderate Muslim world and how that is undermining the ultimate struggle we have, which is the radicalism that we find in some parts of the Muslim world.

I would like to focus for a minute on transportation security, and the reason I would like to focus there is that I used to say a long time ago when I was in the courtroom all the time that the courtroom that really mattered in terms of how we treated people was municipal court because that is where all the people came. Most people's contact with our judicial system has to do with going to court on a speeding ticket or something like that. They never have contact with what I call the "rarified atmosphere" of those rooms with all the lawyers around a deposition table or the litigation arguments that go on in big Federal courthouses around the country.

As people consider whether or not we are safer, really the face of our security many times is what they encounter when they travel. And that is where they are made to feel whether they are safer or not. And, Secretary Chertoff, I have been confused and I think the American people have been confused about what I would consider an inconsistent and a stutter start-stop in many different areas of airport screening and transportation security. And this seems to be a trivial example, but it is a great example of what I am talking about.

We all were taking liquids until one day no one could take liquids anymore. Didn't we know liquids were dangerous before that date? And if we didn't, why didn't we? And why did it appear that it was a knee-jerk reaction instead of something that was an overarching, consistent policy that had been well thought out?

Buried in that policy, after we decided liquids were dangerous, seems to be some kind of nonsensical thing that happened. And now, I was on a flight just yesterday where mothers were comparing notes:

"Well, I got my apple juice through. Did you get your apple juice through?"

"I got my formula through that was already mixed. Did you have to mix yours?"

And then the one that bugs women across America, particularly those of us who travel a lot, the mascara. I know it seems small, but for most people in America, they do not understand why mascara is a problem. It does not appear to be consistent or have any kind of rhyme or reason to it, and the reason I think that is important is because it is the face. It is the face that the traveling public sees. In fact, it is the face most Americans see.

So I would appreciate a little bit of input on that, and then I would like to ask some specific questions about advanced baggage screening and airlines' ability to pre-screen manifests.

Secretary CHERTOFF. I think you have basically asked two questions: Why did we suddenly put in place a ban on liquids, which we then modified slightly? And then some particular elements of the ban.

We knew that liquids were a vulnerability prior to the attack in London, or the attempted attack in London. We also were working hard to come up with a technology that would separate out dangerous liquids from non-dangerous liquids, and we had not found and have not yet found a technology that will do that in real time, meaning we can do it if you take a bottle and put it in a device, but if you multiply that by the millions of people who travel every day, it would be impossible.

What I think the London plot brought home to us was that the enemy had not only focused on liquids but had come further along in coming up with ways to defeat the measures we were using of a non-technological basis to detect potential problems, and that was in particular a focus on detonators as opposed to liquids themselves. And some of the measures we were taking to inspect liquids, without getting into too much detail here, were clearly—the enemy had figured out a way to potentially defeat it.

So having recognized where the enemy was, we determined that at that point the risk balance had changed. Our initial response was, of course, to make this happen very quickly. It had to be done in about 6 hours in a very—in an overnight session which I participated in. And then ultimately, after some careful study, again balancing the risk, we determined that a 3-ounce rule where you put 3-ounce containers in a 1-quart clear plastic bag was the right mix. It made it impractical to smuggle in explosives, but would allow people to bring in things that they like to have on airplanes. We did coordinate this, by the way, with the Europeans, and I think this will remain in place until such time as we are confident

enough operationally that we have detection equipment that we can loosen up.

Now, I can tell you, for example—let me say two things. The general rule is if it pours or smears, it is a liquid, and it has to go in that plastic bag. That is the simplest way I can put it. Sure, you can always come up with an example of something that is at the margin, but we have to come up with a rule that can be applied consistently across the board.

Do people sometimes succeed in smuggling things past the screeners? Sure they do. People sometimes smuggle drugs into the country. No system works 100 percent. But even if we are working 90 percent, that is a huge barrier to the enemy which is planning to try to smuggle something on an airplane.

So I think we have the balance struck right there. We obviously would love to get the technology in place, but I am not going to do it until I am confident it meets operational requirements.

Senator MCCASKILL. Can you briefly, since I am just out of time, talk about why we are now estimating that it is going to be 2024 before we get advanced baggage screening in place across this country? And what about the airlines being able to effectively screen their manifests with the sharing of information?

Secretary CHERTOFF. Well, the first thing is that we obviously do screen all the baggage currently now that goes in the hold of the airplane. We do it in a variety of different ways. Some of it is in line; some of it is not in line.

One of the challenges we have that is probably a little bit beyond the scope of the hearing is recognizing that the technology is changing and we need to find a method of financing and acquiring the technology that does not require billions of dollars in investments in equipment that becomes obsolete in 3 or 4 years. It is a little bit like having to keep buying your PC over and over again. It gets irritating after a while.

On the issue of screening the manifests, under Secure Flight, assuming Congress funds the request that we have made in the current budget, by the end of next year we should be doing all the manifest screening ourselves as you take it in, which will eliminate one of the real irritants, which is that when we take people off the watch list, the airline does not necessarily do it. So assuming we get the money from Congress, we should get that done by the end of next year.

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

Chairman LIEBERMAN. Thanks, Senator McCaskill.

I have been impressed, as others have this morning, by the reports that the four of you have given us about the progress we have made in closing some of the operational gaps on our side and in adjusting to meet an ever-changing enemy, and part of that is obviously prevention.

There is another side to this prevention of acts of terrorism carried out by Islamist extremists, and that is what has come to be called the battle of ideas, the battle for the hearts and minds of the Muslim world.

I know there are some programs in the State Department that are directed toward entering that battle globally, but what about

here at home? I do not know that any one of you is expected to play that role. I must say I have been impressed, Director Mueller, in our own series of hearings on the threat of Islamist radicalization here in the United States that the FBI has done some very significant outreach to the American Muslim community.

But let me start at this end of the table and work back to Secretary Chertoff. Are we effectively fighting the battle of—maybe I should go back one step further. You alluded to this in your opening statement. Do we have a problem of Islamist radicalization here at home? And if we do, what are we doing as the government working with the Muslim community to try to engage on the level of ideas and ideology? Because this is a war, but it is ultimately a war against and with an ideology that is inimical to our own values of freedom, tolerance, and diversity.

Mr. MUELLER. To the question of whether we do have a problem, I would say we do. It would be irresponsible to say that we do not. And if you look at some of the groups that we have investigated over the last couple of years and ultimately disrupted and prosecuted, you have to say yes, we do have a problem, particularly with the ubiquity of the Internet now and the ability for one to access anyone around the world who spews this radical ideology.

In terms of programs, as I have alluded to and I think you have held a hearing on—since September 11, 2001, we have had any number of ways that we undertake outreach to the Muslim American community, Arab American community, and Sikh American community. And that has been effective in the sense of working with these communities to understand the FBI, but also working with communities to develop ways, generally in local jurisdictions, to address the radicalization issue.

When I meet with Muslim leaders, the one point that we try to make is that the worst thing that could happen to the Muslim community here in the United States is another attack such as September 11, 2001. And so a great deal of activity that has to be undertaken to address this has to be done by the Muslim community itself and a recognition by the Muslim community, 99.9 percent is as patriotic and American as anybody else in this room or elsewhere, but to identify those individuals who may be subjected to that type of tutoring and the like, and to address it themselves or alert us that this may cause a problem. And that is within our particular bailiwick.

Chairman LIEBERMAN. Let me ask you this, and then I will move on to anyone else on the panel who wants to answer. Do you take it to be in any sense the responsibility of the FBI to engage in this battle of ideas here at home within the Muslim American community?

Mr. MUELLER. Put that way, I would say no, that it would not be our responsibility for any religion to engage in the war of ideas. I do think it is our responsibility to explain that once one goes over the line and it becomes not a war of ideas but a criminal offense, this is what you can expect, and to elicit the support of those in whatever religious community to assist us in assuring that those who cross that line are appropriately investigated and convicted.

Chairman LIEBERMAN. Thanks. Admiral Redd or Admiral McConnell, do you want to add anything on this subject, which is the battle of ideas?

Admiral REDD. I would just make the point, which I think we had another discussion, that if you understand that this is obviously a long-term issue which is going to be with us for some time, and the fact that strategic planning, the strategic operational planning is not very glamorous, nonetheless what we have done as a government is something which is, I think, very foundational, and gone through and laid out the war on terror, and one of the four pillars in that war actually is countering violent Islamic extremism, the war on ideas. It goes through, lists a number of tasks, assigns those tasks to different Cabinet officers—

Chairman LIEBERMAN. Who is doing them domestically?

Admiral REDD. The domestic part is probably the hardest part, and as you have just noted, we do not have a home office, per se, as the Brits do.

Chairman LIEBERMAN. Yes.

Admiral REDD. Primarily it is DHS and the FBI in their various roles. But overseas and obviously the other problem is how do you split this apart because something that is on the Internet does not stop at the water line, obviously.

Chairman LIEBERMAN. Correct.

Admiral REDD. So as you know, the State Department in recent days or recent months has stood up a group to get our counter-messaging out. But, again, the key to this thing is, one, it is going to be a very long battle; two, it is not just an American issue. It has to have the support of governments and of Muslim clerics around the world.

Chairman LIEBERMAN. Admiral McConnell, Secretary Chertoff, my time is running out, but I want to give you each a chance briefly to respond.

Admiral MCCONNELL. Senator, I think it is an excellent question and a very critical question, and the community I represent is primarily limited to foreign. If it doesn't have a foreign nexus, foreign focus—

Chairman LIEBERMAN. Right.

Admiral MCCONNELL. Even if there is a domestic situation, the intelligence community would only be engaged if the domestic situation was in contact with, influenced by someone in a foreign dimension. So our community is focused on foreign.

We contribute analytically to understanding. We would make that information available to policymakers who may be able to use it. But we are for the most part limited to foreign.

Chairman LIEBERMAN. Secretary Chertoff.

Secretary CHERTOFF. I do not want to repeat what others have said. Let me be specific about what we do.

We have what we call an Incident Management Team, which is chaired by the head of our Civil Rights and Civil Liberties Office. When there is an event in the world at large or domestically that we think will have an impact on the Islamic community because there is a terrorist element to it, we in advance, to the extent we can, of it becoming public, convene a group of community leaders, give them a heads-up, work with them to try to make sure that the

community is reassured that this is not going to become a general problem for the community at large.

In addition, we do quite a bit of aggressive outreach. I do it personally. I meet with community leaders. We had a group of, I guess, people in their early 20s that we convened for a conference that I had an opportunity to deal with, as well as going around and traveling around the country.

I will say I have kind of a bottom-line thing I say to the community. It is a battle of ideas, and in the end, when you are trying to counteract radicalization that is directed at people within the Muslim community, the people who are best situated to counteract that is the community itself.

Chairman LIEBERMAN. Right.

Secretary CHERTOFF. They do not want to hear the government argue theology. What they want to hear are community imams and community leaders arguing theology. And so one of our big pushes is to get the community to step up and get more involved in the process of counter-radicalization.

Chairman LIEBERMAN. I could not agree more. When somebody like bin Laden puts out a tape, or Zawahiri, obviously it is one thing for somebody from the U.S. Government to respond, but the really credible response would come from some leadership within the Muslim community. I thank you for your answer.

Senator Stevens, I know you are in the middle of another meeting, but I would be happy to call on you now.

OPENING STATEMENT FOR SENATOR STEVENS

Senator STEVENS. Well, thank you very much, Mr. Chairman. I am, and I wanted to come to ask the Director one specific question, and that deals with the attempts to give some type of immunity to those providers of telecommunications to respond to the government's requests for information. What is the status of that, Mr. Director? And how important is it for us to finish that and make a decision on that?

Admiral MCCONNELL. Senator, thanks for the question. It is absolutely essential, and the status currently is we have a temporary reprieve that is prospective, meaning going forward. So in the law that was passed and signed by the President on August 5, there is liability protection for those in the private sector who assist us going forward. We do not, however, have liability protection for the carriers or the private sector that assisted us in the past, and that is the key element we have to address in the coming months.

Senator STEVENS. Have you lost any of the cooperation you had in the past because of that hiatus?

Admiral MCCONNELL. Not at this moment, but we are on a path to lose all that cooperation. That was clear as we were negotiating over the summer.

Senator STEVENS. What is the deadline? We are marking up the defense bill this week, I believe, and other bills that have looked at this issue before.

Admiral MCCONNELL. Yes, sir. If we could get retroactive liability protection in the current time frame, it would put us in a very good position going forward. That is the key issue.

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

Chairman LIEBERMAN. Thank you, Senator Stevens.

Now, still on a first round for a couple of our colleagues, Senator Akaka, you would be next, followed by Senator Carper.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman. Even at this time I want to add my welcome to our witnesses here, and I would like to ask Secretary Chertoff about the DHS proposal to create a National Applications Office.

Let me preface my remarks by saying that I recognize the value of using imagery to improve our ability to prepare for and respond to disasters. It was at my initiative that the Office of Geospatial Affairs was created in the Department. Leaving a blueprint of critical facilities is important to our first responder community. However, at this point in time, I am concerned about the privacy impact of the new proposal to expand the Department's surveillance in the United States. I am also disturbed by the Administration's failure to consult with relevant committees of Congress, including this one.

After press reports revealed this program several weeks ago, my Committee staff asked for a briefing on the issue, but to date, the Department has failed to respond to this request. This raises further suspicions concerning the Department's intent. It is not clear what this new office will do.

Do national applications mean national technical means? As you know, national technical means include a much broader range of capabilities than just satellite imagery. Is this the case, Mr. Secretary?

Secretary CHERTOFF. I am glad, Senator, for the opportunity to clarify something which has probably become a little bit more obscure than it needed to be.

First of all, I apologize if there has been a delay in briefing you. I know well in advance of this rolling out, a number of committees were briefed. We probably did not brief all that we should have briefed, but we did brief the intelligence committees, the appropriating committees, and I want to make sure we complete that process.

This is really less of a big deal than it has been made to appear. There has always been something called the Civil Applications Committee, which is basically a way in which when customers in the civil domain want to use our satellites to get imagery, they operated through this committee to task the satellite to do the work. And as you pointed out, the vast majority of that was natural disasters, things of that sort.

I think the recommendation by outside consultants with some experience with the imagery a couple of years ago was that we were not being systematic and disciplined in the way we deployed these assets, and so the determination was made to take the cost of the Civil Applications Committee and have DHS become the executive agent, basically essentially Executive Secretariat of what used to be the Civil Applications Committee but what is now going to be renamed the National Applications Office. It is chaired jointly by Director McConnell and myself, and it will involve the participation

of all the stakeholders. And what it is designed to do is create a disciplined way for prioritizing how these imagery assets are used when they are requested by a civil agency.

Here is the critical point from a privacy standpoint. None of this changes any of the authorities or restrictions that are applied to the use of these means one iota. There is no suggestion here that this Applications Office is going to make it—is going to lift any restrictions or create any exceptions or circumvent any of the existing rules that currently govern the use of these means in various kinds of contexts.

Lawyers have been involved in designing this from the very beginning. Lawyers will be involved in the process of dealing with any request to use these means. And the bottom line is the authorities and restrictions that are currently in place will remain in place in every respect moving forward.

Senator AKAKA. Secretary Chertoff, the domestic use of national technical means raises very serious privacy and civil liberty issues. As you know, privacy and security safeguards must be built into any program at the beginning. While I understand that DHS' Chief Privacy Officer has issued a Privacy Impact Assessment, which is now being revised, I am curious as to whether the DHS Privacy Advisory Committee has reviewed and commented on the program. If so, what were its views?

Secretary CHERTOFF. Well, as I said, the Privacy Officer and the DNI's Civil Liberties and Privacy Officer were involved as of last fall in designing this program. Now, obviously the program is classified so the ability to share the details of it on the outside is a little bit restricted. But, again, let me try to make clear that the vast majority of uses one can envision here involve uses that have been of long standing. They involved, for example, imagery of things that people are doing out in the open in places that are visible to the naked eye or to an airliner flying overhead. And, in fact, although I think we are better than Google Earth, I do not think it is terribly different than Google Earth.

So I do not think any of these raise novel privacy issues. What we have tried to do, though, is build a process and to make sure that if we should wind up with an unusual application, we do not step over the line. And the process is built to have lawyers reviewing this at every stage of the process, much the same way as any other methodology or technique we might use for purposes of homeland security or law enforcement.

Senator AKAKA. Thank you for your responses. Mr. Chairman, thank you.

Chairman LIEBERMAN. Thank you, Senator Akaka. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks very much.

Gentlemen, thank you for joining us today and for your stewardship, for your service for our country, some for many years.

Mr. Mueller, you talked a little bit about the no-fly list, and I think you said—and I think it is a quote almost—that we scrubbed the no-fly list and cut it in half. And to that I can only say good for you. We have any number of people in my State who have the

misfortune of being given the wrong name by their parents, and they have ended up on the no-fly list and have gone through all kinds of trouble and turmoil, which I mentioned to at least one of you before. And every now and then I hear from them now, and they send not bouquets but thank-you notes, and it is a lot better than what we had before.

I realize how important it is to have no-fly lists and to make sure that they are accurate, but I also appreciate the fact that the work has been done to scrub it and clean it up.

The second thing I want to say—I think it was Admiral Redd, I believe it was during your comments, your testimony, not in response to a question. One of the things you said is our intelligence is better. Almost a verbatim quote: “Our intelligence is better.” And I want you to go back and talk to us about how is it better as it relates to the ability to get better human intelligence. What are we doing better in that regard, both inside this country and out?

Admiral REDD. Well, I think it is hard to talk very far into that, obviously, for all the reasons you understand. I think if you saw the *Washington Post* yesterday, you saw that there were an awful lot of folks who had been taken out of circulation, or taken off the battlefield. I think that is one of a number of instances which there was basically demonstration of the fact that our intelligence has gotten better. It is not only human intelligence, it is also signals intelligence and other stuff. But it is very difficult to go into many details. And as I mentioned in another comment, we have to be very careful about that because some of those sources are very fragile.

So I guess I would have to say look at the results. The terrorists are—I also said they are a very difficult target. You are talking about individuals. All the things we have been talking about here, how do you stop a single individual from coming across, and you do it by going after every element of the terrorist life cycle, starting with recruitment but through travel, communications, training, all the things that go on.

In open session—it is very hard to go much deeper than that, sir.

Senator CARPER. I understand. As an old air intelligence officer in the Navy, I can appreciate what you are saying. Let me follow it up, though, with a related question. I think since September 11, 2001, we have heard on any number of occasions that a shortage of folks with key language skills has been a problem. I just want to ask what, if any, progress has been made in recruiting and retraining key intelligence and other personnel with some knowledge of Arabic or other languages that are useful in counterterrorism.

Admiral REDD. I want to defer that one, if I could, to Director McConnell, since that is more along his line in terms of the training of the community. I will just say in general that not only in language but in analytic capability, writ large, obviously we have been growing a lot of folks. And as you will recall from your earlier days, if you want a petty officer with 10 years’ experience, it takes 10 years. We have been trying to stuff 10 years into 4 or 5 years. But in the analytic community, we have had to bring an awful lot of folks on line.

I will let Admiral McConnell talk about the language—

Senator CARPER. Admiral McConnell, are you willing to answer that question?

Admiral MCCONNELL. Yes, sir, I am.

Senator CARPER. Before you do, let me just add, maybe give you a second half to the question. Do you know of anything that we are doing to encourage more students to take up some of these languages early on?

Admiral MCCONNELL. Let me combine your questions, sir.

Senator CARPER. That would be great.

Admiral MCCONNELL. You asked specifically about Human Intelligence (HUMINT). We are on a path to double our HUMINT capability, so from September 11, 2001 until now, doubling the number of case officers and capability in the field.

The second thing I would comment is focus—

Senator CARPER. Over what period of time? Any idea?

Admiral MCCONNELL. Since September 11, 2001, until in the current time frame, it will double. And as Admiral Redd mentioned, just adding a body is one thing, but adding a trained body who speaks a language is another thing. So with the language capability, significantly improved, not enough yet. One of the things that we have decided to do or that we are attempting to do is to recruit more first-generation Americans. They have never been specifically ruled out by either law or policy, but by practice and custom. So we are trying to change the cultural approach inside the community. So if we have a first-generation American who speaks a language, understands the culture of the area of concern, that we would, in fact, bring them into the community and make them a part of it. So there are a number of initiatives to—

Senator CARPER. Any luck on that?

Admiral MCCONNELL. Yes. We have had significant luck, and we have had a lot of focus on training in languages, like Urdu, Farsi, and Arabic and so on. So much better than we were. We still have some distance to go, but that is our objective, to keep us focused on this particular problem because it is the most significant threat we face.

Senator CARPER. Good. Thanks. Thanks for that report.

At a hearing last week, Comptroller General David Walker—I call him “General Walker”—of GAO reported that maritime security is one of the areas where the Department of Homeland Security has had some of its best successes in recent years, and this is probably more for you, Secretary Chertoff. Witnesses from the GAO and the Department both testified that some of the reasons for the success are the fact that Congress did get involved and that the Department was able to work with us to devote some significant time and resources to the effort. I would ask are there other areas where we can see some similar progress or the potential for progress where that kind of attention on our part, as well as yours, can leave the kind of success that we have enjoyed with maritime security, or maybe chemical security, for example.

Secretary CHERTOFF. Well, there is, of course, as you know, Senator, one gap in the chemical security legislation that we had. Now, we are currently on the verge of issuing Appendix A, which is going to be very specific to people in the chemical sector about what is required from them in terms of self-evaluation, what are considered

to be the high-risk chemicals and the quantities at which they have to begin to submit themselves to regulation.

Wastewater treatment plants and water treatment plants were exempted from this, so that is an area where we are currently internally looking at the question of what are our authorities, if we need to use authorities. I have certainly argued to people in that sector that they need to be mindful of the fact that chlorine is a very dangerous chemical and it can be used in a variety of nefarious ways. And, therefore, securing chlorine against theft is something that they have to make their business.

Another area where we are, again, certainly looking at regulatory action, if not congressional action, is, as I said earlier, general aviation, in particular, private jets coming from Europe and Asia, where we want to make sure we have the ability to screen for weapons of mass destruction in the way we are doing with containers. And, finally, small boats is the area we are doing some work in now.

Again, I believe we have ample authorities through the Coast Guard, but I also want to make sure Congress works with us, first to make sure we are adequately funded to do what we need to do; and, second, to make sure we do not have backsliding. Sometimes the industry pushes back when we try to put security measures in place, and it is important to make sure that if we do put measures in place with respect to small boats we do not wind up getting pushed backwards.

Senator CARPER. Okay.

Admiral MCCONNELL. Could I follow on, if I may?

Senator CARPER. Please, yes.

Admiral MCCONNELL. You asked me things you could focus on. We are about to start a debate this month on a very important piece. If you think about it at a summary level, a major piece in the intelligence community, what do we do? We take pictures. We have human-to-human interaction—HUMINT, you mentioned earlier. Or we listen to other people's communications. That other people's communications is called "signals intelligence." We are going to debate that this month about whether to change or modify the law that was passed in August. It is very important that we retain that capability because it is a significant portion of what we are able to do with regard to foreign threats to the country.

Senator CARPER. I would just say in closing that we had a tough vote on the night of August 3, and some of us on our side voted with the majority on the other side. And I have personally taken—I would suggest to some of you I have taken a fair amount of flack from folks who are concerned about civil liberties, potential abuses to civil liberties. And I am encouraged to hear that the vote that we took was one that may have led to a better outcome in Germany than would otherwise have been the case.

I would just urge us, I would urge my leadership and I would certainly urge you in the Administration to work with us to find—let's not wait until January or the end of the year. Work with us now in the weeks ahead to find the right common ground so that we could go after the bad guys, do the right job there, protect civil liberties. There is a way to do both.

Admiral MCCONNELL. There is a way to do both.

Senator CARPER. Thank you.

Chairman LIEBERMAN. Thanks, Senator Carper. For my part, may I say that any flack you receive on that issue is wholly undeserved. I really believe it. I think this is intercepting communications between those who are not in the United States, and if it hits an American, Admiral McConnell and his folks go to court. I just think it self-evidently covers—that is what we need to do to protect the American people and also protect their liberties.

You have been very encouraging this morning, the four of you. I want to give you a small piece of encouragement. We promised that we would not keep you beyond 12:30, and we will not. So there will be a few other questioners, but we want you to be able to get back to your assigned responsibilities.

Senator Collins and I have already had our time on the second round, so in order of original appearance, we go now to Senator Coleman and Senator Voinovich.

Senator COLEMAN. Thank you, Mr. Chairman. Let me talk about the capacity to bring nuclear material into this country.

Secretary Chertoff, you talked about the ability to screen perhaps 100 percent of the cargo coming into this country and the efforts you are doing on cargo before it comes into this country, which is really ultimately where we need to be. I mean, God forbid a device went off in the port of Long Beach or New York, something like that. My question, though, has to do with the ability to detect shielded special nuclear material in lead pipes. I asked the question before about the resources that you need to do what has to be done. There are some difficulties even with the systems we have with certain types of nuclear material. Can you talk a little bit about where we are at in being able to truly screen that kind of material? Are there research issues, financing? I just want to know what we are doing to make sure that you have the tools that you need to prevent nuclear material from getting into this country.

Secretary CHERTOFF. The current operational technology, you are right—and I want to be careful how I say this—is much more challenged when it deals with heavily shielded material. It depends on what the nuclear material is. The greater the emitter, the harder it is to shield. But with respect to certain kinds of materials that can be used in a nuclear bomb, it is possible to shield it.

Currently, therefore, the way we deal with shielding is we really want to have a combined system where we both passively test for emissions, but we also actively test to see if there is dense material in the container which could be suggestive of shielding. And the constraint we face, which we are tapping overseas by building an integrated system, is how do you make sure you can pass containers through passive and active at the same time.

While we are building out a system to use both of those techniques, which is partly an issue of money, but it is also partly an issue of having foreign ports agree to do this and having them have a geographical footprint that allows us to do this, we are working on technology, which I cannot say is imminent, that would allow us to detect even rather heavily shielded material. But that is a bit of a ways off.

I would also say I would not underestimate the importance of intelligence in helping us focus and target on those containers where

there might be a higher risk, where we might actually want to open the container or at least pull it out and do a much more active interrogation.

Senator COLEMAN. I would hope when we talk about intelligence that it is one thing to rely upon detectors, which may or may not do what they need to do; it is another thing to be able to lock down nuclear material wherever it is to make sure that it is not in the hands of the bad guys. If I may say, one of our challenges with Iran, trying to figure out where they are at. It is one thing if they are depending upon their own abilities to generate material that can be used for atomic weapons. It is another thing if there is material out there on the market that they can have access to.

Admiral McConnell, in terms of that issue, of using intelligence to ensure that there is not nuclear material being bought or sold on the black market, where are we at with that?

Admiral MCCONNELL. I am very focused on that because we have information that al-Qaeda, as an example, has stated an intention to try to acquire nuclear material. So it is an area of intense focus. I wish I could be more optimistic to tell you that we have great confidence that we could always detect it. There are always potential work-arounds, but an area of focus, we have some sensors that would aid us in that capability, but it takes the entire panoply of intel resources to be able to do this. You have to penetrate targets. You have to have human agents. You have to be able to find places on a map, take the pictures, and also do the signals intelligence part. But it is an area of focus.

Senator COLEMAN. Let me just shift gears. It has been interesting with this panel here. The latest Osama bin Laden tape, first, is that his beard? It is a different-looking guy. Can you give me an assessment of what that tape is all about? Is there a purpose to it? Do we expect—is it a signal? I am not sure what we can talk about here, but I would like to get a better understanding of what we know after viewing that tape.

Admiral MCCONNELL. So far we do not think there has been a signal. He has done this periodically, as has Zawahiri, and there has not been a correlation necessarily between one of these tapes or a public statement and a particular event.

The big question in the community this morning is: Is that beard real? Because, as you know, just a few years ago, the last time he appeared, it was very different. So we do not know if it is dyed and trimmed or real, but that is one of the things we are looking at. But no specific message. It does reflect intent, and the big change for me as an intelligence analyst in the community, back in the Cold War it was very easy to do capability and always difficult to determine intent. In this situation, it is very difficult to capture the capability, a single human being in a given place, nuclear material, or whatever. So capability is the challenge, but intent is clear.

Senator COLEMAN. Again, my time is very short. Just following up on that, much of the discussion was American politics. Do we have a sense of someone who we assume is in a cave somewhere, do we have any sense of his ability to be tracking what happens in daily American politics?

Admiral MCCONNELL. Sir, the Internet has revolutionized that process, so we have good evidence that the al-Qaeda leadership reads the press, particularly the editorials, and——

Senator COLEMAN. And some of the things that are said in Congress.

Admiral MCCONNELL. And the Congress, no doubt. Every part of the debate, it is all watched very closely. And remember, there is an American in that group in Pakistan who is an adviser, I am sure. But there is a very close focus on this Nation because we are so open in what we do and what we say and where it might take someone.

Senator COLEMAN. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Coleman. Senator Voinovich.

Senator VOINOVICH. Director McConnell, Senator Akaka and I have held hearings on the security clearance process as part of our responsibility for the Oversight of Government Management Subcommittee. The security clearance system has been on GAO's high-risk list for quite some time. In the last hearing we had, Clay Johnson indicated that you were going to undertake a new system that would get the job done as part of your 100-day plan. Currently, I understand there is a wait time of 203 days for individuals awaiting clearances.

What is the status of the new system? Have you discussed it at all with Comptroller General Walker, who will be determining whether or not our security clearance system should be removed from the high-risk list? What is your strategic plan? Are there metrics that will be used to judge whether or not the new system in place is effective?

Admiral MCCONNELL. Sir, first of all, it would be fair to say that there is a debate. Some would argue that we need to go faster and do better with the current system. General Jim Clapper and I, in DOD, representing all the intelligence capability in the Department of Defense, and me on the DNI side, we have agreed to run a pilot, and our fundamental premise is we want to re-engineer the process. You mentioned 203 days. General Clapper and I believe we should be able to do that process in 30 days or less.

Why do we believe that? We can look at the commercial models where they clear people very quickly, people that handle billions of dollars of transactions. What is the difference? If you can automate the process and clear people quickly, and then change the way we do business, that we monitor the life cycle of the employee, we can get to faster in the front and better protection in the back.

I would submit, of the spies we know about, all but one or two of them did it for money. And of the spies that we know about, almost every one of them did not know they were a spy when they came in on the front. So the key is life-cycle monitoring. So we are trying to run the pilot to make it go much faster and hopefully be much more effective. We will know more about the end of this pilot in some months.

Senator VOINOVICH. Will we know about it before this Administration leaves office?

Admiral MCCONNELL. Yes, sir. If we are going to have any impact at all on the system, we have to do it before this Administration—

Senator VOINOVICH. How soon?

Admiral MCCONNELL. It is months, sir. It took us a period of time to agree to it. This was one of the issues, when I came back in the government, that was very important to me as having been on the outside struggling with it. So I made it a priority. We got the agreement from the Defense Department. We worked with Clay Johnson. We are running the pilot, and in some matter of months, we will be able to tell you if it is working or not.

Senator VOINOVICH. I would suggest also that your people spend some time with the Government Accountability Office because during this Subcommittee's hearing last week, Mr. Schneider from DHS and Comptroller General David Walker spent about 20 percent of their time quibbling over the definition of what the metrics were to determine whether or not DHS had done what it was supposed to do.

Is there anyone that is really working on this whole issue of winning the hearts and minds of Muslims here in the United States and around the world? This is not a new issue. And, quite frankly, I am not confident that anybody has really sat down to figure out a major effort in this area to win the hearts and minds of people not only here in the United States but around the world. Could you comment on that?

Secretary CHERTOFF. Yes, let me venture into this. Although I do not think there is a single person, we do have a committee, and I think it is actually chaired by the head of our Civil Rights and Civil Liberties Office, that looks at that issue in the United States. I think the Bureau and the Department of Justice are represented on it. We do not deal with the overseas element. We deal with the domestic element of it. And a lot of it is outreach, and it is from the top level down to the regional and local offices to get people from the government out into the community trying to recruit individuals to come into government service. I do not mean as informants. I mean to occupy positions in government service so that the community feels they are part of the process of homeland security and law enforcement. Part of it is giving notice to community members when something is happening in the world so they can reassure the community. And some of it is just a lot of outreach to get the community engaged in the process of counter-radicalization.

This is all supported by research that we do. We do a lot of research through our Intelligence and Analysis Directorate looking at studies. Some of them are academic studies; some of them are studies we get from overseas as to what causes radicalization. I think the FBI does a lot of that as well, and they tend to be maybe a little more focused on individual cases. We tend to be maybe a little bit more general.

So we do have a very focused strategy on this issue. I should say—and I have to be a little careful here because the First Amendment does limit us to some extent in getting into the area of what I would call too upfront efforts to persuade or convince. I think we generally feel, at least in our Department, that we are

best served by getting the community itself to get out there and—

Senator VOINOVICH. What would give me comfort is to see how these efforts are linked. I recently met with Imam Abdul Rauf, who has organized a forum of Muslim religious scholars to work on connecting democracy and the U.S. Constitution to the foundations of Islam to show that they are compatible.

I think that much greater effort has got to be made in this area. We are on the defense, and we are trying to secure the country. But I think that unless we recognize the challenge that we have got on this other side, our success will be limited. We need to have an offense here, and I am not sure we have one.

Admiral REDD. Senator, if I could comment on that. As I mentioned earlier, we have built this thing called the National Implementation Plan, which is the overall blueprint. One of the four pillars of that is exactly that—countering violent Islamic extremism. And it goes through and lays out a number of tasks, assigns those tasks to different Cabinet officers. You have heard about the domestic part of it, and you are correct, the State Department has a lead for the overseas piece of it. And we are starting up—Karen Hughes has an operation, as you know, the Counterterrorism Communications Center, which is designed to be on a very tactical basis to respond to things that happen around the world.

But clearly this is tough. This is new for us. Some people try to compare it to the public diplomacy thing we did during the Cold War. But even that is significantly different because we were basically talking to Western or similar cultures in those days.

But it is not just an American issue, obviously. As you mentioned, it is going to take people who have credibility in the area, whether it is here in the United States or overseas. I would say that a lot of foreign governments have obviously woken up to this and are becoming more involved. But it is going to be a long—it is going to be a generation—

Senator VOINOVICH. I have taken enough time, but all I can tell you is from my perspective how well we do in that regard will have a major impact on how long this war against Islamic extremist religious fanatics goes on. I really bring to all of your attention that something should be done to pull everybody together and figure out a master plan on how this thing is going to work.

Admiral REDD. I could not agree with you more, sir.

Chairman LIEBERMAN. Thanks, Senator Voinovich.

Senator Akaka, we will have a last round, and then Senator Collins did not use all her time, so I am going to have her ask one last question.

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

Admiral McConnell, more than a year ago, we learned that the CIA had closed the bin Laden issue station, a unit that had focused exclusively on finding Osama bin Laden and his top lieutenants. At that time the CIA said that it did so partly because al-Qaeda had changed form, evolving from a hierarchical organization with bin Laden at the helm to one characterized by a collection of splinter cells. However, both were testimony that the July 2007 NIE stated that bin Laden and his deputy have been able to regenerate al-Qaeda and key elements of its homeland attack capability.

Given this assessment, do you believe that a unit dedicated to finding, capturing, or killing Osama bin Laden and his top officials should be re-established?

Admiral MCCONNELL. Sir, it is established. I would say it is probably a matter of semantics, but we have such a unit. Osama bin Laden and Zawahiri are our No. 1 and No. 2 priority, very strong and significant focus. And so we are pursuing it with significant resources.

Senator AKAKA. Admiral, if bin Laden has reconstituted the al-Qaeda organization so that it looks similar to its original pre-September 11, 2001 form, then do you believe that finding him should be the top priority?

Admiral MCCONNELL. Top priority; yes, sir. And I would add another dimension. You mentioned splinter groups a moment ago. I would describe it a little differently. There are extremists in virtually any country. What al-Qaeda has been successful in doing is linking them. So now if you start across Northern Africa, in Algeria, Tunisia, Libya, Egypt, Lebanon, all the way across, there are groups now that affiliate with and some even change their names to be al-Qaeda. So it almost takes on the connotation of a franchise.

So I think the reasoning maybe a year ago was splintering, but the fact that they have sanctuary in that tribal area between Afghanistan and Pakistan has allowed them to adapt and morph. With the sanctuary and committed leadership, they have rebuilt the middle tier. What they do not have is the vast numbers of recruits to carry out the acts they would like to perpetrate. So that is where we have our focus, is to try to cut off the head of the snake.

Senator AKAKA. Admiral Redd, in early 2004, then-CIA Director George Tenet said that al-Qaeda's leadership was seriously damaged and had continued to lose operational safe havens. Today we have a different picture of al-Qaeda, one in which the organization has become resurgent and is rebuilding.

What in your opinion has changed? And why hasn't the United States been more successful in heading off such a resurgence?

Admiral REDD. I think if you look back, Senator, at the history from September 11, 2001, it has been a series—as all warfare, if you do not mind me using the analogy—of puts and takes, or pressure and response. And I would say the single most critical factor over the last year, year and a half, has been the resurgence of that safe haven in the tribal areas of Pakistan.

Senator AKAKA. Do you believe that, as currently configured, the Executive Branch agencies are well placed to help reverse that tide?

Admiral REDD. I think, sir, the whole thrust of our testimony has been that the agencies are working together in ways that we have never worked together before, whether it is across attacking terrorists or protecting and defending the homeland. But the short answer is you never stop on that, and you keep moving, you keep trying, and you keep pushing. And that is clearly one of our highest priorities.

Senator AKAKA. Admiral McConnell and Admiral Redd, the July report issued by the National Counterterrorism Center stated that the key to al-Qaeda's resurgence has been the use of ungoverned

spaces in Pakistan and, in particular, areas along the Pakistan-Afghan border. Yet I understand that Pakistan restricts the deployment of American troops in these areas in hot pursuit of those terrorists' networks.

As long as these safe havens exist, what is there to prevent the continued resurgence of al-Qaeda? Admiral McConnell.

Admiral MCCONNELL. If the safe havens continue to exist, we will continue to have this problem. About a year ago, the leadership in Pakistan made a decision as a way to address the problem is to form an alliance or a peace treaty, if you will, with the tribal leaders in this area. Remember, this area has never been conquered by anyone, not even Pakistan—never been controlled by Pakistan. It is a separate enclave in their constitution, so it is an independent region in that border area.

So the leadership in Pakistan decided they would make an accommodation with the leadership to force the foreigners—to be expelled. That did not work. We counseled against it. It did not work.

Now, what has changed since that time? President Musharraf has moved two additional divisions into the area, is applying additional pressure. We are cooperating with the Pakistanis, providing information, intelligence. We are working it from the Afghan side of the border, working with Special Operations Forces and so on. So intense focus, but as of this point in time, we have not been able to eliminate it. But it is our No. 1 priority.

Senator AKAKA. Would you comment, Admiral Redd.

Admiral REDD. I would just agree with Director McConnell. I mean, we clearly understand the high priority of this. The cooperation out there is significant. I think it is fair to note, too, that the Pakistanis themselves are also victims of al-Qaeda's violence. It is not just the United States. But it is a longstanding issue, and it is one which has a lot of policy dimensions to it. It is being worked very hard.

Senator AKAKA. Thank you for your responses. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka.

We have reached 12:30, but Senator Collins did not use her whole time, and Senator Carper, who is a very effective advocate, has asked to ask one more question. If any of you have an urgent need to depart, we will understand. If not, two more questions.

Senator Collins.

Senator COLLINS. Thank you. That is, we will understand if it is after our questions.

This Committee has worked diligently to try to identify shortcomings and gaps in the legal authority that you have as we try to fight this war against terrorism. Last year, for example, Secretary Chertoff, you told us that we needed authority in the area of chemical security, and we passed legislation giving you that. More recently, Admiral, you came to us on the FISA issue.

I would like to ask each of you to identify any legislative reforms or authority that you need to more effectively do your job as we battle terrorism. Secretary Chertoff, we will start with you, and we will just go down the panel.

Secretary CHERTOFF. I did mention the issue of wastewater and water treatment, and I think we are contemplating what we might

do to address that issue and whether we ought to make a suggestion to Congress.

If I might, I would like to request the opportunity to actually think about that and come back with a little bit more of a comprehensive answer than I give just off the table.

Senator COLLINS. Thank you. Admiral Redd.

Admiral MCCONNELL. Like Secretary Chertoff, I need to give you a more deliberative answer, but I have been back only a few months, as you are aware, and the title is Director of National Intelligence. I think "Director" may be a little bit of a misnomer. I am more of a coordinator. So when I want to make a hard decision, it is a little bit like this body. As opposed to deciding, you get to engage in dialogue and debate and so on. It was made reference earlier that it is interpersonal skills. Well, mine have been tested quite a bit to try to get hard decisions made.

So at some point, I will formulate some recommendations about do we need to make some adjustments to how we are organized. We did not create a Department of Intelligence. We created a Director of National Intelligence who has a responsibility of coordinating a community of 15 of 16 agencies who work for another Cabinet officer. So there is a challenge or two embedded in that.

Senator COLLINS. Thank you. Admiral Redd.

Admiral REDD. As you know, I wear the two hats on the intelligence sides. Obviously, in fact, I am actually part of the DNI, and the DNI has actually used his authorities to help us out in some cases. So I think I would certainly identify with everything Admiral McConnell said.

I think there is a question which is not now but is probably a year or so down the road, on the other race to strategic operational planning. As you know, when the 9/11 Commission came out, they had in mind a much more, shall we say, aggressive or directive view of that. I do not think we are far enough down the road to know whether that is desirable or even doable. We are working together. But I think that is something that in a couple of years the Congress may want to come back and look at.

Senator COLLINS. Thank you. Director Mueller.

Mr. MUELLER. One of the areas we are concerned about and have been for some time is, first of all, the lone wolf actor who is not tied in with any particular group overseas, and we addressed that in legislation a year or so ago. But as you have self-radicalization growing and radicalization in the United States, where it does not have any foreign component, we operate under Title III, the criminal side of the house. And over a period of time, as technology has improved—and the statutes focus on facilities, a particular facility as opposed to the target. One of the things I would like an opportunity to get back to you on is the possibility of making modifications to make it easier with appropriate safeguards to do interceptions of those individuals who might be self-radicalized and intent on undertaking terrorist attacks as opposed to other criminal activities within the United States, without any foreign nexus.

Senator COLLINS. Thank you. And let me just conclude by thanking you all for your extraordinary service. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Those are important answers. Senator Carper.

Senator CARPER. I would second that closing comment from Senator Collins.

Secretary Chertoff, I am going to telegraph my picture and let you think about this while I make a comment or two. It is rare that you come before us that I do not ask you about rail security and transit security, and that will be my question, to ask you for an update. We have talked here today a little bit about maritime security and chemical security, but I want, before we leave, for you to give us a bit of an update on how we are doing with respect to security for people who ride trains and people who take transit, especially rail transit.

I want to go back to Senator Akaka's questioning of you, Admiral McConnell, and he focused a good deal on Osama bin Laden, and you mentioned—I think what you said is, "Our focus is to cut off the head of the snake." I urge you to maintain that focus.

Secretary Chertoff, your Department is going through a rule-making with respect to potentially establishing reporting requirements for those who have significant quantities of propane on their properties. You probably heard a little bit about this. On the Delmarva Peninsula, we have hundreds of chickens for every person who lives there. There are 300 chickens for every person who lives in Delaware. We have a lot of chicken farms, and we have tens of thousands of them around the country, and your agency has been intent on trying to establish some kind of reporting requirement for chicken farmers who have significant quantities of propane.

I think we are in the process of trying to infuse some common sense into that argument. I would say good and we look forward to the final outcome.

One of our chicken farmers on the Delmarva Peninsula said, "The worst thing that could happen if they blow up my propane in my chicken house is we end up with barbecued chicken." So he did not think it was all that bad. But I would just ask that we focus more on where the real threat lies. I do not think that is where it lies.

Your name has been in the news as a potential Attorney General. I do not have any question that you would be a very fine Attorney General. I heard last week that you had asked not to be considered, and I think we need in your Department continuity. Not worst things that could happen, but one of the not so positive things that could happen would be to just add to that turmoil, so I applaud your decision. I hope the President was listening.

Here is your opportunity to respond to my question: How are we doing on transit security, rail transit security in particular?

Secretary CHERTOFF. First, just on the issue of propane, let me make clear that there was a preliminary rule that was put out. It is put out precisely for the reason that we do want to get comments back, and it is not uncommon and it is pretty easy to anticipate that we are going to take those comments into effect.

It is going to be a line-drawing issue. There is going to be an amount of propane that is large enough and close enough to a major population area that we will have to regulate it. But we really do not want to regulate chicken farmers. We are not worried about barbecued chicken.

With respect to rail security, as you know, Senator, we put out not only a round of grants earlier this year, but then a supplemental round. So we have got several hundred million dollars out there, and we would be very focused on a risk-based approach in which we look at those elements of the rail system that are the most vulnerable. If we are talking about passenger rail, that tends to be a highly populated mass transit, particularly where you are dealing with track that is underground or underwater. And, frankly, that is where we are putting most of our money and most of our effort.

At the same time we are doing a couple of other things. We are working to increase the number of what we call VIPR Teams. These are combined teams of TSA personnel, and now we are adding in some Coast Guard and Custom Border Patrol personnel that we surge into a train station or we went onto the Seattle ferries last month, with canines, with handheld devices. They are not meant to be steady state, but they are meant to be random surge operations, similar to what the New York Police Department does where every week or so they put a whole bunch of police cars out and they surge into an area and in a counterterror operation. So we are proceeding with that, too.

The third thing is we are looking at different kinds of systems that would be used to potentially detect explosives without putting into place in train stations what we have at airports, which would not work architecturally. That is a technological challenge. I promised Admiral Cohen I was going to use this word in a hearing, and I am now going to use it. Muon technology, which involves the subatomic particles, is apparently a promising technology but some distance off; that if, in fact, it is capable of being implemented, would allow us to detect in a stand-off way explosives in a confined area, like a train station or something.

So we are proceeding on all of those tracks, and it is a very high priority for us.

Senator CARPER. Mr. Chairman, thank you for giving me that opportunity. One last quick thing I would say is Senator Voinovich was talking about how do we defuse some of the hatred and animosity toward our country, and he, I thought mentioned—in the back-and-forth some good ideas were discussed. I would suggest that one of the things that needs to be done is for a real serious effort to be made in support of what is going on in the dialogue between the Israelis and the Palestinians on the West Bank. That by itself is not going to solve this problem, but to the extent that the Palestinians could end up with a homeland of their own and the Israelis could end up with peace and secure borders, that would sure help.

Chairman LIEBERMAN. Thanks very much, Senator Carper.

Thanks to the four of you. I must say, Senator Collins and I just said before she had to go that while the first part of what we asked you to do today, which is to assess the current threat environment, obviously your assessment is serious, it is sobering. This is an alarming and persistent threat environment. But the second part, which is to give us a report on the status of institutional reform to deal with the threat, has been, in my opinion, greatly encour-

aging, understanding that we all know that we have got a lot more to do.

I would add that the four of you each bring tremendous experience and talent to this assignment. You are impressive in your individual capacities, and you give the definite impression that you are working well together as a team. And I will note with some particular appreciation in this capital city that you seem not to let your egos get in the way of carrying out your assigned responsibilities to protect our homeland. So we thank you for all that, with the understanding that we have got a lot more to do. We look forward to doing it together to protect our country and its people.

The record of the hearing will remain open for 15 more days for additional questions and statements. I thank you all again. The hearing is adjourned.

[Whereupon, at 12:43 p.m., the Committee was adjourned.]

APPENDIX



STATEMENT FOR THE RECORD

MICHAEL CHERTOFF

SECRETARY
UNITED STATES DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

UNITED STATES SENATE
HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE

"CONFRONTING THE TERRORIST THREAT TO THE HOMELAND:
SIX YEARS AFTER 9/11"

SEPTEMBER 10, 2007

INTRODUCTION

Thank you, Chairman Lieberman, Ranking Member Collins, and Members of the Committee for the invitation to appear today. I appreciate this Committee's steadfast support for the Department and your many actions to improve our effectiveness.

At the outset, I'd like to acknowledge the strong working relationships we share with the Director of National Intelligence (DNI), the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC), as well as many other federal, state, and local partners working around the clock to protect our country and the American people from terrorist attacks.

None of us alone can keep our nation safe from the threat of terrorism. Protecting the United States is a mission we share and one that requires joint planning and execution of our counterterrorism responsibilities; effective information collection, analysis, and exchange; and the development of integrated national capabilities.

Of course, tomorrow marks the six-year anniversary of the 9/11 attacks. As our nation remembers this unconscionable act of terrorism and the murder of nearly 3,000 innocent men, women, and children, it is appropriate that we take a moment to assess the current terrorist threat facing our country, weigh our efforts to defend the United States against additional attacks, and set our priorities for the future.

It is no accident that we haven't suffered a major terrorist attack on U.S. soil since 9/11. I believe it is the result of the President's leadership, this Committee's support, and the hard work and constant vigilance of hundreds of thousands of men and women – including the 208,000 employees of the Department of Homeland Security – who are working tirelessly both at home and overseas to protect our country.

Since 9/11, our nation has put in place critical tools that have strengthened our ability to identify terrorist threats to our homeland, dismantle terrorist cells and disrupt terrorist plots, and prevent terrorists from crossing our borders or assuming false identities to carry out attacks.

Among other successes, we foiled serious terrorist plots to attack U.S. military personnel at Fort Dix, New Jersey, and a plot to explode fuel pipelines at John F. Kennedy Airport in New York City. In August of 2006, we also worked with British authorities to disrupt a threat that would have killed thousands of Americans aboard commercial aircraft departing the United Kingdom.

But while we have successfully raised our barrier against terrorist attacks, the fact remains that we are still a nation at risk. The recently issued National Intelligence Estimate makes clear that we continue to face a persistent threat to our homeland over the next several years. We also cannot discount the danger posed by homegrown terrorists, isolated individuals or groups that initiate their own plots after becoming radicalized.

Our nation faces a set of important choices. How do we respond to this ongoing threat? What actions are necessary to protect our country? And how do we build upon our success to date?

OUR DEPARTMENT'S ROLE

As you know, DHS was created to unify and coordinate federal, state, and local capabilities to prevent, protect against, and respond to all hazards – including terrorist attacks.

Congress gave us broad authorities under the Homeland Security Act of 2002 to prevent terrorist attacks in the United States, reduce our nation's vulnerability to terrorism, and assist in the response to and recovery from major attacks. The Intelligence Reform and Terrorism Prevention Act of 2004 also strengthened our ability to share intelligence, improve information sharing and first responder communications, and enhance border and transportation security. Among its key initiatives, the law established the requirement for a secure document to enter or re-enter the United States. We continue to make progress in implementing this key recommendation of the 9/11 Commission. We also have benefited tremendously from the SAFE Ports Act of 2006, which formalized efforts to enhance port security, improve cargo inspections, and strengthen radiation detection, among others.

We recognize that we cannot protect every person from every threat at every moment. To do so would require unlimited resources and would be at a tremendous cost to our freedoms, our economy, and our way of life. Our challenge is to manage risk consistent with our understanding of threats, vulnerabilities, and consequences, and then prioritize our resources to protect against high-threat, high-consequence events.

Since becoming Secretary, I have set five major goals to focus our Department's efforts on a core set of objectives. These goals are as follows: 1) keeping dangerous people from entering our country; 2) keeping dangerous cargo out of our country; 3) protecting critical infrastructure; 4) boosting emergency preparedness and response; and 5) strengthening DHS integration and management.

Because the focus of this hearing is threats to our homeland, my testimony will highlight only the first three goals: preventing dangerous people and dangerous cargo from entering our country, and protecting critical infrastructure. I will also discuss our efforts to share information and intelligence necessary to achieve these goals. I will reserve a discussion of emergency preparedness and the Department's internal management functions for a subsequent hearing. In addition, I testified on these issues last week before the House Committee on Homeland Security.

PROTECTING AGAINST DANGEROUS PEOPLE

A key priority for our Department remains keeping dangerous people from entering the United States to engage in criminal activity or to carry out terrorist attacks. If we can

prevent dangerous people from infiltrating our borders then we have successfully dismantled a large part of the threat.

Passenger Screening

One of our most important screening tools is information we collect about visitors seeking to enter the United States. We gather this information electronically through our Advance Passenger Information System (APIS), from Passenger Name Record (PNR) data, and through biometrics collection under US-VISIT.

Leveraging this information allows us to check passenger names against terrorist watch lists, search for connections between known and unknown terrorists, and run biometric finger scans against fingerprint databases and integrated watch lists in real-time. With these systems, we have prevented thousands of dangerous people from entering the United States, including individuals suspected of terrorism, murderers, rapists, drug smugglers, and human traffickers. Let me provide a couple of examples.

In May of this year, a British citizen attempted to board a flight from London to the United States. Using PNR data, U.S. Customs and Border Protection (CBP) officers determined the individual as a watch list match. Airline security officers prevented the man from boarding and he was turned over to British authorities for further questioning.

And in April of 2006, at Boston's Logan Airport, CBP officers used PNR information to identify two passengers whose travel patterns exhibited high-risk indicators. During the secondary interview process, one subject stated that he was traveling here on business for a group that is suspected of having financial ties to Al Qaeda. The examination of his baggage revealed images of armed men, one of them labeled "Mujahadin." Both passengers were refused admission.

This year we reached an important agreement with the European Union that will allow us to continue sharing PNR data while protecting passenger privacy. We will also continue to collect PNR data from flights originating in other regions around the world. In addition, we are moving forward with a regulation that will require general aviation aircraft entering the United States to provide comprehensive passenger manifest information to CBP prior to departure. This will help us prevent private aircraft from being used to bring potentially dangerous people or weapons into the United States.

In partnership with the Department of State, we are also expanding collection of biometrics at U.S. embassies and consulates overseas to include 10 fingerprints of an individual. The Department of State will have capabilities to collect 10 prints at all visa issuing posts by the end of CY 2007. This November, we expect to deploy 10 fingerprint collection capabilities to an initial set of ten U.S. airports, and we expect to have capabilities to collect 10 prints at all U.S. ports of entry by the end of CY 2008. Capturing 10 fingerprints will allow us to search databases for latent terrorist fingerprints. The Coast Guard also has implemented a program to collect biometrics on individuals

intercepted in the Mona Passage near Puerto Rico, giving us greater insight into who is seeking to enter the United States illegally through our maritime domain.

Secure Identification

As part of our Western Hemisphere Travel Initiative (WHTI), we've taken steps to prevent terrorists from using fraudulent documents to enter our country. As of January 23, 2007, citizens of the United States, Canada, Mexico, and Bermuda seeking to enter or re-enter the United States from within the Western Hemisphere must present a valid passport or acceptable alternative document if arriving by air.

Beginning January 31, 2008, we will also end the acceptance of oral declarations alone at the border and require U.S. and Canadian citizens to present either a WHTI-compliant document or government-issued photo identification, such as a driver's license, and proof of citizenship, such as a birth certificate, to enter the United States at land and sea ports of entry. We also anticipate fully implementing WHTI in 2008, whereby travelers will need WHTI-compliant documents – a passport, a passport card, a NEXUS card, or other acceptable document as defined in the WHTI final rule – for land and sea border crossings. We will consider a number of factors in determining the date for full implementation including the availability of WHTI-compliant documents.

The 9/11 Commission noted that for terrorists, travel documents are like weapons. We intend to take those weapons off the table. By requiring secure documents to enter the United States, we will make it harder for people to use fraudulent credentials to cross our borders, and we will make it easier for our inspectors to separate real documents from fake, enhancing our security and ultimately speeding up processing.

We also continue to work with states to enhance the security of driver's licenses under the REAL ID Act. Drivers' licenses are the primary form of identification in our country. We must make sure these documents are not easily forged or misused, and that consistent security standards are in place for their production. We are also actively engaging several states, including Washington, Vermont, and Arizona, and we are in discussions with several others to develop a more secure, enhanced driver's license that will strengthen border security and facilitate entry into the United States.

Border Security

Of course, we remain committed to effective border security to prevent the illegal entry of people between our ports of entry. Despite the failure this year to pass comprehensive immigration reform, we are aggressively moving forward to bolster security at the border in a number of important areas.

We have increased the size of the Border Patrol from approximately 9,000 agents in January 2001 to almost 14,500 agents today. We have worked with Governors to deploy thousands of National Guard forces to support construction of new fencing and vehicle barriers, with a target of 370 miles of fencing and 300 miles of vehicle barriers by the end

of next year. We have installed high-tech cameras and sensors, and deployed unmanned aerial vehicles as part of SBInet. We have expanded CBP air and marine branches to increase our coverage of the border. We have established Border Enforcement Security Task Forces to work collaboratively with state and local partners to fight criminal activity in border cities. And we have developed an Intelligence Campaign Plan for Border Security to provide comprehensive intelligence support for our operations.

As a result of these efforts, we have seen significant decreases in apprehensions – down 21 percent overall along our southern border, and in some sectors down as much as 68 percent – reflecting decreased flow due to stepped-up security. While we will never be able to hermetically seal our border, our efforts have strengthened our ability to keep dangerous people out of the country and have made our nation safer.

PROTECTING AGAINST DANGEROUS CARGO

Threats, of course, come in many shapes and sizes, including dangerous cargo infiltrating the international supply chain. Our greatest concern with respect to a cargo-borne threat is a terrorist attempting to smuggle a weapon of mass destruction into our country through our sea ports, land border crossings, or maritime borders.

Overseas Inspection

Since 9/11, we've built a system of layered security to identify and intercept such cargo before it reaches our shores. We now require advance information – including comprehensive manifest information and shipping history – on all containers bound for the United States, and we inspect all cargo that we deem to be high-risk. Through our Container Security Initiative, we've also deployed U.S. inspectors to 52 foreign seaports covering more than 80 percent of container traffic to the United States.

Radiological and Nuclear Detection

As part of our Secure Freight Initiative, in conjunction with the Department of Energy and the Department of State, we are also placing radiation detection equipment, imaging machines, and optical character readers in an initial set of seven foreign ports. Three of these ports – Port Cortes (Honduras), Port Qasim (Pakistan), and Southampton (U.K.) – will scan 100 percent of the cargo coming to the U.S., fulfilling Section 231 of the SAFE Port Act requirements. Operation testing on a more limited capacity will take place in the four remaining locations. This testing will provide important information on how we can address the unique screening challenges associated with larger and more complex ports. At home, we've installed more than 1,000 Radiation Portal Monitors at critical seaports and land ports of entry to detect radiation before containers are allowed to enter the domestic supply chain. By the end of this year, we will scan nearly 100 percent of cargo for radiation at our major seaports and we will scan nearly 100 percent of cargo at all ports of entry by the end of next year.

We remain concerned that a small vessel could be used to launch a *U.S.S. Cole*-style attack against our maritime infrastructure or to smuggle dangerous weapons, materials, or people into our country. To address this threat, we continue to work with small vessel owners and operators across the country to better understand risks associated with small boats and to identify ways to improve our detection and tracking capabilities.

We also recently launched an initiative to reduce vulnerabilities associated with small vessels operating in U.S. waters. Through our West Coast Maritime Preventive Radiological Nuclear Detection pilot program, we will work with local authorities, beginning in the State of Washington, to conduct vulnerability and risk assessments and field evaluations; provide technical guidance and expertise; and deploy radiation detection technology and equipment to key maritime pathways with a view toward enhancing radiological scanning of small vessels.

PROTECTING CRITICAL INFRASTRUCTURE

Whether our aim is protecting boats, bridges, or other critical infrastructure, we cannot do so effectively without strong partnerships with private sector owners and operators of our nation's critical infrastructure. Consistent with our risk-management philosophy, we want to protect the most critical assets from the most serious threats.

Sector Specific Plans

Earlier this year, we completed all 17 Sector Specific Plans of the National Infrastructure Protection Plan. These plans are our roadmap for working with the private sector to assess vulnerabilities in our nation's infrastructure, set priorities, measure our effectiveness, and ensure accountability.

This is the first time in our nation's history that the government and the private sector have come together on such a large scale – across our entire economy – to develop a joint plan to reduce risk and protect key assets and resources. It is a tremendous milestone for our Department, the private sector, and the American people.

Aviation Security

As we know, our nation's transportation sector remains a target for terrorists. Since 9/11 we have continued to add additional layers of security to protect the traveling public while ensuring its freedom of movement.

Our commercial aviation system now benefits from multiple security measures, including hardened cockpit doors, Federal Air Marshals, Federal Flight Deck Officers, 43,000 Transportation Security Officers trained to detect explosives materials and devices at checkpoints, explosives detection canine teams, 100 percent passenger and baggage screening, and enhanced inspection of air cargo.

To stay ahead of evolving terrorist threats, the Transportation Security Administration (TSA) has implemented a program to train its workforce to focus on passenger behavior for signs of malicious intent. The Screening Passengers by Observation Techniques (SPOT) program builds on proven methods to identify potential threats based on a person's behavior, not physical characteristics. This program already has proven successful. In August of this year, a TSA Behavioral Detection Officer trained under the SPOT program identified an individual at a ticket counter carrying a loaded gun and more than 30 rounds of ammunition. The SPOT program also has netted drug carriers, illegal aliens, and terrorism suspects.

In August of this year, TSA also published a proposed rule to streamline watch list procedures for domestic air travelers under our Secure Flight program. We intend to transfer control of watch lists checks from the airlines to TSA. This will result in greater consistency in how these checks are conducted and will reduce hassle for misidentified travelers.

Improvised Explosive Devices

Homeland Security Presidential Directive 19 established a national policy to protect our country against the threat of domestic improvised explosive devices (IED). We have seen the damage and loss of life that IED attacks have caused in Iraq and Afghanistan, and earlier this summer terrorists used a vehicle-borne IED in the attack against the Glasgow Airport. We must continue taking steps to prevent the use of such weapons in our own country.

To address this threat, our Science and Technology Directorate (S&T) has established a counter-IED task force to leverage existing multi-agency research and investments to deter, predict, detect, defeat, and mitigate the impact of IED attacks.

Beginning in FY 2008, S&T plans to accelerate and bolster its research and development of counter-IED technologies and products. S&T also continues its important work to develop, test, and evaluate a range of technologies and systems to detect explosives threats to air cargo systems, airport checkpoints, passenger baggage, mass transit systems, and critical infrastructure such as bridges and tunnels.

In addition, the Attorney General has led a review of ongoing activities in order to report to the President ways in which we might improve our security against terrorist use of explosives in the United States. The President called for this effort in Homeland Security Presidential Directive 19, and the Department of Homeland Security has been a leading partner in executing the President's direction.

Chemical Security

To keep dangerous chemicals out of the hands of terrorists, we have initiated a risk-based chemical security program using the regulatory authority we were granted last year by Congress.

In April of this year, we issued an interim final rule that requires chemical companies to assess the risks posed by their facilities and the chemicals they house or produce, and to implement security countermeasures to meet federal chemical security standards.

Because we want to approach chemical security comprehensively, we've also taken steps to protect dangerous chemicals in transit. Through agreements with the rail industry, we will reduce the time that rail cars carrying toxic inhalation hazards (TIH) remain at a standstill in rail yards. Further, last year we proposed regulations to require a positive chain of custody and better tracking capabilities for rail cars transporting TIH and other high-risk hazardous materials. In addition, we worked closely with the Department of Transportation on its proposed regulations to require rail carriers transporting TIH and other high risk materials to select the safest and most secure routes. When finalized, these actions will significantly reduce the risk of an airborne chemical threat endangering our cities and major population centers.

Biological Security

Providing early-warning biosurveillance information on human and animal health, the food and water supply, and the environment is critical to preventing a biological attack against our homeland or mitigating its impact.

Through the National Biosurveillance Integration Center, we are building an integrated system for collecting, monitoring and evaluating biological threat information so that we can rapidly characterize biological threats, whether man-made or naturally occurring. The center, which we expect will be fully operational by the end of next fiscal year, will integrate information coming from federal partners to develop a real-time understanding of the new and evolving biological threats we face.

Our BioWatch program also has been in continuous operation since 2003 and is present in more than 30 of our nation's largest metropolitan areas to provide an early detection capability in the event that a biological agent is released into the air. We are working on the development of the next-generation BioWatch system that will be fully automated to provide faster detection and analysis capability.

We also continue to work with our federal partners, including the Department of Agriculture and the Department of Health and Human Services (HHS), as well as state, local and private sector partners, to establish a well-coordinated readiness and response architecture for food and agro-defense. In addition, we've conducted formal risk assessments of 28 biological agents and used the resulting information to inform the acquisition of medical countermeasures by HHS and to prioritize and inform other national investments in biodefense.

Cyber Security

We must work in partnership with the private sector to protect our nation's cyber systems and to reduce our vulnerability to attacks that have the potential to cause serious disruption and economic damage.

Part of our strategy involves helping federal agencies regulate traffic on their cyber and communications networks using our "Einstein" intrusion detection system. Through our U.S. Computer Emergency Readiness Team (U.S. CERT), we also work with the public and private sectors to identify potential cyber threats, share warning information, and coordinate incident response activities.

For example, during a recent denial of service attack against the Government of Estonia, U.S. CERT leveraged international partnerships to quickly raise awareness of the attack, share information, and mitigate its impact. U.S. CERT coordinated with federal, international, and private sector partners to identify more than 2,500 sources of attack from 21 North Atlantic Treaty Organization (NATO) countries. This information was shared with military, intelligence, law enforcement, and CERT personnel from NATO member nations.

Through our Science and Technology Directorate, we are also conducting research, testing, and standards development to fortify our nation's communications infrastructure, including our cyber networks.

SHARING INFORMATION AND INTELLIGENCE

Of course, the common thread that ties together and supports all of these efforts is effective information collection, analysis, and sharing. I've said before that information is our radar for 21st century threats. Reliable, real-time information and intelligence allows us to identify and characterize threats, target our security measures, and achieve unity of effort in our response.

The Department of Homeland Security is both a collector of intelligence and a consumer of intelligence. Two of our components – the Coast Guard and our Office of Information and Analysis – sit at the table with the Intelligence Community and work hand-in-hand with our partners at the DNI, FBI, and NCTC.

Our department is also a tremendous consumer of intelligence. Intelligence shapes how we respond to threats, it arms our frontline personnel with information they need to do their jobs, it impacts how we invest our resources, and it allows us to make risk-based decisions.

We are dedicated to being a full partner within the Information Sharing Environment (ISE), and in so doing we are equally committed to sharing timely, relevant information with federal, state, local, private sector, and international partners.

Office of Intelligence and Analysis

Under the leadership of our Chief Intelligence Officer, we've refashioned and made more robust our intelligence enterprise at DHS. Our Office of Intelligence and Analysis (I&A) has improved the quality of intelligence analysis across the Department, including a focused effort to train our professionals to recognize information with intelligence value. I&A also has more fully integrated intelligence collection across the Department's components; raised our visibility within the Intelligence Community; and improved transparency with Congress.

To counter the threat of radicalization and extremism in our homeland, I&A also has created a branch focused exclusively on this issue. This branch seeks to expand our understanding of the "how and why" radicalizing influences take root. Our Office for Civil Rights and Civil Liberties is part of this focused effort to better understand radicalization, improve our capacity to counter domestic radicalization, and engage Muslim Americans, Arab Americans, and other key communities.

We remain committed to implementing the Intelligence Reform and Terrorism Prevention Act of 2004 and the President's directives to improve information sharing across our Department while protecting civil liberties and privacy. To this end, in February we issued a *Policy for Internal Information Exchange and Sharing Memorandum* to all DHS components to make sure they have access to terrorism, law enforcement, and homeland security information within DHS that is relevant to their mission. We also constituted an Information Sharing Governance Board, chaired by Charlie Allen, our Chief Intelligence Officer, to oversee the implementation of this policy. Hugo Teufel, our Chief Privacy Officer, sits on this board to ensure privacy and civil rights laws and policies are followed and institutionalized.

State and Local Fusion Centers

Of course, we must continue to share timely, relevant, and useful intelligence and information with the full range of our homeland security partners. Our goal is two-way flow. We want to provide useful information to our state and local colleagues, and we seek to benefit from their direct links to their communities and their visibility into potential terrorist plots developing at the grassroots level.

A major driver of this collaboration is State and Local Fusion Centers (SLFC) that promote information sharing and exchange across at all levels of government. We are working closely with the Program Manager for the ISE and the other members of the Information Sharing Council to support national efforts to include state, local and regional fusion centers as a robust part of the ISE.

We see tremendous value in creating a national network of state and locally run information clearinghouses that provide a clear, effective channel for information exchange as well as accurate, timely, and actionable intelligence products and services in support of homeland security.

We are working with the Department of Justice to gather, aggregate, and review data collected to evaluate the level of capability of state and major urban area fusion centers across the nation. Once this assessment process has been completed, we will be in a better position to offer recommendations to SLFCs on staffing, services, and resources.

To date, we have deployed 17 DHS intelligence officers to SLFCs across the country and we plan to have officers in as many as 35 sites by the end of fiscal year 2008. We are also deploying our Homeland Security Data Network (HSDN) to fusion centers to foster information sharing and exchange up to the Secret level. Twenty fusion centers will have HSDN access by the end of this year and we will double that capacity by the end of next year. In addition, we are building an analytic training program – equivalent to what we have for our own intelligence officers – for state and local analysts who work in fusion centers, and we are in the process of developing privacy and civil rights training.

Closed Circuit Television

States and cities have taken the lead in developing information and intelligence fusion centers with important support from our Department, including more than \$300 million in grant funding. But another important counter-terrorism tool we continue to support is the development and deployment of closed circuit television (CCTV) systems.

Multiple cities – including New York, Chicago, San Francisco, and Philadelphia – have invested in CCTV systems to improve monitoring of potential incidents, protect transportation systems and critical infrastructure, and enhance response and mitigation measures.

We believe these systems, when used transparently and in accordance with appropriate privacy laws, have enormous potential to boost eyes on the ground, identify anomalous or threatening behavior, and aid in terrorist and criminal investigations. Indeed, we need look no further than the use of CCTV cameras following the terrorist attacks last year in London to see their potential benefits. The perpetrators of the attacks were identified with the help of London's camera network, and the four individuals who attempted to explode bombs in the subway two weeks later were swiftly identified and brought to justice through use of CCTV cameras.

CCTV systems are a critical component of our layered approach to securing critical infrastructure, and we will continue to allow states and cities to fund these systems using DHS grants.

National Applications Office

Finally, it is important that we use the technological assets of the Intelligence Community to our greatest advantage. To this end, our Department has established the National Applications Office (NAO) to leverage the assets and capabilities of the Intelligence

Community for civil applications, homeland security, and law enforcement purposes, including disaster preparedness, emergency management, and border security.

Our goal is to work with intelligence agencies to improve access to appropriate intelligence products for domestic users at all levels of government. The NAO will not expand existing capabilities or change how these systems are used. This program will also be subject to robust oversight by privacy and civil liberties offices within our Department, the DNI, as well as the independent Privacy and Civil Liberties Oversight Board.

WORKING AS ONE TEAM

Our value as a Department rests in our network of assets and people, and our ability to leverage that network to achieve integration and work effectively with our federal, state, and local partners.

While it will take time for us to reach full maturity, there is no question we have made substantial progress to build shared critical capabilities, work as one team, and create a Department that is more than the sum of its parts.

Part of our success in thwarting terrorist plots has been a direct result of our ability to work together. During the plot against fuel pipelines at JFK airport, our Department worked closely with the FBI to assess the threat to airport infrastructure, inform the owner of the pipeline, and release joint DHS-FBI intelligence products. Our Intelligence and Analysis Office and the Transportation Security Administration both played critical roles in supporting the investigation and eventually disrupting the plot.

Representatives from Immigration and Customs Enforcement also worked with the FBI to take down the terrorist plot against our military personnel stationed at Fort Dix, New Jersey. Our Department also closely coordinated with the FBI, other national security agencies, and our international partners during the liquid explosives threat to commercial aviation just over a year ago. During this threat, TSA deployed Federal Air Marshals to the United Kingdom and other international destinations to expand its mission coverage. CBP also increased its enforcement efforts within U.S. airports, deploying special response teams, canine units, and explosive detection technology.

CONCLUSION

On September 11, 2001, no one would have predicted the passage of six years without another terrorist attack on U.S. soil. Some believe our country hasn't suffered another attack because we've been lucky. Others contend the terrorist threat has diminished and we are no longer in danger.

I disagree. Over the past six years, we have disrupted terrorist plots within our own country and we've turned away thousands of dangerous people at our borders. We've

also witnessed damaging terrorist attacks against some of our staunchest allies in the war on terror.

I believe the reason there have been no additional attacks against our homeland is because we've successfully raised our level of protection and we've succeeded in frustrating the aims of our enemies. That's not to say our efforts have been flawless or that our work is done. On the contrary, we must move forward aggressively to build on our success to keep pace with our enemies.

Our improvements to passenger and cargo screening, critical infrastructure protection, and intelligence fusion and sharing must continue. While no one can guarantee we will not face another terrorist attack in the next six years, if we allow ourselves to step back from this fight, if we allow our progress to halt, if we don't continue to build the necessary tools to stay ahead of terrorist threats, then we will most certainly suffer the consequences.

I'd like to thank this Committee for your ongoing support for our Department. We look forward to working with you and with our federal, state, local, and private sector partners as we continue to keep our nation safe and meet our responsibility to the American people.

**Senate Homeland Security and Governmental Affairs
Committee**

10 September 2007 hearing on

**Confronting the Terrorist Threat to the Homeland:
Six Years after 9/11**



Statement for the Record

of

J. Michael McConnell

Director of National Intelligence

Statement for the Record

Director of National Intelligence, 10 September 2007

Senate Committee on Homeland Security and Government Affairs

“Confronting the Terrorist Threat to the Homeland: Six Years After 9/11”

Chairman Lieberman, Ranking Member Collins, and members of the Senate Committee on Homeland Security and Government Affairs: Thank you for your invitation to appear before the committee to provide a status report on the nation’s efforts to confront terrorist threats to the nation and to describe the implementation of institutional reforms mandated by Congress and by Presidential directive since September 11, 2001.

It is my privilege to be accompanied by Michael Chertoff, Secretary of Homeland Security, Robert Mueller, Director of the Federal Bureau of Investigation, and Vice Admiral John Scott Redd, Director of the National Counterterrorism Center.

Terrorist Threat to the U.S. Homeland

I would like to begin my statement with a discussion of the findings of the July 2007 National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the most authoritative written judgment of the Intelligence Community (IC) on a particular subject and a declassified version of this NIE’s key judgments was made available on the Internet. It assessed the following:

- The US Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa’ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.
- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa’ida to attack the US Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.
- We are concerned, however, that this level of international cooperation may wane as 9/11 becomes a more distant memory and perceptions of the threat diverge.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts to put operatives here.
- As a result, we judge that the United States currently is in a heightened threat environment.
- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.
- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the US population.
- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.
- We assess Lebanese Hizballah, which has conducted anti-US attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.
- We assess that the spread of radical—especially Salafi—Internet sites, increasingly aggressive anti-US rhetoric and actions, and the growing number of radical, self-generating cells in Western countries indicate that the radical and violent segment of the West's Muslim population is expanding, including in the United States.
- We assess that other, non-Muslim terrorist groups probably will conduct attacks over the next three years given their violent histories, but we assess this violence is likely to be on a small scale.
- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect

with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

The analytic effort that culminated in this NIE was strengthened by many of the intelligence reforms realized since September 11.

Intelligence Reforms Since 9/11

I turn now to the transformation we have undertaken in the IC to meet the challenges of today and the threats of tomorrow.

The Intelligence Community has made significant strides in addressing the underlying deficiencies exposed by the attacks of 9/11. This morning, I would like to first highlight a few of the flaws in America's intelligence system that existed before 9/11; second, detail the steps we have taken thus far to build a stronger Community; and, finally, turn our gaze to initiatives that will further these reforms.

Generally speaking, before 9/11 America's Intelligence Community was structured to win the Cold War—a traditional struggle between two great powers. The Community was downsized during the 1990s and while it consisted of over a dozen agencies with unique mandates and competencies, we lacked a national-level intelligence apparatus to manage effectively the Community and synthesize information from across the government to support a host of customers—policymakers, warfighters, and law enforcement officials—with various, and often competing, requirements. This construct led often to the “stovepiping” of information within agencies that guarded their cultures and their secrets. Data was provided on a “need to know” basis. “Information sharing” was considered more an exposure to foreign espionage than a path to a smarter intelligence enterprise. Accordingly, analysts in one agency were not encouraged to work with analysts in others. There were few processes in place to collaborate, share lessons learned and best practices, and manage the Community as an enterprise.

In the past, policy barriers also prevented the government from attracting young people of promise with the skills and backgrounds needed to strengthen our national defense. Too often, agencies became so focused on protecting sources and methods that they made it nearly impossible for first- and second-generation Americans to serve the intelligence enterprise. This was a serious deficiency that denied the country the efforts of those with the language fluencies, political,

scientific, and technical skills, and cultural insights that we need to bolster our workforce and improve our intelligence.

Structurally, the Community was also largely divided between domestic and foreign intelligence.

The end of the Cold War and the advance of globalization enabled the acceleration of threats stemming from international terrorism, weapons of mass destruction (WMD) proliferation, failed states, and illegal drug trafficking. These threats, among others, move at increasing speeds due to technology and across geographic and organizational boundaries, blurring the distinction between foreign and domestic, and between strategic and tactical events. As we witnessed on 9/11, radical extremist movements continue to use global terrorism to further their causes by attacking innocent people without regard to national boundaries and state and non-state actors continue to demonstrate their intent to acquire WMD through illicit means.

To confront today's threats, we have made many changes in the way we conduct intelligence, law enforcement, homeland security, diplomatic, and defense activities. Implementing the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) along with the recommendations from various in-depth studies—such as the 9/11 Commission Report, the WMD Commission Report, internal Executive Branch reviews and reports by both houses of Congress—the Community received direction and the mandate and many of the tools needed to build an effective, results-oriented enterprise. The Intelligence Reform Act provided a mechanism for overhauling the IC by providing a new office, the Office of the Director of National Intelligence (ODNI), with the tools and mandate to unify and direct the efforts of our 16 intelligence agencies.

With these new mechanisms, we are working to forge an integrated Intelligence Community that spans the historical divide between foreign and domestic intelligence efforts. Far from being a buzz word, integration means ensuring that our various specialized intelligence missions operate as a single enterprise. An integrated and collaborative Community is a critical advance because no single agency has the capacity to evaluate all available information—lest we forget that over one billion pieces of data are collected by America's intelligence agencies everyday.

While we recognize that much more must be accomplished, the professionals of the Intelligence Community take pride in the notable progress we

have made over the past six years. I would like to describe our accomplishments thus far in four main areas: our efforts to **structure** the Intelligence Community to meet 21st century challenges; **improve** analysis through cross-agency integration and technical initiatives; develop a **collaborative** Community that provides the right information to the right people at the right time; and **build** a dynamic intelligence enterprise that promotes diversity to gain and sustain a competitive advantage against our adversaries.

Structuring the IC

The principal legacy of the IRTPA was the establishment of the office of the Director of National Intelligence with assigned responsibilities to serve as the chief intelligence advisor to the President and National and Homeland Security Councils and to head the IC to ensure closer coordination and integration. The DNI is afforded responsibility to determine the National Intelligence Program and significant authority over personnel policy. In a larger sense, the creation of the DNI allows one person to see across the wide American Intelligence Community, identify gaps, and promote a strategic, unified vision.

I will leave to my colleagues with me here today the discussion of the specifics of their efforts, but I would like to highlight the key structural changes, in addition to the establishment of the ODNI, that have been undertaken since 9/11.

Working closely with the Department of Justice and the FBI, we supported the creation of the FBI's National Security Branch to integrate the FBI's counterterrorism, counterintelligence, WMD, and intelligence programs. We also supported the creation of Field Intelligence Groups in every FBI field office—a major step in the FBI's effort to transform itself into a preeminent domestic counterterrorism agency. Furthermore, the Executive Assistant Director of the National Security Branch now works closely with me and my leadership team, ensuring close coordination on addressing the FBI's intelligence mission.

We established the National Counterterrorism Center (NCTC), the government's hub for all strategic level counterterrorism intelligence assessments, which draws on collected terrorist intelligence from agencies across the U.S. Government with access to more than 30 different networks carrying more than 80 unique data sources to produce integrated analysis on terrorist plots against U.S. interests at home and abroad. This kind of fusion is conducted nowhere else in government—and it was only an aspiration prior to 9/11.

The results are tangible. NCTC produces a daily threat matrix and situation reports that are the Community standard for current intelligence awareness. In addition, NCTC hosts three video teleconferences daily to discuss the threat matrix and situation reports to ensure the intelligence agencies and organizations see all urgent counterterrorism information.

We also established the National Counterproliferation Center (NCPC), the mission manager for counterproliferation, which has developed integrated and creative strategies against some of the nation's highest priority targets, including "gap attacks" (focused strategies against longstanding intelligence gaps), "over the horizon" studies to address potential future counterproliferation threats, and specialized projects on priority issues such as the Counterterrorism-Counterproliferation Nexus.

ODNI Mission Managers for high-priority topics, such as North Korea, Iran, counterintelligence, and Cuba and Venezuela, have also made considerable progress by identifying intelligence priorities, gaps, and requirements and engaging in strategic planning and collection management in the larger context of other intelligence collection and analytical priorities.

In the last few months, we also established an Executive Committee (EXCOM) to advise the DNI in the discharge of his responsibility for the coordination of all intelligence activities that constitute the domestic and foreign intelligence efforts of the country. This EXCOM is composed of the heads of all major intelligence producers and consumers and provides a biweekly forum for the key stakeholders to gather and provide common guidance on the development, implementation, and evaluation of activities of the IC.

Within the past six months, we also named a Deputy Director of National Intelligence (DDNI) for Acquisition to enhance the efficiency and effectiveness of our acquisitions. The DDNI for Acquisition has drafted a strategy to improve the acquisition process and recommended modifications to acquisition authorities. We are also in the process of standing up the Intelligence Advanced Research Projects Activity to create synergy and innovation across the IC by harnessing technology in new ways to create strategic advantage.

These three initiatives were highlighted by the Intelligence Community's 100 Day Plan for Integration and Collaboration, which we launched in April and concluded in August. The 100 Day Plan identified 24 specific initiatives and tasks to be accomplished on a rigorous timeline; of those 24, 17 tasks were achieved in

that timeframe and the remaining tasks are scheduled to be met in the coming weeks. The Plan was designed to build on the successes so far—many of which I will discuss here—and to jumpstart further efforts. Initiatives were aligned to six integration and transformation focus areas:

1. Create a Culture of Collaboration
2. Foster Collection and Analytic Transformation
3. Build Acquisition Excellence and Technology Leadership
4. Modernize Business Practices
5. Accelerate Information Sharing
6. Clarify and Align DNI's Authorities.

I have discussed the specifics of this Plan in other forums and will not detail it today, although I note that the focus on accountability and achieving identified targets has given a renewed emphasis to transforming the Community and executing these reform initiatives. I will speak again of our planning process at the conclusion of my testimony.

Improving Analysis

Cross-Agency Integration

Two of the main goals of intelligence reform are to build a sense of community among foreign, military, and domestic intelligence agencies and, through that kind of collaboration, improve the quality of analysis. For greater collaboration to occur, however, analysts must be able to identify and contact peers and counterparts working on related topics.

Prior to the creation of the ODNI, analysts had no easy way to obtain contact information on analysts from other agencies. Today, they have the Analysts Yellow Pages. Launched in February 2006, the Analysts Yellow Pages is a classified, web-based phonebook and a single stop for obtaining contact information on analysts in all IC agencies. It is accessible on the Joint World-wide Intelligence Communications System and allows users to search for analysts across the Intelligence Community by name, by intelligence topic, country, or non-state actor, or by agency. Search results provide contact information including name, agency, phone number, and email address. Our ODNI Chief Information Officer (CIO) is developing a common method to identify, in perpetuity, all the individuals across the IC.

The Information Sharing Environment

Created by IRTPA, the Program Manager for the Information Sharing Environment (PM-ISE), operating in coordination with the interagency under guidelines issued by the President and statutory authority—a well as with strong support from this Committee—has led the charge with our state, local, tribal, private sector, and foreign partners to transform government-wide terrorism-related information sharing policies, processes, procedures, and most important ,workplace cultures, to normalize the sharing of terrorism-related information as part of how we do business.

Section 1016 of the IRTPA and as amended by the 9/11 Commission Act of 2007, established the Office of the Program Manager and provided it with government-wide authority to plan, oversee and manage the ISE. The ISE is a trusted partnership among all levels of government that facilitates the sharing of information relating to terrorism. Creating the ISE is not about building a massive new information system; it is policies, processes/protocols and technology that enable the sharing of this information among Federal, State, local, tribal, private sector entities and our foreign partners.

To guide efforts to establish the ISE and implement the requirements of Section 1016 of IRTPA, on December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment*. In this Memorandum the President prioritized efforts that he believes are most critical to the development of the ISE and assigned to relevant Cabinet officials the responsibility for resolving some of the more complicated issues associated with information sharing.

The PM-ISE in consultation with the Information Sharing Council, State, local, and tribal governments, and private sector partners have made significant progress against the President's priorities in the following areas:

- Development of proposed Common Terrorism Information Sharing Standards (CTISS). The CTISS program develops and issues functional standards that document the rules, conditions, guidelines, and characteristics of business processes, production methods, and products supporting terrorism-related information sharing. (Presidential Guideline 1)

- Establishment of a Federally-sponsored interagency capability in the NCTC to enable the production and dissemination of Federally-coordinated terrorism-related information to state, local, and tribal authorities and the private sector. (Presidential Guideline 2)
- Establishment of a national, integrated network of State and major urban area fusion centers that optimizes our capacity to better support the information needs of State and local authorities, as well as efforts to gather, analyze, and share locally generated information in a manner that protects the information privacy and legal rights of Americans. (Presidential Guideline 2)
- Development of the *Presidential Guideline 3 Report: Standardize Procedures for Sensitive but Unclassified (SBU) Information*. The Report will recommend to the President a new Controlled Unclassified Information (CUI) Framework for rationalizing, standardizing, and simplifying procedures for SBU information in the ISE. (Presidential Guideline 3)
- A repository of information on over 400 unclassified and SBU international information sharing agreements with foreign governments. (Presidential Guideline 4)
- PM-ISE publication of ISE Privacy Guidelines, including development of an implementation guide for Federal agencies. (Presidential Guideline 5)

Although the effort to implement the ISE is well underway, it is essential that implementation activities take place within a broader strategic context of enhancing our Nation's ability to combat terrorism. The ultimate goal is not simply information sharing for the sake of sharing information. The objective is to improve our national capacity to protect the nation from future attack.

Information Sharing Initiatives within the IC

Initiatives in support of information sharing specifically within the IC include the efforts of the CIO and the ODNI Analysis directorate, to profoundly change how IC components collaborate with each other. We have integrated Internet technologies into the Intelligence Community's secure and unclassified Intranets, giving individuals the ability to collaborate as groups, peer-to-peer, and in self-identified teams. We are also developing virtual communities of analysts who can securely exchange ideas and expertise across organizational boundaries. Through our pilot Library of National Intelligence initiative, we are providing analysts across the Community a searchable database of disseminated Intelligence products. In a later phase, even if a particular user does not have the clearances to

review a desired document, he or she will (in most cases) be advised of the product's existence and offered the opportunity to request access to it.

And analysts are also increasingly using interactive, classified blogs and wikis, much as the tech-savvy, collaboration-minded user would outside the Community. Intellipedia, the IC's version of Wikipedia, and "A-Space" a common workspace environment likened in the press to the commercial website "MySpace," are perhaps the best-known examples. Such tools enable experts from different disciplines to pool their knowledge, form virtual teams, and quickly make complete intelligence assessments.

Efforts to improve collaboration do not stop at the water's edge—literally. Under CIO auspices, we have created the capability for US persons to communicate via email with their Allied counterparts overseas. The solution does not require special networks or equipment but has dramatically changed our capability to share information in a timely manner. The Allied Collaborative Shared Services program and email projects have improved how the US Intelligence Community shares intelligence with our partners.

The underlying principle here is a simple one: no one has a monopoly on truth.

Much the same principle animates our engagement with outside professionals who can challenge our analytic assumptions, provide deep knowledge, insights, and new ways of thinking. Through the Analytic Outreach Initiative, ODNI is expanding networking opportunities for IC analysts and encouraging them to tap expertise on key issues wherever it resides through conferences, seminars, workshops, and exchanges. These outside experts—whether academics, business people, journalists, technical experts, or retired intelligence officers—contribute to proof and validation exercises and to lessons learned processes. They also provide a critical surge capability, especially in areas where IC resources are slim.

We have also taken steps to safeguard the impartiality of our analytic products. As mandated by the IRTPA, the ODNI established an Assistant Deputy for Analytic Integrity and Standards, who serves as the focal point for analysts who wish to raise concerns regarding politicization, bias, or the lack of objectivity, appropriate alternative analysis, or dissenting views in intelligence products. The Office of Analytic Integrity and Standards challenges the IC to evaluate its work and enforce standard that will produce the best possible analytic product for our

customers. The AIS is also promoting the use of diverse analytic methodologies. For example, AIS has developed an Introductory Analysis course for new IC analysts, who will receive instruction in critical skills, establish contacts in other agencies, and gain better appreciation of the diversity within the IC.

Many of these improvements would be of little use if they did not reach our customers, including the policymakers of this Committee. Specifically, you may have noticed the qualitative improvements to our National Intelligence Estimates, the IC's most authoritative written judgment on a particular subject. Specifically, NIE Key Judgments no longer contain a list of conclusions but are written to explore more thoroughly the implications of our critical underlying conclusions. Appendices and annexes now provide full transparency of their analytic judgments through the careful identification of sources and intelligence gaps, and by "showing our homework"—essentially, describing the analytic train of reasoning we use to arrive at our conclusions. The main text now highlights the full range of analytic judgments and their implications, bringing dissenting opinions to the fore so policymakers have the benefit of the full picture. We applied many of these lessons learned to the NIE on Homeland Security Threats that I discussed earlier.

Developing a Collaborative Community with a Responsibility to Provide

In the years since 9/11, multiple studies have attributed our inability to prevent the terrorist attacks to the inability or unwillingness of government organizations to share critical information and intelligence fully and effectively. Our success in preventing future attacks depends upon our ability to gather, analyze, and share information and intelligence regarding those who would do us more harm. The intelligence and information sharing structures that enabled the winning of the Cold War need greater flexibility and resilience to confront today's threats from transnational terrorists. Most important, the long-standing policy of only allowing officials access to intelligence on a "need to know" basis should be abandoned for a mindset guided by a "responsibility to provide" intelligence to policymakers, warfighters, and analysts, while still ensuring the protection of sources and methods.

In short, those responsible for combating terrorism must have access to timely and accurate information regarding our adversaries. We must:

- Identify rapidly both immediate and long-term threats;
- Identify persons involved in terrorism-related activities; and

- Implement information-driven and risk-based detection, prevention, deterrence, attribution, response, protection, and emergency management efforts.

Accomplishments Thus Far

In the aftermath of 9/11, our Nation began the historic transformation aimed at preventing future attacks and improving our ability to protect and defend our people and institutions at home and abroad. As a result, we are now better informed of terrorist intentions and plans and better prepared to detect, prevent, and respond to their actions. Improved intelligence collection and analysis has helped paint a more complete picture of the threat, and more robust information sharing has provided us a greater capacity for coordinated and integrated action. Several information sharing successes since 9/11 include the following:

- The enactment of the “USA PATRIOT Act” helped remove barriers that once restricted the effective sharing of information and coordination between the law enforcement and intelligence communities.
- The establishment of the Department of Homeland Security (DHS) and DHS’s Office of Intelligence and Analysis has enhanced the sharing of information between federal, state, and local government agencies, and the private sector which in turn has enhanced our ability to detect, identify, understand, and assess terrorist threats both to and vulnerabilities of the homeland to better protect our Nation’s critical infrastructure, integrate our emergency response networks, and link state and federal governments. The Chief Intelligence Officer of DHS is now responsible for integrating the intelligence activities of that Department, providing overall guidance on homeland security-specific issues.
- The Terrorist Screening Center was created to consolidate terrorist watch lists and provide around the clock operational support for federal and other government law enforcement personnel across the country.
- The growth and maturation of the 101 Joint Terrorism Task Forces (JTTF) in major jurisdictions throughout the United States, with support from Field Intelligence Groups (FIGs), has substantially contributed to improved terrorism-related information sharing and operational capabilities at the state and municipal levels.

Through these and other efforts, the United States and its coalition partners have made significant strides against al-Qa’ida, its affiliates, and others who threaten us. Collaboration and information sharing have helped limit the ability of al-Qa’ida and like-minded terrorist groups to operate. We have uncovered and eliminated

numerous threats to our citizens and to our friends and allies. We have disrupted terrorist plots, arrested operatives, captured or killed senior leaders, and strengthened the capacity of the Nation to confront and defeat our adversaries.

Building a Dynamic Intelligence Enterprise

Joint Duty

Building a collaborative intelligence enterprise goes beyond merely sharing information. It also means fostering a new, Intelligence Community-wide culture without destroying the unique perspectives and capabilities of each agency. In this effort, the IC has a useful model in the Defense Department, which was revolutionized by the Goldwater-Nichols Act of 1986. That Act unified the military establishment and laid the foundations for a “joint” military by establishing incentives for interservice collaboration (such as requiring a joint duty assignment to achieve flag rank) and promoting joint training and development).

Recently, we took a dramatic step toward realizing a similar bedrock shift within the Intelligence Community. Through the authorities granted to the DNI by the IRTPA, I signed a directive mandating civilian joint duty for intelligence officers across the IC. This was a key accomplishment of our 100 Day Plan. Now, if an up-and-coming officer aspires to the senior-ranks of the Community, he or she will have to serve a tour of duty at a different agency during his or her career. The experience provides the officer with a broader perspective and brings the Community a long way toward the collaborative and unified ideal.

Recruitment Initiatives

Since the establishment of the ODNI, we have been working vigorously to recruit intelligence officers with the backgrounds and skills that will strengthen our security.

The Intelligence Community’s 100 Day Plan for Integration and Collaboration highlighted the need to recruit and retain first- and second-generation Americans with diverse background, critical language skills, and a nuanced understanding of foreign cultures to strengthen the nation’s security. In accordance with initiatives specified in this Plan, the ODNI hosted an inaugural IC Heritage Summit and the first IC Leadership Colloquium in June 2007, beginning a dialogue with national and regional Heritage Community organizations and internal IC affinity groups and special emphasis program leaders. The results from these two events, and the

feedback from the external and internal groups, were the foundation for developing the first IC Heritage Community Recruitment, Hiring, and Retention Strategy for first- and second-generation Americans. These groups, as well as our legacy communities, provide a rich pool of diverse talent that has not been consistently tapped into as a source to enable the IC to more accurately reflect the “face” of the American people.

In addition, we have established a formal Intelligence Community Recruiting Subcommittee, consisting of IC Agency Recruitment organizations, that meets regularly to discuss common issues, share best-practices and recruiting successes, plan annual IC collaborative recruiting events, network with leading external recruiting companies and consultants, and recommend solutions to individual IC Agency challenges.

We also developed a centrally funded IC corporate recruiting strategy to recruit collaboratively at national- or high-priority IC target events. Since 2005, the number of events at which we have recruited has more than doubled from 10 to about 25. We pursue a wide-range of applicants by recruiting at a broad array of national career fairs and conferences, including those hosted by: the Society of Hispanic Professional Engineers (SHPE), the National Society of Black Engineers, the American Indian Science and Engineering Society, the Thurgood Marshall Leadership Institute, Women for Hire, and Asian Diversity Career Expos. The IC is also a major sponsor of SHPE and events for the Careers for the Disabled.

Since the enactment of the IRTPA, the IC has established an IC-wide resume database that allows the sharing of resumes from collaborative events and IC Agency referrals and allows recruiters to search for highly-qualified applicants, especially those with desirable backgrounds or language fluencies.

We also established an annual campaign to recruit students from universities deemed Centers for Academic Excellence (CAE). The IC CAE program was established in 2004 to increase the diversity of the IC’s applicant pool for entry-level professional positions. The program provides technical and financial support to a diverse cohort of ten specially-selected American colleges and universities so they can develop and deliver degree programs that prepare their graduates for IC jobs in the sciences, information systems and technology, regional studies, and foreign languages.

These initiatives will require follow-on implementation to recruit and hire personnel with the backgrounds and skills considered essential to improve the

diversity and ability of the IC workforce, but with continued emphasis and support from the Administration and the Congress, I believe we are well positioned to succeed.

Focused Emphasis on Diversity

I would like to make special mention of the strong support we have received from the Congress in our efforts to diversify our workforce. Representative Silvestre Reyes, Chairman of the House Permanent Select Committee on Intelligence (HPSCI), has, in particular, worked closely with us to promote the recruitment of traditionally underrepresented groups. Chairman Reyes and I both addressed the first IC-wide Affinity Group and Special Emphasis Program Leadership Colloquium in June 2007, and the Chairman hosted a panel on diversity and the Intelligence Community last month in El Paso, Texas with Jose A. Rodriguez, the outgoing director of the CIA's National Clandestine Service.

We have also completed the first IC EEO and Diversity Strategy (Five-Year Plan for 2007-2012) as a priority initiative in our 100 Day Plan, responding to the HPSCI mark draft language and addressing a fundamental need to ensure that the IC workplace continues to be characterized by fairness and equality. Without such assurance, we cannot expect to attract and retain a workforce that looks like America and can operate in a global threat environment. Furthermore, our IC hiring and promotion practices must at least equal, and preferably surpass, other government agencies in transparency and equity if the American people are to willingly extend to us the latitude absolutely necessary to protect our nation.

Security Reform

The recruitment and hiring of first- and second-generation Americans brings into sharp relief a weakness that has plagued the Intelligence Community for decades: the onerous security clearance process required to work in the IC. The IRTPA mandated the reformation of security clearance procedures, and it remains one of our top priorities.

As someone who has worked in the private sector and been exposed to the other side of the security clearance process, I can speak from experience of the frustration that often accompanies lengthy and seemingly unnecessary delays in getting individuals cleared for duty.

Accordingly, we identified security clearance reform as a top priority for the 100 Day Plan and established a Tiger Team at the ODNI Special Security Center to lead this crucial reform. We are undertaking this security reform initiative jointly with the Department of Defense. We have designed a transformed clearance process and developed a plan to assess the validity of this process.

The comprehensive reform of the security clearance process remains our ultimate goal in order to deliver high-assurance security clearances, fairly, efficiently, and at the lowest possible cost. The new process will be based upon end-to-end automation, new sources of data, analytical research, and best practices. Some of these pieces already exist in the Community but they need to be integrated into a single process.

Foreign Language Initiatives

To build a strong foundation for the future of the Intelligence Community, we must also increase foreign language capacity among our workforce and support the study of languages among America's youth. To that end, ODNI is sponsoring a major Intelligence Community study of how to optimize foreign language staffing, taking into account language and proficiency requirements, retention, training, and cost, and comparing the roles played by civilian, military, and contractor personnel in performing foreign language tasks. The study is being conducted by the RAND Corporation and initial results are expected in 2008.

The ODNI also purchased a Community license for on-line language training software in 150 languages. All IC personnel will be able to utilize this resource. We are also supporting several research projects to improve the effectiveness of foreign language training, including evaluations of both commercially-developed and government-sponsored on-line language training programs.

Furthermore, ODNI has initiated a new collaborative program, called the Language Education and Resources Network to share best teaching practices and learning materials in critical languages developed in language schools throughout the U.S. government. Major workshops have been held in Chinese and Arabic, with additional workshops planned in Persian, Hindi, Urdu, and Korean within the next year.

We have also sponsored conferences and facilitated information sharing to enhance key capabilities in human language technology, such as machine

translation and content extraction. ODNI is developing a Human Language Technology Roadmap, to guide and prioritize investment across the IC.

To fill critical gaps, ODNI is spearheading an initiative to create temporary hiring billets, to speed up the on-boarding process for applicants with outstanding foreign language skills, including heritage community applicants. Temporary billets could be used to hire personnel who are awaiting clearance and allow them to work in unclassified settings, such as open source research, or to permit placement of personnel who have been cleared, but for whom no permanent billet is immediately available.

Finally, ODNI—in partnership with the National Security Agency—leads STARTALK, a new program in summer language education. A part of a Presidential initiative to improve critical language skills, STARTALK will provide funding for programs in over 20 states and Washington D.C. to educate both students and language teachers. The classes focus on Arabic or Chinese and range from week-long tutorials to nine-week immersions. Through this program, hundreds of young people will receive education that will enrich their lives, enhance their futures, and strengthen our nation's global competitiveness—yielding substantial returns for an initial investment of only five million dollars.

Looking to the Future

The passage of the IRTPA and the creation of the DNI were important steps toward building an integrated and collaborative Intelligence Community that is well positioned to defend the nation—but they must be part of a larger reform effort.

To support the IC vision of integration and collaboration we initiated a deliberate planning process based on the principles of transparency, accountability, deadlines, and deliverables. The first phase of these efforts—the recently completed 100 Day Plan—was designed to jump-start the process and build momentum. The next phase—the 500 Day Plan—is intended to sustain and accelerate that energy with an expanded set of initiatives and a greater level of participation. This latter plan was developed through a Community-wide effort beginning last May through the use of working groups, blogs, and wikis to solicit input from the Community. During our coordination process, we identified several core priorities and over 30 supporting initiatives. The core initiatives represent major long term impact projects that will be monitored and reported on a biweekly

basis to my office and reviewed by the EXCOM monthly; they represent “major muscle movements”—something required for this transformational effort.

The 500 Day Plan will be executed through cross-organizational and Community-wide engagement and collaboration. Working groups for each initiative will include key stakeholders from throughout the Community. It is through implementation of these initiatives that the IC will continue to increase its efficiency and effectiveness and further meet the national security challenges of the 21st century.

Protect America Act of 2007

Finally, I would like to make note of an issue on which I hope the Congress takes action in the coming months. The recent enactment of the Protect America Act of 2007 provided a necessary update to the Foreign Intelligence Surveillance Act (FISA). This critical legislation has already assisted the IC in closing a critical gap in the IC’s ability to provide warning of threats to the country. This Act sunsets in less than six months, and I believe that making its changes permanent will be an important step toward ensuring the protection of our Nation. Importantly, the Act provides for meaningful oversight of activities. The Department of Justice’s National Security Division, IC general counsel offices, and the ODNI Civil Liberties and Privacy Office, in addition to existing oversight mechanisms within the IC, will all be involved in overseeing implementation of the Act’s authorities.

I am committed to keeping the Congress fully and currently informed of how this Act has improved the ability of the Intelligence Community to protect the country and look forward to working with the Congress to obtain lasting FISA modernization.

Conclusion

In closing, we have come a long way over the past six years developing a more integrated, more collaborative intelligence enterprise, and I believe the result has been a stronger Community better positioned to know the world and anticipate surprise. While we have seen success in our efforts to **structure** the Intelligence Community to meet 21st century challenges; **improve** analysis; develop a **collaborative** Community that provides the right information to the right people at the right time; and **build** a dynamic intelligence enterprise that promotes diversity

to gain and sustain a competitive advantage against our adversaries, our work is far from done.

With your support, I look forward to building a legacy of reform that will outlast our own time and provide for the protection of the Republic in the decades to come.

Mr. Chairman, this concludes my remarks. I welcome any questions you may have. Thank you.

**Confronting the Terrorist Threat to the Homeland:
Six Years after 9/11**

**to the Senate Committee on Homeland Security and
Governmental Affairs**

10 September 2007



Honorable John Scott Redd

Vice Admiral, U. S. Navy (Ret.)

Director

National Counterterrorism Center

**Statement for the Record
by
The Honorable John Scott Redd
Director, National Counterterrorism Center (NCTC)
to the United States Senate Committee on Homeland Security and
Governmental Affairs
September 10, 2007**

Chairman Lieberman, Ranking Member Collins, distinguished members of the Committee, thank you for the opportunity to testify before you today on our nation's efforts to confront the terrorist threat to the homeland since 9/11.

Since 9/11, sweeping legislative and organizational changes—many of which are attributable to this committee—have fundamentally altered how we protect and defend U.S. interests at home and abroad against terrorism. In particular, the U.S. Government has made substantial progress in building our counterterrorism (CT) capability, developing a strategy based on a detailed understanding of al-Qa'ida and the global movement of violent extremists, and reorganizing the government to remedy the shortfalls revealed by the 9/11 attacks. I will discuss some of these developments with you today.

None of what I will say should be understood to mean that we do not continue to face real and significant challenges. We must continue to improve our intelligence collection on the hardest targets. We must continue to mature our coordination with state and local officials so that the federal government supports their efforts and benefits from their many capabilities. We must better coordinate departmental efforts to counter radicalization both at home and abroad. And we must ensure that departmental planning and budgeting is done in a manner consistent with a U.S. Government-wide effort to counter the terrorist threat we face now and are likely to face in the future.

I would like to briefly review the role NCTC is playing, and will play, to further sustain this progress through enhancing the U.S. Government's capability to detect, disrupt, and deter the threat of terrorism against U.S. interests both at home and abroad.

Today, as directed by the Intelligence Reform and Terrorism Prevention Act (IRTPA), NCTC performs two significant functions in the War on Terror. The first, Intelligence, is a familiar one and one in which I report to the DNI. The second is Strategic Operational Planning. As you are well aware, in this second role I report to the President and am responsible for producing the U.S. Government's overall War Plan for the War on Terror (WOT).

In both roles, NCTC's work is truly an interagency effort. We are part of the ODNI and benefit from his authorities. Our staff includes some 400 U.S. Government employees, the vast majority of whom are on rotation from one of 16 federal departments and agencies, including CIA, DoD, and FBI. This rotational structure is deliberate and embodies the model of "Joint Duty" that has proven so successful within the Department of Defense. By bringing so many departments and agencies together at NCTC, we are able to capitalize on the diverse talents and perspectives that only a truly joint workforce can provide.

I would now like to highlight just a few of the areas in which we've seen improvement over the last few years. I'll speak first to the changes in intelligence and then to those related to strategic operational planning.

In the intelligence area, we have made significant progress translating into action the lessons learned from 9/11 and WMD Commissions. An effective intelligence enterprise requires analysis, information sharing, and interagency collaboration, and NCTC continues to lead the counterterrorism community in all three areas.

Analysis. Analysis is at the heart of the counterterrorism intelligence process, and therefore also at the center of NCTC's mission. Our officers involved in the analytical process understand that their insights and judgments may figure directly in the defense of our nation and our allies. Analysis literally *counters terrorism*: it surveys the battlefield, identifies enemy forces and their intentions, and lays the groundwork for an effective offense and defense that use every instrument of national power—from military force to public diplomacy, and everything in between.

NCTC's analytic mission, as defined by IRTPA, is a broad one. As the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism, with the exception of purely domestic terrorism, our mandate crosses the foreign and domestic divide, and requires us to support the full spectrum of intelligence customers. Central to performing this critical responsibility is providing all of our analysts with intelligence from throughout the U.S. Government. This is, as you know well, a revolutionary concept within the Intelligence Community. But today that concept is reality at NCTC; analysts can and do see sensitive intelligence from the CIA, FBI, Department of Defense, Department of Homeland Security, and other organizations.

This base of knowledge enables us to provide our customers with all-source, integrated analysis. NCTC, in collaboration with a wide array of government partners, generates a spectrum of integrated, analytic products – tailored to the needs and interests of our customers, including the President, Departments and Agencies, and the Congress. Our products range from immediate reports providing situational awareness about largely unevaluated intelligence—for example a daily Threat Matrix and twice daily Situation Reports—to in-depth finished intelligence such as the National Terrorism Bulletin and the President's Daily Brief. Significantly, virtually all of these reports for senior policy makers are coordinated by NCTC, as the DNI's Mission Manager. The purpose of that is to ensure that differing views are not only represented, but that they are also put in context.

NCTC's analytic efforts are not just focused on today's most pressing issue. While we spend significant time analyzing current threat streams to ensure that policy makers are kept fully informed, we also analyze longer-term trends in homegrown terrorism, radicalization, terrorists' use of the Internet, and future terrorists' tactics and weapons. In short, we seek to inform on the full range of terrorism topics.

One of the ways in which we ensure policymakers are informed by the best intelligence possible is to provide Intelligence Community-wide coordinated analysis that includes different agencies' views when such differences exist. The Interagency Intelligence Committee on Terrorism (IICT) serves as our primary forum to do this. Although the IICT

existed before 9/11, it has expanded and improved its activities since that time. The chairmanship has also been elevated so it rests with the Director of NCTC. We take very seriously our responsibility to ensure that IICT products fully and faithfully represent dissenting views—should they exist—among agencies.

Finally, NCTC—in conjunction with the DNI—has over the past year sought to best leverage the Intelligence Community’s finite analytic resources for counterterrorism. One important corollary to this is to avoid having every agency cover the same issues. To that end, we have identified agency-specific missions, designated lead responsibility for subject areas, and ensured appropriate competitive analysis so that the Intelligence Community is not single-threaded on important issues. This alignment, called the *Analytic Framework for Counterterrorism*, is a tangible recognition that not every agency can cover every topic all the time—and that to try to do so would not serve the U.S. Government well.

The Analytic Framework is focused on four counterterrorism mission areas:

- **Tactical Offense:** Analysis supporting direct action against the terrorist enemy – led by department and agency analytic elements.
- **Tactical Defense:** Analytic warnings of planned terrorist attacks and operations – led by NCTC, and Defense Intelligence Agency (DIA) in the case of threats to U.S. military targets.
- **Strategic Offense:** Analysis to guide national policy and policymakers in countering violent extremism and radical ideology as a threat to our way of life – led by NCTC.
- **Strategic Defense:** Analysis supportive of efforts to reduce our vulnerability to terrorist attacks and future terrorist capabilities – led by NCTC for strategic warnings, and relevant departments and agencies for vulnerability assessments.

One immediate impact of the Framework's adoption has been the shift of some CIA resources to NCTC so that the former can focus on operational support and the latter can concentrate on strategic analysis, such as the "War of Ideas."

Information Sharing. Let me now turn to the second critical piece of our intelligence enterprise—information sharing. NCTC is committed to sharing information quickly, effectively, and consistently.

Under the IRTPA, NCTC has the responsibility "to ensure that agencies, as appropriate, have access to and receive all-source intelligence products needed to execute their counterterrorism plans or perform independent, alternative analysis," and "to ensure that such agencies receive intelligence needed to accomplish their assigned activities." Today I'll highlight four of our principal efforts: sharing intelligence within the federal government, sharing intelligence with state, local, and tribal governments; bringing together departments and agencies to discuss current threats; and, comprehensive watchlisting of individuals of concern.

At the core of our mission is ensuring that all our federal partners have the intelligence they need. Prior to 9/11 there was no comprehensive place to go if an analyst or operator wanted to find all disseminated terrorism intelligence available to the U.S. Government. Today, NCTC Online (NOL) allows more than 60 U.S. Government elements to share information electronically. It serves as a key classified repository and collaboration tool, reaching intelligence, law enforcement, defense, homeland security, foreign affairs and other federal organizations with a counterterrorism mission. It now hosts more than 8,000 authorized users and holds over seven million terrorism documents.

NOL is also available at different levels of classification. This means that even if users are not permitted to see everything, they can automatically see those materials that fit their security clearances. And this capability is particularly important in helping us with the next information sharing initiative—sharing with state, local, and tribal officials.

NCTC's information sharing responsibilities go beyond that of the Federal Government. IRTPA states that the Director of NCTC is responsible for "supporting the Department of Justice and the Department of Homeland Security, and other appropriate agencies, in fulfillment of their responsibilities to disseminate terrorism information to State and local governments." More recently, with the recent passage of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, NCTC has been given additional responsibilities to tailor CT-related information and products for timely passage to state, local, and tribal governments.

As initially proposed as part of the President's ISE Guideline implementation and later directed by the legislation, we are working with FBI, DHS, the Program Manager for the Information Sharing Environment and state and local officials to establish, within NCTC, the Interagency Threat Assessment and Coordination Group (ITACG). Led by a DHS detailee, with a deputy from FBI, this group will provide additional counsel and subject matter expertise to the federal Intelligence Community and facilitate the sharing of intelligence products tailored to the needs of state, local and tribal entities. It will further strengthen the overall national counterterrorism and homeland security effort.

Our information sharing responsibilities also require us to facilitate robust interagency communication about ongoing operations and events. NCTC chairs regular video teleconferences to maintain U.S. Government-wide situational awareness. Intelligence, law enforcement, homeland security, military, and diplomatic officials from roughly 17 U.S. Government organizations come together three times a day, seven days a week, 365 days a year, to exchange information and collaborate on response options. This is a fundamental change: Before 9/11, there was no routine mechanism to maintain situational awareness across the U.S. Government.

Finally, NCTC also plays a pivotal role in the terrorist watchlisting process. For the past four-plus years, NCTC has served as the U.S. Government's central repository for information on international terrorist identities, known as the "Terrorist Identities Datamart Environment," or TIDE for short. The TIDE database includes, to the extent permitted by law, all information the U.S. Government possesses on the identities of individuals known

or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to international terrorism.

The establishment of TIDE marked a major milestone in the nation's CT effort, compiling into one database information on all known and suspected international terrorists. Before 9/11, watchlisting efforts were spread across multiple databases managed by multiple agencies, a significant vulnerability in the nation's efforts to defend against terrorist attack.

Each day, TIDE sends the FBI's Terrorist Screening Center (TSC) a sensitive but unclassified subset of terrorist identifiers to populate the U.S. Government's consolidated watchlist. This consolidated watchlist, in turn, supports efforts to screen, detect, and interdict the travel of known and suspected terrorists here and overseas. These screening efforts encompass the work of consular officers at embassies, Customs and Border Protection (CBP) personnel, law enforcement organizations across the United States, and foreign and domestic air carriers that fly to the United States. So today, an applicant for a State Department visa is checked against the watchlist at a consulate overseas. At U.S. ports of entry, a border crosser's passport, visa, or driver's license is also checked against the CBP's subset of the consolidated watchlist. And at a routine traffic encounter inside the United States, a suspect's identity is checked against the Terrorist Screening Database (TSDB) through the National Crime Information Center. Finally, airline screening personnel review passenger lists for all flights traveling to the United States to identify individuals who are believed to be a threat to civil aviation or the homeland or who should have additional screening prior to boarding a plane.

Examples of the types of activity that warrant an individual's entry into TIDE and terrorist screening systems include:

- Commission of an international terrorist activity;
- Preparation for or planning of international terrorist activity;
- Collection of information on potential targets for international terrorist activity;
- Collection or solicitation of funds or other items of value on behalf of international terrorist organizations or activity;

- Recruitment of members into international terrorist organizations;
- Provision of material support (e.g., safe houses, transportation, communications, funds, false documentation, weapons, or training) to international terrorist organizations; and,
- Membership in or representation of an international terrorist organization.

While the number of names contained in TIDE has grown since its inception in 2003 from approximately 100,000 to over 500,000, this figure represents every identity associated with individuals entered in the database. This distinction is significant because of the multiple aliases and name variants of terrorism suspects. As a result, the number of actual individuals recorded in TIDE is closer to 400,000. And although TIDE continues to grow, individuals' names are also regularly removed when it is determined that they no longer meet the criteria for inclusion. As a result, more than 10,000 names were removed from TIDE in 2006.

Interagency Collaboration. You will note that NCTC's analytic and information sharing efforts are but a part of the larger CT intelligence effort. Let me now turn, then, to the third piece of NCTC's support for CT intelligence—its coordination of the larger counterterrorism intelligence community. As the DNI's "Mission Manager" for counterterrorism, I am responsible for ensuring that all parts of Intelligence Community work toward a coherent, cohesive counterterrorism vision. Let me give you some of examples of IC-wide efforts that NCTC is leading.

First, NCTC orchestrates the counterterrorism National Collection Plan, which identifies information needs and requirements, assesses collector capabilities, and feeds CT requirements into the collection mechanisms. Second, NCTC has conducted the first-ever comprehensive CT analytic workforce analysis. In March of this year, we published *The Counterterrorism Analytic Posture of the Intelligence Community: A Baseline Report*, which gives us a foundation for evaluating the Community of today and developing recommendations for how to position the Community of tomorrow. The results are now being used to implement improved training and retention plans for the Intelligence

Community. We have also developed a systematic "lessons learned" process to capture best practices to improve the efficacy and efficiency of our efforts. We believe that by creating mechanisms to conduct lessons learned studies the CT Community has, over the past year, taken significant steps towards fostering a culture of learning

Thus far I have addressed NCTC's intelligence responsibilities; I would like to turn now to our second role—Strategic Operational Planning (SOP) for the War on Terror.

SOP involves a wide spectrum of planning functions. It bridges the gap between coordinated interagency policy and strategy and tactical operations by departments and agencies to implement that strategy. Essentially, SOP takes interagency planning to a new and much more granular level than we have historically undertaken as a government.

In this role we lead an interagency planning effort that brings all elements of national power to bear in the War on Terror. That includes the full weight of our diplomatic, financial, military, intelligence, homeland security and law enforcement activities. The strategic operational planning effort is new to the U.S. Government. It involves a three-part continuous process: planning, implementation and assessment. NCTC is leading an interagency effort to build processes for all three phases. We've completed the first phase of planning by the CT community, and we're now in the process of guiding the implementation of the plan and assessing its effectiveness.

NCTC's planning efforts span a spectrum from strategic, deliberate planning to more dynamic planning.

The National Implementation Plan (NIP), which was approved by the President in June 2006, is the keystone document for our strategic—or deliberate—planning. The NIP is truly an unprecedented effort to bring together disparate parts of the U.S. Government that have a role in countering terrorism. Building on the President's unclassified National Strategy for Countering Terrorism (NSCT), it incorporates five years of planning, analysis, operations, and successes in the War on Terror. Each of the strategic objectives is further

divided into specific tasks assigned to a Cabinet-level officer for action and other Cabinet officers for support.

The primary value added of the NIP is that it provides a comprehensive, coordinated plan of action that clearly assigns responsibility, sets priorities, illuminates areas of coordination, and provides a framework for assessing success and, ultimately, assigning resources.

In the spectrum of plans, the NIP is overarching and strategic, both in the scope of tasks it contains and the planning process that it initiates for the U.S. Government. Other interagency strategic operational plans have a more focused functional or regional scope—such as the National Strategy to Combat Terrorist Travel—but follow the same process of planning, implementing, assessing, and adjusting.

At the more tactical end of the planning process are dynamic planning efforts, including those established to address emerging threat streams—for example what we have assessed to be the current heightened strategic threat window. For this reason, the White House directed NCTC to establish and lead an Interagency Task Force (ITF) to develop additional options and measures to increase intelligence collection and disrupt potential al-Qa'ida planning. Although led by NCTC, the ITF comprises a core group of representatives from the departments and agencies with the greatest responsibility for implementing new activities in the near term—including the Departments of Defense, State, Homeland Security and Justice.

Each week senior White House and Departmental officials review the actions proposed by the ITF, consider alternative options, and provide further direction on particular activities or measures recommended by the task force. Although I am unable to publicly describe specific actions taken by any single agency or department without undermining their effectiveness, I can report that the ITF has implemented a number of coordinated offensive and defensive measures designed to decrease the likelihood of a successful terrorist attack against the United States and our interests abroad. In addition, the ITF is continuously evaluating intelligence to recommend the most appropriate actions, assess

ongoing operations, and ensure that U.S. Government resources are aligned to most effectively address the threat.

After we have developed a plan to address a specific CT issue or challenge, and taken it through NSC's policy approval process, we move into the implementation phase. NCTC's role in this implementation process is not directive; as clearly delineated in the IRTPA, we do not tell agencies and departments how to do their jobs or when to execute specific actions. Instead, the legislation charges us with the "interagency coordination of operational activities." In practice this means monitoring the key elements of the plan to ensure execution by the relevant departments and agencies. It means working through the obstacles to implementation that inevitably arise. It means identifying the gaps in the plan that are only apparent when execution begins or when the enemy adapts to ongoing activities. Finally, it means highlighting resource issues so that we can match our limited resources to our most urgent CT priorities.

The strategic planning process is less than glamorous. However, as the former Director for Strategic Plans and Policy (DJ-5) for the Joint Staff, I believe it is absolutely critical to the long term success of our government as we prosecute the long war on terror. It is, in short, a revolutionary new way of doing business for the U.S. Government.

Throughout this process, all of our SOP efforts are designed to provide the context and the connective tissue to link the President's CT strategy with the operations and activities on the front lines of the War on Terror.

In closing, I would reiterate that we have come a long way in the last two years as a Center and in the last several years as a Community despite our continued challenges, six years after 9/11, I believe the United States is better prepared to fight this war than at any time in our history. Let me list seven reasons why I believe that.

First, our intelligence is better. Terrorists are clearly a difficult target, but our collection, analysis and production are significantly improved.

Second, we have made major strides in information sharing – in getting that intelligence to the people who need it.

Third, we have taken the fight to the enemy and achieved significant successes in the field. Thousands of terrorists have been taken off the field of battle and dozens of plots have been disrupted.

Fourth, we are attacking every element of the terrorist life cycle, including travel and finance.

Fifth, this is not only an American effort. We are working more closely and more effectively with a greater number of allies around the world to defeat the terrorists.

Sixth, and of special interest to this committee, we have taken significant steps to make the homeland a hostile place for terrorists to enter and operate.

Finally, through a new strategic planning effort, we are laying the groundwork to take the efforts already underway to a new level of integration and effectiveness.

All of this means we are safer than we were on September 11, 2001.

But we are not safe. Nor are we likely to be for a generation or more. We are in a long war, and we face an enemy that is adaptable, dangerous, and persistent and who always has a vote. While we have won many battles since 9/11, there are many battles yet to be fought and setbacks are certain to come along the way.

Thank you. This concludes my remarks.

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
SEPTEMBER 10, 2007

Good morning, Chairman Lieberman, Senator Collins, and members of the Committee. I appreciate the opportunity to be here today to discuss the terrorist threats facing our nation and the measures the FBI has undertaken to confront them.

It is appropriate that this hearing takes place on the eve of September 11. The horrendous events that took place six years ago tomorrow have changed forever the way we look at threats and how we respond to them. As painful as it is to recall, we cannot let the memory of that day fade. Rather, remembering it inspires us to greater efforts to protect the Homeland.

In response to those attacks – and to other acts and threats of terrorism – the FBI realigned its priorities – making counterterrorism, counterintelligence, and cybersecurity its top three priorities – and shifted resources to align with those priorities. Since 9/11, the FBI has set about transforming itself into a national security agency, expanding our mission, overhauling our intelligence programs and capabilities, and undergoing significant personnel growth. Indeed, the last six years have been a time of unprecedented change for the FBI.

Although we recognize that there is much more work to be done, we have made remarkable progress. Today, the FBI is a stronger organization, combining greater capabilities with our longstanding commitment to the security of the United States, while upholding the Constitution and protecting civil liberties.

Threats Facing the U.S. Homeland

As the July 2007 National Intelligence Estimate (NIE) on terrorist threats to the U.S. Homeland found, al-Qa'ida remains the most serious terrorist threat to the Homeland, and will continue as such for the foreseeable future. Although the United States and our partners have had successes in weakening al-Qa'ida's capabilities, the group continues to persist and evolve.

Al-Qa'ida has been resilient in rebuilding its leadership and creating new safe havens. The group's ability to recover from successful U.S. government efforts targeting its personnel and infrastructure and its mergers with regional groups, such as Iraq's Jama'at al-Tawhid wal-Jihad and the Algerian-based Salafist Group for Predication and Combat (GSPC), which became al-Qa'ida in Iraq and al-Qa'ida in the Islamic Maghreb, have created a more diffuse violent Islamic extremist threat that complicates the task of detecting and deterring plots against the Homeland.

As has been noted in many fora, the most serious threat to our security would result from terrorists acquiring Weapons of Mass Destruction, such as chemical, biological, radiological, and nuclear (CBRN) weapons. Such weapons could enable adversaries to inflict massive harm against Americans, our military forces at home and abroad, and our

friends and allies. The NIE assesses that al-Qa'ida will continue to try to acquire and employ CBRN material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

Al-Qa'ida's message of violence has inspired followers around the world and is evidenced by its merger with the GSPC, which created AQIM. Following the merger, the GSPC, who used to focus on their own agendas, are now publicly declaring their allegiance to al-Qa'ida and may be more willing to assist al-Qa'ida in carrying out attacks against the Homeland. Al-Qa'ida is also inspiring individuals with no formal links to the group. The threat of homegrown terrorists or extremists, acting in concert with other like-minded individuals, or as "lone wolves," has become one of the gravest domestic threats we face.

In 2007, the FBI, working with our federal, state, and local partners, disrupted several attack plans that reflect the broader problem of the homegrown threat: On June 1, 2007, the United States Attorney's Office for the Eastern District of New York charged four individuals with conspiring to attack John F. Kennedy International Airport by planting explosives to blow up the airport's major jet-fuel supply tanks and pipeline. The leader of this group, U.S. citizen Russell Defreitas, was arrested by the FBI Joint Terrorism Task Force (JTTF) in New York City on June 1, 2007. On June 28, 2007, a six count indictment was returned charging Defreitas and three others with conspiracy to: attack a public transportation system; destroy buildings; attack aircraft and aircraft materials; destroy international airport facilities; and attack a mass transportation facility. The indictment also charges Defreitas and another with surveillance of a mass transportation facility.

On May 7, 2007, the FBI Philadelphia JTTF, in cooperation with state and local agencies, arrested six individuals, disrupting an alleged plot to attack Fort Dix, New Jersey. The group includes a Jordanian-born, naturalized U.S. citizen, Mohammed Shnewer. Also in the group were two legal resident aliens: Serdar Tatar, born in Turkey; and Agron Abdullahu, a Kosovar Albanian, who entered the United States as a refugee in 1999. Three Albanian brothers, Shain, Eljivir, and Dritan Duka – all of whom were born in Macedonia, and entered the country illegally – were also among those arrested. All except Abdullahu were charged with conspiracy to murder members of the uniformed services and other charges related to their plans to kill as many soldiers at the Army post as possible. Abdullahu was charged with aiding and abetting the Duka brothers.

As these cases illustrate, the diversity of homegrown extremists and the direct knowledge they have of the United States makes the threat they pose potentially very serious.

FBI Participation in the NIE Process

The FBI played an integral role in the drafting of the NIE, and concurs fully in its judgments. Based on those judgments, the FBI produced its yearly National Threat Assessment (NTA) for international terrorism, which is tailored to address the FBI's specific counterterrorism mission. This yearly assessment provides strategic warning of the most critical threats facing the U.S. Homeland, identifies critical intelligence gaps, and highlights emerging operational trends that require immediate collection and analysis to counter possible future threats. Furthermore, it helps shape our strategic response to identified threats.

FBI Response to Identified Threats

Fighting terrorism is a team effort that requires a collaborative response from all levels of government. As we have crafted our response to the threats identified in the NIE, we have engaged our federal, state, local, and community partners.

Al-Qa'ida - The changing nature of the threat from al-Qa'ida was apparent well before the publication of the NIE, and we began taking steps to address the information on the heightened threat as we received it. We have been working closely with the National Counterterrorism Center and our partners in the Intelligence Community in developing our operational responses to specific threat reporting. As with any potential threat to our national security, we identify information related to threats, launch investigations based on that information, and work with our partners in federal, state, and local law enforcement to identify suspicious activities that may be signs of pre-operational activity. Every day, we and our partners receive numerous reports of threats, the vast majority of which turn out to have little or no basis in fact. Nevertheless, we treat every threat report seriously and leave no stone unturned in resolving the threat.

In response to the assessments outlined in the NIE and the FBI's National Threat Assessment, our Counterterrorism Analysis Section generated more than 900 distinct actions, products or responses in support of internal and external customers that were designed to add clarity to threats to the Homeland and to identify and request collection in areas where more insight is needed. These included Intelligence Assessments and Bulletins (over 170), Current Intelligence Reports, collection taskings, and briefings to other FBI personnel, other Intelligence Community agencies, Congress, the Executive Branch, and foreign liaison services.

We are mindful of the new nature of the threat posed by al-Qa'ida and the more diffuse Islamist extremist threat, and are expanding our efforts to cover the new range of potential threat operators or actors. In particular, al-Qa'ida's attacks on the United Kingdom and on other overseas allies, along with the NIE's assessment that al-Qa'ida has created new sanctuaries, have led us to reinforce and expand our global partnerships.

Homegrown Radicalization – Much of the U.S. government's attention focuses on al-Qa'ida. However, as the terrorist plots we have dismantled this year indicate, we also have a problem with homegrown radicalization inside the United States. Although we assess that the level and intensity of extremism inside the United States does not equal that in the United Kingdom or elsewhere in Europe, we are well aware that we have extremists in the United States who wish to do us harm. As with any intelligence we receive on overseas threats, we also employ our own intelligence capabilities and leverage those of our federal, state, and local law enforcement partners to uncover plots by extremists in the United States.

Identifying these individuals and groups is a tremendous challenge, and the role of our law enforcement partners is critical in these efforts. Local police officers on the streets are the frontline of the war on terrorism. They may often be the first to detect potential terrorists. The vast jurisdiction of state, local, and tribal officers brings invaluable access to millions of people and resources, which can help protect the nation and its citizens.

The information gathered on the street and in our communities is one of the most powerful tools we have. The 18,000 state and local police departments and 800,000 full time sworn state and local police officers in the United States serve as a tremendous force multiplier in our efforts to protect the Homeland from terrorist attack.

Recognizing the crucial role they play in our counterterrorism mission, we have greatly enhanced our law enforcement partnerships by expanding the number and staffing of our Joint Terrorism Task Forces (JTTFs) and increasing our participation in state and regional fusion centers.

The JTTFs are multi-agency task forces around the country that the FBI established to address terrorism. In more than 100 locations nationwide, the JTTFs comprise local, state, and federal law enforcement and intelligence agencies that share information and conduct operations to prevent and dismantle terrorist plots.

In addition to the JTTFs, the FBI is committed to participation in all leading state-wide Fusion Centers, select Multi-Agency Intelligence Centers (MAICs), and the Antiterrorism Advisory Councils (ATACs) in federal judicial districts. More than 250 FBI personnel are currently assigned to 36 fusion centers throughout the United States. We have established connectivity to the FBI's SECRET-level computer network in 25 of the 36 supported fusion centers, and have obtained security clearances for 520 state and local law enforcement officers assigned to fusion centers.

Sixteen of the 36 fusion centers in which the FBI is involved are co-located with the FBI's respective Field Intelligence Groups (FIGs), leading to even stronger partnerships. The FIGs provide an intelligence link to the JTTFs, FBI Headquarters, and the U.S. Intelligence Community.

Among the ways the FBI makes national intelligence more readily available to state, tribal, and local law enforcement agencies is through the Law Enforcement Online (LEO) network.

Since 2002, the FBI has produced and disseminated more than 266 timely threat assessments and situational awareness bulletins geared toward state, local, and tribal law enforcement highlighting the tactics and vulnerabilities of international and domestic terrorist groups, as well as potential indicators of terrorist activity. Because it is important that the federal government speak with one voice on terrorism, 80 percent of the assessments and bulletins issued in FY 2007 were produced jointly with the Department of Homeland Security.

The FBI's Terrorist Screening Center (TSC) also plays a crucial role in providing actionable intelligence to state and local law enforcement. TSC was created to consolidate the government's approach to terrorist screening and to create a single comprehensive watch list—the Terrorist Screening Data Base (TSDB)—of known or suspected terrorists. The TSC makes its records available to the National Crime Information Center (NCIC) for access by government investigators, screeners, agents, and state, local, and federal law enforcement officers. This ensures that local, state, and federal terrorist screeners have ready access to information and expertise they need to respond quickly when a known or suspected terrorist is encountered within the United

States, at U.S. borders and ports of entry, and outside U.S. borders or at American Embassies and consulates.

In addition to reinforcing our relationship with the Law Enforcement Community, fostering good relations with Muslim and South Asian communities can play a key role in assisting us in identifying potential operatives al-Qa'ida may have sent to conduct operations against the Homeland. Members of these communities are well-placed to detect suspicious activities by newcomers to the community. They may also know of radicalization of individuals toward violent Islamic extremism within their communities.

The FBI has been developing an extensive outreach program to Muslim, South Asian, and Sikh communities to develop trust in those communities and to dispel myths about the FBI and the U.S. Government and to address concerns in those communities. Initiatives in this outreach program include the following:

- Special Agents in Charge in all 56 FBI field offices conduct Town Meetings with Arab and Muslim communities across the country. Major events have been held in New York, Washington and Los Angeles, as well as Springfield, Detroit, and Chicago.
- I meet periodically with members from the major Muslim and Arab community based organizations and civil rights groups.
- The Assistant Director for Public Affairs and the FBI's Community Outreach Program conduct regular conference calls to deal with issues of mutual concern with national Muslim leaders. The calls occur bi-monthly, with action items recorded and progress updated. The same group can be called together for a conference call on short notice in the event of a major incident and or controversy.
- Members of the Arab-American community attend the Citizens' Academy, a popular eight-week program designed to give community leaders an overview of the FBI and Department of Justice policies and procedures.

The members of these communities have an equal stake with the rest of American society in ensuring that terrorists are not able to threaten our way of life. The goal of our outreach efforts is to ensure that we are one community in the fight against terrorism.

Hizballah - The NIE also mentions the potential threat from Hizballah, which, before 9/11, killed more Americans than any other terrorist group. The FBI actively addresses Hizballah activities in the United States that potentially pose a threat to our nation. The FBI and the Department of Homeland Security's Immigration and Customs Enforcement (DHS-ICE) have had success using a combination of criminal and immigration laws to augment existing intelligence investigations of U.S.-based Hizballah matters.

"Single Issue" Groups/Domestic Terrorism - The terrorist threat does not just emanate from violent Islamic extremists. Domestic terrorists, such as white supremacists, anarchists, and eco-terrorists, remain a concern. The FBI continues to develop and maintain close liaison with law enforcement, the private sector, and the Intelligence Community to maximize the exchange of analysis and intelligence to counter these domestic terrorism threats. We use a variety of investigative techniques to gain

intelligence to deter, dismantle, and prevent attacks by domestic terrorists, and we are enhancing our nationwide networks of FBI Special Agents, analysts, and JTTF investigators dealing with domestic terrorism. We are also disseminating analytic products and providing domestic terrorism briefings to DHS, JTTFs, potential targets of domestic terrorism, and state and local law enforcement entities.

Improvised Explosive Devices – The Intelligence Community has identified IEDs and explosives as the most likely threats we face from terrorist groups. We have successfully disrupted significant plots to attack the United States and its interests, including the recently foiled plot in Germany. As IEDs are likely to be one of the most serious threats that we will continue to face, the need for a more unified national approach is clear. At the request of the Attorney General, the FBI took the lead role within the Department of Justice in response to Homeland Security Presidential Directive 19 to formulate a strategy with recommendations on how to best address potential use of explosives by terrorist groups with the homeland. We work closely with our counterparts at the Department of Homeland Security and the greater law enforcement and intelligence community to detect and interdict bombing plots in their planning and execution stages.

Weapons of Mass Destruction – Among the efforts the FBI has undertaken in response to the WMD threat identified in the NIE is proactive outreach to those in the private sector, academia, and the research community who work with potential WMD elements to educate them on the FBI's WMD-prevention goals and to foster stronger relationships.

Our historical relationship with local law enforcement also enhances the FBI's WMD programs and our national efforts to respond to these threats. Within our field offices, we have established WMD coordinators who foster consistent and substantive liaison relationships with local law enforcement personnel and emergency first responders. These coordinators also build partnerships with the scientific community, industry, academia, and other entities with a role in WMD-related investigations and incident response. Cohesive relationships in this area are critical for a timely, coordinated, and effective FBI response to WMD incidents.

Alignment of the FBI to Effectively Combat Threats

In addition to the measures we have taken to counter specific threats, the FBI has enhanced its ability to succeed in our broad national security mission by aligning our organization and programs to most effectively counter the post-9/11 threat.

Chief among the changes we have implemented is the development of an enhanced intelligence program, which we began implementing in early 2002. In 2003, we created an Office of Intelligence, which was charged with creating a single program to manage all FBI intelligence production activities. We also expanded our analytic, reporting, and intelligence capabilities.

Our efforts were communicated to Congress, the 9/11 Commission, and the WMD Commission. They offered additional recommendations and guidance on how to further strengthen the FBI's intelligence program. In response, the FBI in February 2005 officially established the Directorate of Intelligence as a dedicated and integrated intelligence service within the FBI. In September 2005, we implemented a Presidential directive based on the WMD Commission's recommendation to establish a "National

Security Service" that integrates the FBI's national security programs under the leadership of an Executive Assistant Director. The National Security Branch (NSB) comprises the FBI's Counterterrorism Division (CTD), Counterintelligence Division (CD), the Directorate of Intelligence (DI), and the Weapons of Mass Destruction (WMD) Directorate. The WMD Directorate was created in July 2006 to consolidate and integrate WMD-related entities within the FBI and to provide a comprehensive approach to issues having a WMD nexus.

The FBI's national security mission is to lead and coordinate intelligence efforts that drive actions to protect the United States. Our goals are to develop a comprehensive understanding of the threats and penetrate national and transnational networks that have a desire and capability to harm us. Such networks include: terrorist organizations, foreign intelligence services, those that seek to proliferate weapons of mass destruction, and criminal enterprises.

To be successful, we must understand the threat, continue to integrate our intelligence and law enforcement capabilities in every FBI operational program, and continue to expand our contribution to the Intelligence Community knowledge base.

A key development in the evolution of the FBI's intelligence program was the establishment of Field Intelligence Groups in each of the FBI's 56 field offices. The FIGs manage and coordinate the FBI's intelligence collection and reporting efforts in the field. From an information-sharing perspective, the FIGs are the FBI's primary component for receiving and disseminating information. They complement the JTTFs and other squads and task forces. The FIGs play a major role in ensuring that we share what we know with others in the IC and our federal, state, local, and tribal law enforcement partners.

As part of the FBI's efforts to enhance our understanding of the national threat picture, we are implementing a Desk Officer Program. The FBI's Desk Officers will assess and adjust collection efforts; identify collection gaps; target collection and source development against these gaps so they are consistent with priority national intelligence requirements; collaborate with partners; and convert and broadly disseminate the consolidated results, leading to enhanced knowledge of the threat environment.

The FBI's desk structure is based on country and topical priorities, as set forth in the National Intelligence Priorities Framework. The Desk Officer Program will focus not only on the management and advancement of existing cases but also on maintaining a networked and coordinated national collection effort. Over time, this program will enhance our confidence that we understand and have penetrated terrorist, criminal, cyber, and foreign intelligence threats.

Another critical element of our enhanced intelligence capability is our Confidential Human Source Program. The FBI, in collaboration with the Department of Justice, is completing a Confidential Human Source Re-engineering Project to enhance and improve the administration and operation of the FBI's Human Source Program.

As part of the Re-Engineering Project, the FBI and DOJ have worked to update guidelines on human source policy and human source validation. The ultimate goals of the Re-engineering Project are to streamline, consolidate, and update all human source guidelines; develop a "one source" concept; and strengthen the validation of human sources.

The release of the new Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources signed on December 13, 2006, marked a pivotal milestone to accomplish the one-source concept. Complementing these guidelines are two manuals: the Confidential Human Source Policy Manual (Policy Manual) and the Confidential Human Source Validation Standards Manual (Validation Manual). The Policy Manual governs source administration including compliance with the AG Guidelines, while the Validation Manual standardizes the FBI's source validation review process. These manuals, along with the new AG Guidelines, took effect on June 13, 2007.

To prepare our national security workforce to work collaboratively against national security threats to the United States, we continue to strengthen our training. As part of these efforts, New Agent Training has been recently modified to provide 100 additional hours of training in all national security-related areas. This includes 50 hours in counterterrorism training and additional instruction in counterintelligence, counterproliferation, and weapons of mass destruction. The additional training hours are designed to add to the flexibility and adaptability of all Special Agents to enable them to work the varied programs required of them.

We have undertaken a comprehensive restructuring of our approach to intelligence training. In addition to augmenting New Agents training so that our Agents understand their role in the intelligence mission, in the past eight months we have developed and are delivering a course targeting FBI Reports Officers (ROs) who play a central role in the intelligence cycle. We are on an aggressive schedule that will reach every "RO" by the end of this calendar year. We piloted and have run multiple iterations of a course for managers of intelligence analysts that is designed to give supervisors, many of whom are Special Agents, the skills and awareness to optimize their role in the intelligence cycle.

Working with the DNI and the Kent School at CIA, we developed and taught the first iteration of a 10-week Intelligence Basic Course that provided 24 analysts foundational skills in critical thinking, writing, and speaking – core competencies of the analytic art. The next course will take place in October. In addition to an intermediate version of this course, we are developing a shorter field version that we plan to deploy in early 2008. This field version is designed as a "refresher course" for analysts to maintain their critical skills.

National training seminars reaching every field office were held to address Field Intelligence Operations, Foreign Intelligence Collection, and Human Source Management and Validation. Beginning last month, the NSB leadership began a series of small group workshops for Assistant Directors-in-Charge (ADICs) and Special Agents-in-Charge (SACs) focused exclusively on decision making and managing field intelligence operations. We continue our successful partnership with the Kellogg School at Northwestern University to train senior and mid-level managers in leading the change that comes with our intelligence responsibilities.

In September 2006, we launched a new Human Source Targeting and Development course, which introduces agents to a systematic approach to identifying, developing, and recruiting human sources. The course incorporates relevant elements from tradecraft

used by other Intelligence Community agencies into a framework for a curriculum that is tailored to the FBI's unique jurisdictional authorities and mission.

Conclusion

With national security at the forefront of our mission to protect America, the FBI has been actively involved in assessing the threats to our nation, which in the case of al-Qa'ida and like-minded groups, remain serious.

In response, the FBI has developed multiple initiatives to counter particular threats, and has realigned our organization to enhance our ability to succeed in our overall national security mission.

Perhaps the gravest danger the United States faces is complacency as the years since 9/11/2001 pass. I can assure you, Mr. Chairman and members of the Committee, that the men and women of the FBI are determined never to forget the horrible attacks of that day. And we will use that memory to spur us on as we carry out our mission to protect the Homeland from terrorist attack while upholding the Constitution and the civil liberties of all Americans.

Question#:	1
Topic:	ETA system
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Responses to Questions from Secretary Chertoff

Question: The Implementing Recommendations of the 9/11 Commission Act (P.L. 110-53) requires DHS to implement a new Electronic Travel Authorization system. People planning to travel from Visa Waiver countries will have to apply electronically in advance – giving DHS plenty of time to check their names against terrorist databases. What are the Department’s plans for implementing the Electronic Travel Authorization system in a timely manner?

The Act also requires Visa Waiver countries to share with us information about travelers who may threaten the U.S. What steps does the Department plan to take to improve information-sharing with Visa Waiver countries?

Answer:

A DHS working group was established to develop a concept of operations and project plan, and to begin the project management process for initiating development and investment. A robust implementation plan is nearly completed, but further progress is thwarted due to the delayed enactment of an FY’08 appropriations bill. As ETA is a new program, it cannot be funded under the continuing resolution. While DHS plans to build upon its existing IT infrastructure and capabilities to stand up ETA, unique software development will need to be undertaken. Once funding has been appropriated or otherwise identified, DHS anticipates beginning a pilot effort within a year. Full operational capability, notwithstanding funding issues, is expected in 18 to 24 months.

DHS will seek to acquire information to assist in determining whether prospective Visa Waiver Program (VWP) travelers are eligible to travel to the United States at least 72 hours in advance. As a requirement to participate in the VWP, participant countries must share timely and accurate information as to whether its citizens or nationals traveling to the United States represent a threat to the security or welfare of the United States. Participant countries must also timely provide the United States with accurate lost and stolen passport (LASP) data. This information significantly deters terrorist travel, identity theft, and transnational criminal activity. DHS is working with the law enforcement and international communities to assess and develop new systems for reporting such information. Regarding the visa screening process, DHS also relies on its Department of State (DOS) colleagues as points of contact overseas to obtain, review and share information that is pertinent to an individual’s eligibility to travel and admissibility to the U.S.

Question#:	2
Topic:	information sharing
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Important strides are being made in creating the capacity for information sharing between levels of government. The FBI has its Joint Terrorism Task Forces and the Field Intelligence Groups; DHS is spurring the development of state and local Fusion Centers; numerous ports have Maritime Interagency Operations Centers; and states have their own Emergency Operations Centers. What is DHS doing to ensure that all these efforts are collaborative and integrated, rather than duplicative, or worse—disconnected? What role is the federal government playing in ensuring that each entity has discrete roles and responsibilities and is receiving the information it needs to perform its functions within the overall Information Sharing Environment?

Answer: DHS recognizes the issues of information sharing at different levels of the government and is working actively with the community to ensure these efforts are collaborated. DHS is working closely with the DOJ, FBI, ODNI, DOD and the Information Sharing Environment Program Management Office (PM-ISE) as it develops and implements Department-wide efforts to enhance information sharing with state, local and tribal governments.

DHS is an integral part of the PM-ISE efforts to address information sharing issues. DHS, with FBI, co-chairs the National Fusion Center Coordination Group (NFCCG), which ensures that FBI and DHS interactions with fusion centers and with State and local entities are coordinated. As part of this effort DHS and FBI are conducting assessments of each state and local fusion center to evaluate their needs and better coordinate on the support provided. FBI and DHS are developing an integrated deployment plan which helps delineate responsibilities for ancillary tasks including the certification of secure spaces and the granting of security clearances to fusion center personnel. An exemplary effort which demonstrates Federal coordination activities is the community effort to address Suspicious Activity Reports (SAR). DHS is working with PM-ISE, DOJ, DOD and other Departments, to examine information flow and analytical processes for SAR.

A key to coordination is the establishment of standards for the exchange of information, such as the National Information Exchange Model (NIEM). DOJ and DHS information systems will use the NIEM to ensure information is compatible and interoperable throughout DHS, DOJ, and regional information sharing systems

To facilitate the flow of threat information from the intelligence community to State and locals, DHS and FBI are leading the Interagency Threat Assessment and Coordination Group (ITACG). The ITACG will provide “detailees” to work in National

Question#:	2
Topic:	information sharing
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Counterterrorism Center (NCTC). This effort will enable the development of intelligence reports on terrorist threats and related issues that represent a federally coordinated perspective and are tailored to meet the needs of state, local, and tribal governments.

Within DHS we have made great strides to establish processes for improved information sharing and partnerships with FBI. DHS and FBI continually collaborate on joint publications and have published over 40 joint products over the last year including Joint Bulletins and Joint Assessments. These products are vetted independently by both organizations and then disseminated simultaneously with joint seals.

DHS has created a law enforcement shared mission community (LE-SMC), comprised of all of the law enforcement and related components (ICE, CBP, USSS, USCG, TSA, and USCIS) across DHS to coordinate disparate voices of law enforcement into a more cohesive effort. This effort is being developed in close coordination with the PM-ISE and DOJ to ensure a unified communications and sharing architecture in our interactions. Our coordinated effort should provide State, local, and tribal with a common interface for sharing law enforcement information.

DHS recognizes the importance of collaborating with other Federal partners to improve information sharing with State, local, tribal and private sector. We actively participate in PM-ISE efforts such as ITAGC and NFCCG to improve coordination across the community. We also engage individually with agencies such as FBI to produce joint products that create and disseminate coordinated information. This is a challenging issue, but we are dedicated to addressing it in a proactive and integrated manner.

DHS fully supports and participates in the Human Smuggling and Trafficking Center (HSTC) an interagency fusion center and information clearinghouse dealing with human smuggling, human trafficking and smuggler support of clandestine terrorist travel. DHS components such as ICE, USCG, I&A and DHS Policy have personnel in the HSTC and others (CBP, CIS, TSA) will soon have staff there. I&A and the HSTC are also increasing their cooperation and coordination.

Question#:	3
Topic:	IEDs
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: You testified that the Department will soon deliver to Congress a strategic document detailing what is being done to counter improvised explosive devices (IEDs).

When will that plan be delivered?

The Department was required by law to deliver a National Strategy for Bombing Prevention to Congress by January 2007. This document has not been received. Will you please explain why the Strategy has not been delivered?

Is the strategic plan you referenced in your testimony meant to fulfill that congressional mandate?

Answer: The conference report accompanying the Department's Fiscal Year 2006 Appropriations Act called for a National Strategy for Bombing Prevention. On February 12, 2007, President Bush signed Homeland Security Presidential Directive 19 (HSPD-19) (Combating Terrorist Use of Explosives in the United States). HSPD-19's requirements met the scope of Congress's request to the Department, and directed the Attorney General, in coordination with the Secretary of Homeland Security, other relevant agency heads, and State, local and tribal governments to assess the numerous efforts underway throughout the nation to thwart the terrorist explosives threat. The President also asked that a report be delivered to him that included recommendations and a forward-looking strategy that recognized the progress made to date while addressing any issues identified throughout the assessment he directed. The National Strategy for Improvised Explosive Devices (NSIED) the Department had compiled in order to address the FY'06 Appropriations Act Conference Report contributed heavily to the Attorney General's effort.

The strategic document referred to in Secretary Chertoff's testimony is the HSPD-19 report, which contains recommendations based on expanded inventories and interagency participation that only a directive inclusive of all Executive Branch agencies could achieve. The NSIED's recommendations formed the foundation for the HSPD-19 report, which, while classified due to the sensitivity of its comprehensive assessment of national capabilities and vulnerabilities, is conceptually similar to the original NSIED. We all agree that we must continue our holistic approach to bombing prevention inclusive of all aspects of deterrence, prevention, detection, protection, and response.

The HSPD-19 report is currently pending clearance and will be delivered to Congress, with appropriate consideration given to its classification, as soon as it is approved by the President. The delivery of the HSPD-19 report will be intended to fulfill the conference report request

Question#:	4
Topic:	CCTV
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: As you described in your testimony, Closed Circuit Television (CCTV) can be a valuable tool in fighting terrorism. At the end of July, the Senate passed the Homeland Security Appropriations bill with a bipartisan amendment I offered, requiring DHS to develop a national strategy for CCTV. A national strategy for CCTV would help DHS allocate grant money more effectively, help States and locals use CCTV systems effectively to protect citizens, and ensure appropriate civil liberties protections. Will you commit to starting work on a national strategy for CCTV so that it might be implemented as soon as possible?

Answer:

The Department of Homeland Security (DHS) continues to research the use of Closed Circuit Television (CCTV) in homeland security applications and is not yet prepared to commit to developing a national strategy. Complex fiscal, legal, privacy, and civil rights/civil liberties issues need to be vetted both internally and externally to DHS. In addition to the headquarters and component program offices responsible for CCTV applications, the numerous Office of General Counsel sections are evaluating CCTV issues, along with the Office for Civil Rights and Civil Liberties and the Privacy Office. A number of other DHS organizational elements are involved in and have strong equities associated with these areas, including the Transportation Security Administration, the Science and Technology Directorate, the United States Coast Guard, and the National Protection and Programs Directorate. Our Federal, State, local, and private-sector partners must be consulted to ensure that their views are considered.

Actions that the Department is undertaking to sort through the issues include:

- The DHS Privacy Office will, in December 2007, sponsor a public forum of academic and government experts, both in the U.S. and abroad, to begin discussion of privacy concerns posed by the use of CCTV and how best to address them. It will also consider the United Kingdom's recently updated "CCTV Data Protection Code of Practice."
- The Privacy Office has drafted a Privacy Impact Assessment specifically designed for DHS programs planning to use CCTV.
- The Office for Civil Rights and Civil Liberties is available to consult with all DHS components on specific projects, evaluating civil liberties aspects of the programs.

Question#:	4
Topic:	CCTV
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

In addition, DHS has identified a number of large-scale considerations that we continue to research to determine whether we will be able to develop a national strategy for CCTV. These considerations include:

- **Cost:**
 - Responsibility for the initial system and the associated installation, upkeep, and maintenance costs and
 - Data storage and other cost considerations.
- **Prioritization and Location:**
 - Methodology for deciding the prioritization of requested or needed systems and
 - Determination of geographical locations and sites, infrastructure assets, transportation points, etc.
- **Policies, Procedures, and Privacy:**
 - Best practices policy regarding CCTV and the use of recorded images;
 - Ownership and access to the system and stored information, and retention periods;
 - Information sharing policies;
 - Suspicious activity or crimes; and
 - Governance of camera use and information.
- **Civil Liberties**
 - Compliance with the Fourth Amendment on state surveillance activities, especially with respect to cameras possessing more than simple optical capabilities, and public/private shared camera feeds and
 - Reducing the day-to-day intrusiveness of web-based surveillance technology (e.g. webcams) while preserving the capability to leverage the full power of the technology in emergency circumstances, and where warranted by legitimate law enforcement interests.

These and the other questions surround the adoption of a CCTV policy and the possible development of a national strategy. Only after we have adequately addressed these considerations will DHS be in a position to consider a commitment to a national strategy.

Question#:	5
Topic:	Visa overstays
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Jon Tester
Committee:	HOMELAND SECURITY (SENATE)

Question: Mr. Secretary, according to one study published last year, as many as 45 percent of illegal immigrants may have come here on a legal visa, and then overstayed that visa. I know that President Bush and others in the administration – as well as some on this side of the aisle -- have expressed a desire to focus the resources of ICE on those who would do harm to the U.S., rather than on those who have come to this country to seek employment. But it is extremely difficult to make that determination when you are dealing with someone who drops off the grid when their visa expires. With that in mind, can you explain what processes the Department uses in order to systematically identify, locate and repatriate individuals who overstay their visas?

Answer: It is important to note there was no mechanism in place before the 9/11 attacks to identify and prioritize visa violators according to risk. ICE created the Compliance Enforcement Unit (CEU) in June 2003 to specifically target visa violators who pose an elevated national security or public safety threat. The CEU focuses on preventing terrorists and other criminals from exploiting the nation's immigration system by developing cases for investigation from the Student and Exchange Visitor Information System (SEVIS), the National Security Entry/Exit Registration System (NSEERS), and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) System. These systems allow the CEU to access information on the millions of students, tourists, and temporary workers present in the U.S. at any one time and identify those who potentially violate their status or overstay their visa.

Working with the U.S. Intelligence Community, ICE maintains a risk-based system to prioritize the hundreds of thousands of potential visa violations it observes annually. ICE is committed to investigating 100 percent of these prioritized potential overstays. In Fiscal Year 2006, ICE reviewed more than 200,000 unconfirmed overstay and immigration status violators, using manual and automated database queries to confirm that the potential violators were still in the United States and in violation of status. Potential overstay and immigration status violators not resolved through database queries are sent to ICE field offices for investigation by the nearly 300 agents assigned to conduct CEU enforcement operations nationwide. However, it is important to note that any one of ICE's roughly 6,000 criminal investigators can and do make arrests for visa violations. On virtually any given day, ICE field agents arrest visa violators who are not necessarily handled or processed by the CEU. In Fiscal Year 2006, there were many thousands of such arrests made by ICE field agents.

Question#:	6
Topic:	privacy report
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Jon Tester
Committee:	HOMELAND SECURITY (SENATE)

Question: I have real concerns with the privacy implications of some of the ways some measures proposed in the name of homeland security impact the rights of law-abiding Americans – from REAL ID to FISA changes right on down the line. One of the ways you can help people like me and many of my constituents who share these concerns is by being as transparent as possible when it comes to public reporting. But as I understand it, although the law requires DHS to report to Congress on privacy issues, including privacy violations, DHS has issued only two reports since 2003, and only one of these has included documented privacy violations. I hope that you understand that ignoring these issues – or not taking them seriously -- does real harm to the Department in the eyes of the public. It has now been 14 months since the last privacy report. When can we expect to see the next one?

Answer: The Privacy Office believes strongly in transparency in carrying out its mission and the office takes privacy complaints very seriously. To date, there have been few privacy-related complaints. When the office has received them, it has followed up on them with an investigation, and report, as appropriate. The next annual report, covering the period from July 2006 to July 2007 will be released in the very near future and includes a section on privacy incidents and complaints. In the interim, we encourage you to visit our website, www.dhs.gov/privacy, which provides information on all DHS systems of records notices, privacy impact assessments and reports on DHS programs.

Question#:	7
Topic:	language proficiency
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: How are you coordinating with other federal agencies on best practices for recruiting, training, and retaining language proficient individuals? What challenges remain?

Answer: DHS recognizes the criticality of non-English language proficiencies to accomplish our mission. We are pursuing an expansion of the current use of incentives for foreign language skills when required by the position(s). We are also actively looking for better ways to recruit, train and retain language proficient employees, including learning from and coordinating efforts with other federal agencies. Some of our current activities are outlined below:

- Based on best practices by the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency, DHS will participate in targeted diversity employment recruitment conferences in seven key locations (New York, Chicago, Boston, Detroit, Bay Area, New Jersey, and the District of Columbia) based on the candidate profiles available in those target markets. The central objective is to go to the locations with the highest percentages of diverse candidates with the backgrounds, skills (language, professional, etc) and education to fill mission occupations instead of waiting for individuals to find DHS.
- The Office of Intelligence and Analysis (I&A), U.S. Coast Guard and other agency components frequently participate with other Federal agencies in the intelligence community at veteran, college and diversity recruitment events aimed at language proficient individuals. These agencies typically include those working closely with the Director of National Intelligence, including DHS.
- The Department participates in the Department of Defense National Security Education Program (NSEP) to attract individuals with language skills and an interest in national security. Recently the Office of Inspector General Human Resource Office, Headquarters Equal Employment Opportunity Office and I&A Office representatives participated in an NSEP job sharing forum. The I&A Office received interest from 12 students and is working on the next steps to hire NSEP students.
- The Department is currently finalizing plans on a collaborative effort with the FBI called the “National Security Internship” program at George Washington University to begin June 2008. This is an intensive eight-to-ten-week, full

Question#:	7
Topic:	language proficiency
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

immersion summer program for qualified undergraduate and graduate candidates from throughout the U.S. that combines Arabic language, Middle Eastern studies, Homeland Security, and on-the-job training experience at DHS or FBI Headquarters. Plans are nearly close to completion and a more detailed overview will be forthcoming.

Although we are making progress, we realize challenges remain, including (1) legal and budgetary limits to the use of incentives for foreign language skills; (2) other agencies competing for the same talent pools; and (3) implementing procedures to calibrate proficiency levels possessed by individuals; as well as the levels required by the job(s). We are working through these challenges.

Question#:	8
Topic:	I&A
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: In a January 25th hearing before the Senate Select Intelligence Committee, Charlie Allen stated that DHS Intelligence and Analysis is “still in the “building” mode,” and has “yet to develop the required expertise and experience to fully implement” DHS’ mission. In your own opinion, is this still the case, and what might you highlight as areas in need? Would language capabilities qualify as one specific area of concern? If this is the case, what type of human capital plan is in place at DHS to recruit language proficient personnel?

Answer:

Training - I&A has developed learning roadmaps to address skills and capabilities for our intelligence analysts. We are in the process of developing specific characteristics of homeland security intelligence, such as Basic Intelligence Threat and Analysis Course (BITAC), which seek to standardize intelligence training across the homeland security stakeholders. We also plan to build mid- and senior-level courses to expand the standardized training at all levels.

Recruiting - In addition to training and professional development efforts, I&A has worked to refine recruiting efforts to build an experienced workforce. I&A is also participating in ODNI's Joint Duty Program in order to bring seasoned intelligence community professionals to I&A on a rotational assignment in an effort to quickly implement their experience and expertise in meeting DHS' mission. I&A does not currently have a requirement for personnel with language proficiencies, but our recruiting efforts are focusing on individuals with cultural competencies based on in-depth knowledge of heritage communities.

Realignment - DHS/I&A realigned its intelligence missions to ensure we were addressing Homeland threats pertinent to DHS’s mission. We reorganized our personnel to focus on the following key threats: 1) People – either those attempting to use fraudulent means to enter the United States for nefarious purposes, or extremists already in the United States, who are driven to violence against Americans; 2) Dangerous materials in the hands of extremists, specifically chemical, biological, radiological, and nuclear materials, as well as explosives; 3) Infectious diseases and threats to agriculture; 4) Borders, especially human smuggling or dangerous cargoes; and 5) Threats to critical infrastructure.

Question#:	8
Topic:	I&A
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Language – DHS and FBI are working out the details of a plan to begin by the summer 2008 an internship program focused on recruiting individuals with language capabilities and in-depth cultural knowledge on countries of concern.

Better products – In addition to investments in analytic training, DHS/I&A has employed talented editors, writers, and production managers to improve intelligence products. In partnership with the intelligence community, the mission of one of I&A's branches is focused on fostering excellence through the introduction of analytic techniques and training opportunities, as well as hosting a speakers' series to deepen analysts' knowledge of Homeland Security topics.

Question#:	9
Topic:	train and certify
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: I know that your agency has developed an introductory program at FLETC to train and certify intelligence professionals. Acknowledging that this program is relatively new, could you describe benefits noticed by your agency and any changes you see in the future to strengthen training? Is there any ability to allow analysts from other components within the Intelligence Community to train in your program?

Answer: In response to the Intelligence Career Force Management Board, DHS developed the Basic Intelligence and Threat Analysis Course (BITAC) for analysts with up to five years of experience. The goal of BITAC is to develop intelligence skills and esprit de corps early in a DHS intelligence professional's career.

DHS will implement a follow-on course, the Mid-Level Intelligence and Threat Analysis Course (MITAC), in April 2008. Additionally, in early FY 2009, DHS will implement the Senior Level Intelligence and Analysis Course (SITAC). Together, the three courses will provide entry-level through senior-level intelligence training for the DHS Intelligence Enterprise.

BITAC is currently available to departmental as well as state, local and tribal partners with priority given to DHS' intelligence professionals. To date, intelligence analysts from DHS, the Department of Interior, the National Security Agency, and some State and Local Fusion Centers have completed the training.

Question#:	10
Topic:	propaganda
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

Question: This past week, Osama Bin Laden reappeared in what appears to be a recently-filmed video after being absent for almost three years. In the 26-minute tape, he makes references to the war in Iraq, the newly elected leaders in Britain and France, global warming and even the real estate markets in the United States. These tapes are just one component of al Qaeda's propaganda machine which is pursuing an aggressive media strategy to spread their message and engage and recruit new members. Over the last two years, its media production company, Al-Sahab, has released over 75 videos that are of high quality and have subtitles in various languages to reach as many people as possible. Al-Sahab also is developing a rapid-response capability and has released new videos within 24 hours of a major news stories. Is the United States losing the propaganda and media war against Al Qaeda?

Answer: Al-Qaeda's propaganda efforts have increased dramatically in breadth and scope since 11 September 2001. Al-Qaeda in the last two years dramatically increased the sophistication of its propaganda while simultaneously reducing production timelines. Of particular concern to the Homeland are recent messages that appeared to be aimed at garnering support for al-Qaeda from minority populations in the United States. Nevertheless, DHS assesses that al-Qaeda's extremist message probably influences the attitudes of only a very small number of radicalized individuals in the United States. Furthermore, recent global polling data suggests a decrease over the past five years in support for al-Qaeda's violent attacks.

Al-Qaeda released statements earlier this year targeting the African-American Muslim community. DHS/I&A assesses that al-Qaeda's attempt to link violent extremist rhetoric to the struggles and grievances of disaffected minority groups might resonate within radical segments of the U.S. population. Thus far, DHS/I&A has no indication that radical groups who might be receptive to these messages have translated sympathy for al-Qaeda into support for violent action within the Homeland.

The Pew Research Center's Global Opinion Trends 2002-2007: A Rising Tide Lifts Mood in the Developing World (released July 24, 2007) found support for terrorist tactics (to include suicide bombings) has fallen since 2002 in seven out of eight countries where the Pew study captured data. The largest declines occurred in Lebanon, Pakistan, Bangladesh, and Jordan.

The USG is working hard to ensure that accurate and timely information about al-Qaeda is provided to a variety of audiences. We are increasing use of creative mediums to

Question#:	10
Topic:	propaganda
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

communicate our messages and are seeing a change in attitudes and opinions in majority-Muslim countries. Six years after the September 11 attacks, polls show that Muslims overwhelmingly reject al-Qaeda's tactics, such as suicide bombings that target civilians. People in America and many other Western nations have expressed strong disapproval of bin Laden and al-Qaeda since the September 11 attacks, but the dramatic decline over the last few years is his standing in these majority-Muslim countries.

Polls in Afghanistan and Iraq show that more than 90 percent of those populations have unfavorable views of al-Qaeda and of bin Laden himself. Polling in Turkey two years ago found that 90 percent of citizens believe the al-Qaeda bombings in London, Istanbul, Madrid, and Egypt were unjust and unfair; 86 percent thought that there was no excuse for condoning the Sept. 11 attacks; and 75 percent said bin Laden does not represent Muslims.

Support for terrorist tactics has fallen in seven of the eight predominantly Muslim countries polled as part of the Pew Global Attitudes Project since 2002; in most cases, those declines have been dramatic. Five years ago in Lebanon, 74 percent of the population thought suicide bombing could sometimes be justified. Today that number has fallen to 34 percent. Similar declines in support have occurred in Bangladesh, Pakistan, Indonesia and Jordan. Perhaps most significantly, one of al-Qaeda's central propaganda points -- that their actions can be justified by Islam -- is losing traction. WorldPublicOpinion.org found in April that large majorities in Egypt (88 percent), Indonesia (65 percent) and Morocco (66 percent) agree: "Groups that use violence against civilians, such as al-Qaeda, are violating the principles of Islam. Islam opposes the use of such violence."

Question#:	11
Topic:	intelligence
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

Question: Last week, Fox News reported that a website hosted by a server in Minnesota was trying to recruit terrorists and gave detailed descriptions about the best way to attack U.S. military bases. Is there any intelligence that indicates these sites are run by Al Qaeda cells in the United States? Is Al Qaeda coordinating the establishment of these sites from abroad or are they set up by independent actors?

Answer: DHS I&A, working through the broader U.S. intelligence community, has no indications that the myriad of radical websites – including those hosted in the United States – are run by al-Qaeda cells in the Homeland. The diffuse nature of Internet information precludes the need for al-Qaeda to have members physically located in country in order to disseminate propaganda; moreover, the information contained within radical websites as well as the sites themselves are continually mirrored from partner sites across the globe such that a site hosted in the U.S. could have received its content from any number of partner sites across the globe, to include disseminated material from al-Qaeda.

Question#:	12
Topic:	information technology
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

Question: What is being done to counter Al Qaeda's media strategy and to dismantle their information technology apparatus?

Answer: The U.S. Department of State's public diplomacy is guided by three strategic imperatives: (1) offering a positive vision of hope and opportunity promoting freedom, including free speech and assembly, freedom to worship, the rule of law, and the rights of women and minorities; (2) isolating and marginalizing violent extremists and undermine their efforts to exploit religion to rationalize their acts of terror; and (3) fostering a sense of common interests and common values between Americans and people around the world. The U.S. Department of State's Counterterrorism Communications Center (CTCC) is developing messages and strategic communications programs to counter terrorist propaganda and extremists' use of the media, with particular attention given to using all forms of media, including the internet, to reach vulnerable youth across the globe. The DHS Office of Strategic Plans/CT Plans provides representation at the and fully collaborates in the development of CTCC's messaging and counter-narrative.

The U.S. Department of State's "Identifying Misinformation" website, in English and Arabic, is devoted to countering misinformation, conspiracy theories, and urban legends that appear in extremist and other web sources. The State Department produces a wide array of print and electronic media describing for foreign audiences, in their own languages, the need to counter those who have committed or wish to commit terrorist acts.

The U.S. Department of State's "Response to Terrorism" website explains U.S. counterterrorism policy. It also provides links to the Electronic Journal series, the National Strategy for Combating Terrorism, the designated Foreign Terrorist Organization list, and the State Department's Country Reports on Terrorism.

The Broadcasting Board of Governors (BBG) continues to build its capacity to broadcast to Muslims in the Middle East and other parts of the world.

The U.S. Department of State's Bureau of Public Affairs Office of Broadcast Services uses television and radio to bring the U.S. foreign policy message to the Middle East and worldwide audiences. There are an ever-increasing number of interviews with Arab and regional journalists/media outlets, including interviews conducted primarily in Arabic.

Question#:	12
Topic:	information technology
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

In the U.S., the DHS Office for Civil Rights and Civil Liberties (CRCL) is working to counter extremist messages, such as al-Qaeda's, by building an unprecedented level of cooperation with, developing and cultivating partnerships with, and promoting civic participation by Muslim Americans and other key ethnic and religious communities. The DHS Office of Intelligence and Analysis (I&A) works closely with CRCL to inform their actions and routinely provides information and assessments related to al-Qaeda-associated threats and messages.

In this regard, CRCL holds regular meetings with ethnic and religious community leaders from Arab, Muslim, Sikh, and South Asian American communities. It also participates in significant conferences and events throughout the year. CRCL plays a leading role in regular community roundtables with the Arab, Muslim, and South Asian American communities in six key cities: Houston; Detroit; Los Angeles; Washington, DC; Chicago; and Buffalo. In addition, CRCL has assembled an "Incident Communication Committee" to engage with Arab, Muslim, Sikh, and South Asian American community leaders in the aftermath of any future terrorist act or homeland security incident.

The DHS Science and Technology (S&T) Directorate contributes to the Department's efforts to counter extremist messages through research aimed at understanding, predicting, and preventing the process of radicalization at the individual, group, and community levels.

The S&T Directorate has created the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Center of Excellence (COE), led by the University of Maryland, to understand the social and behavioral aspects of terrorism and responses to terrorism. START COE has over 30 active research projects on the social behavioral aspects of terrorism and is engaged in a multi-campus project to encourage dialogues among Muslim, Christian, and Jewish students, develop multimedia arts programs focused on fostering respect for different faith traditions, and build the social relationships between faith traditions that can help mitigate potential conflicts when more serious differences arise.

The S&T Directorate's Human Factors Division (HFD) has as one of its core missions "to apply the social and behavioral sciences to improve detection, analysis, and understanding of the threats posed by individuals, groups, radical movements." This Division has created a dynamic research program on radicalization and radicalization deterrence. The START COE supports HFD's operational focus by providing fundamental knowledge discovery. HFD builds on this knowledge with research programs that identify actionable indication and warnings that support the effective use of intervention and deterrence options. HFD's programs through the national labs also

Question#:	12
Topic:	information technology
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

integrate these indicators into products for use by intelligence analysts, policymakers, and operational components in identifying a threat and preventing an attack.

Secretary Chertoff has identified the issue of radicalization as a significant priority for the Department. In response to the Secretary's desire to understand the issue and develop strategies to counter the phenomenon, the Office of Strategic Plans and the S&T Directorate organized an internal DHS Radicalization and Engagement Working Group (REWG). The REWG was organized with several goals - increasing awareness of the issues surrounding radicalization within DHS and the United States Government (USG); coordinating and integrating the radicalization efforts of various DHS components, as well as the efforts of the USG; identifying radicalization research gaps that could be addressed through projects funded by the S&T Directorate or our international partners; and establishing DHS as a leader in policy, operations, and scientific research related to radicalization. It is comprised of several key components and offices within the Department, including, among others, the Office of Policy, I&A, Federal Emergency Management Agency, the S&T Directorate, Citizenship and Immigration Services, Immigration and Customs Enforcement, the Homeland Security Advisory Council, and CRCL.

Question#:	13
Topic:	WHTI
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

Question: I appreciate the flexibility in the roll-out of the land and sea phase of WHTI, but remain concerned about the summer 2008 target, particularly given the disruption in passport production this spring and summer. In your testimony you also discuss a driver's license approach to WHTI which I fully support but which will not be deployed by summer 2008. The sequencing is difficult to understand, though. Why would an American get an enhanced driver's license if they already had to get a passport to meet the summer 2008 deadline? One corner of Minnesota, the Northwest Angle, can only be reached by driving through Canada. These folks rely on visitors to the Angle to provide services, tourism dollars, and emergency response. I have long suggested that a creative solution needs to be found for the Northwest Angle so that not only can they travel with ease to the rest of the state, but so that their visitors can likewise reach them. Can you tell me whether the Department is going to take into account the unique needs of communities like this in its final rule?

Answer:

The implementation of a travel document requirement and the standardization of travel documents are critical steps to securing our Nation's borders and increasing the facilitation of legitimate travelers. On January 31, 2008, DHS proposes to end the practice of accepting verbal declarations alone as proof of citizenship at our land and sea ports. United States and Canadian citizens will be required to carry a WHTI-compliant document or government-issued photo identification, such as a driver's license, and proof of citizenship, such as a birth certificate. The implementation of a travel document requirement will not diminish CBP's ability to utilize existing protocols and other inspection processes to admit travelers with unique and exigent circumstances, such as those who travel to and from unique geographic locations such as the Northwest Angle. DHS/CBP will continue to allow a degree of flexibility to certain travelers based upon unique and exigent circumstances.

With respect to full implementation, the Notice of Proposed Rulemaking made clear that while DHS anticipates this in the summer of 2008, it is contingent on a number of factors. DHS/CBP will take a phased, deliberate approach to implement WHTI. The transition period will ensure that citizens of the United States and Canada will be able to obtain the documents necessary to satisfy WHTI while addressing at the earliest possible time the security vulnerability identified by the 9/11 Commission. The phased approach to WHTI implementation will ensure that DHS is able to effectively communicate the

Question#:	13
Topic:	WHTI
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

requirements to United States and Canadian citizens and that acceptable WHTI-compliant documents will be available to them.

For states that work with DHS to develop enhanced driver's licenses or identification cards (EDLs), their residents will have the option to obtain and use an EDL in order to enter the United States at land and sea ports of entry.

EDLs will also contain facilitative technology, giving residents choosing to obtain an EDL the travel benefit of using this technology when crossing the border. We encourage states to begin working on EDL projects with DHS so that their residents can have this option; however, EDLs and passport cards are not the only proposed alternatives to comply with upcoming documentary requirements. Residents of border communities also have the option of enrolling in existing DHS Trusted Traveler Programs (NEXUS, SENTRI and FAST).

Question#:	14
Topic:	border security
Hearing:	Confronting the Terrorist Threat to the Homeland: Six Years After 9/11
Primary:	The Honorable Pete V. Domenici
Committee:	HOMELAND SECURITY (SENATE)

Question: Secretary Chertoff, I would like to discuss border security with you, too, because as you know, porous land borders create a potential route for terrorists to use to enter the U.S. I applaud your efforts to improve border security by putting thousands of new border patrol agents on the ground, constructing new border fencing and vehicle barriers, and providing new border security technologies and other border assets, but I think we can, and must, do more. I have long advocated the use of unmanned aerial vehicles for border security efforts. Section 5201 of the Intelligence Reform Act required that DHS develop and implement a plan for the surveillance of the southwest border of the United States using UAVs. Where are you at in carrying out this plan?

What do you need from Congress to further secure our nation's borders?

Answer:

The U.S. Customs and Border Protection's (CBP) Air and Marine National Air Strategic Plan was delivered to Congress in 2006 and is currently being implemented. Updates to this plan were submitted to Congress in August 2007. The Unmanned Aerial System (UAS) program has funding resources consistent with department funding priorities and in accordance with the Strategic Plan.

Of the four UASs, formally known as Unmanned Aerial Vehicles (UAVs), acquired to date, two are operational on the southwest border and two new assets will be delivered in November 2007 and January 2008. One of these two will deploy to the northern border and the other will deploy to the southwest border. This will bring the total number of assets on the southwest border to three.

Two more UAS/UAVs are funded, but not yet on contract. These assets should be delivered in late fiscal year 2008/early fiscal year 2009; one will be deployed to the northern border, and the other will be delivered as a maritime variant that will operate over the Southeast Caribbean, Eastern Pacific, or Great Lakes operating areas as required.

CBP UAS/UAVs have flown more than 1,300 flight hours in support of border security missions. The UAS program is credited with the seizure of more than 15,000 pounds of marijuana, the apprehension of approximately 2,200 illegal aliens and narcotics traffickers, and more than 2,300 detections of illegal entrants.

CBP plans to expand the UAS capability on the Southwest border by installing Ku Band satellite communication assets in Sierra Vista, AZ and at the Air and Marine Operations Center in Riverside, CA. Ku Band infrastructure will allow CBP to fly Predator Bs beyond line of sight thus covering greater areas of the southwest border.

Hearing Date: September 10, 2007
Committee: HSGAC
Member: Senator Lieberman
Witness: Director McConnell
Question: 1

Question 1: (U) The Implementation Plan for the Information Sharing Environment, released in November 2006, contained 41 actions that were intended to be completed by June 30, 2007. How many of these have been completed? For the action items that have not been completed, please provide a brief explanation and an estimated timeline for completion.

Answer: (U) The Information Sharing Environment (ISE) Implementation Plan has 48 Phase I actions. Thirty-one of these actions have been completed. The remaining 17 actions are currently being completed in the interagency along with our State, Local and private sector partners.

(U) Issues such as alerts and notifications, identity management, implementation of new and emerging collaborative technologies, standards, training, incentives for information sharing, and a private sector framework are all actively in progress and resulting in improved interagency collaboration. Some of these critical ISE issues will remain works in progress as they are continually adjusted to support the counterterrorism mission.

(U) As the ISE progresses from planning to implementation, the Program Manager-ISE is working with stakeholders and Congress to revise and update the actions as required. The ISE Implementation Plan will continue to support the overall vision provided by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Section 1016, and is intended as a living document to accommodate the evolving terrorist threat against this Nation.

Hearing Date: September 10, 2007
Committee: HSGAC
Member: Senator Lieberman
Witness: Director McConnell
Question: 2

Question 2: (U) Important strides are being made in creating the capacity for information sharing between levels of government. The FBI has its Joint Terrorism Task Forces and the Field Intelligence Groups; DHS is spurring the development of state and local Fusion Centers; numerous ports have maritime interagency operations centers; and states have their own Emergency Operations Centers. What is the DNI doing to ensure that all these efforts are collaborative and integrated, rather than duplicative, or worse—disconnected? What role is the federal government playing in ensuring that each entity has discrete roles and responsibilities, and is receiving the information it needs to perform its functions within the overall Information Sharing Environment?

Answer: (U) The PM-ISE assisted in crafting the DHS response to their version of this query. The DHS response accurately represents ODNI's participation in the collaboration process.

Hearing Date: September 10, 2007

Committee: HSGAC

Member: Senator Voinovich

Witness: Director McConnell

Question: 1

Question 1: (U) The Intelligence Reform and Terrorism Prevention Act of 2004 instructed the Director of National Intelligence to prescribe personnel policies and programs for the intelligence community. At the time, we were concerned about whether or not you would have the authority to get the job done. Your written testimony describes some key programs that the intelligence community has initiated, such as mandatory joint duty before entering senior ranks and a formal process for recruiting throughout the intelligence community. Do you have sufficient authority to develop and oversee a common workforce throughout the intelligence community?

Answer: (U) The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 charged the Director of National Intelligence (DNI) with recruiting, developing, and retaining an Intelligence Community (IC) workforce that is sufficiently talented, trained, diverse, and “joint” to accomplish our critical national security mission. However, many IC agencies and elements have, since their inception, developed and administered their own personnel systems and human capital management practices without regard to other IC agencies, but the establishment of some common personnel policies is essential if the IC is to develop a stronger sense of unity and community. Integrating personnel systems that developed over time requires overcoming years of tradition and independence. The IRTPA provided the DNI the authority to establish such policies and the DNI has begun to do so in many critical areas, including civilian joint duty, pay and performance management, and a human resources information systems. The personnel authorities provided to the DNI with respect to the IC are limited and ambiguous, and they overlap with the authorities of those cabinet secretaries with IC employees. None of the human capital authorities provided to the DNI by the IRTPA “override” those of any cabinet official, such as the Secretary of Defense, even on matters such as civilian joint duty which are mandated by the IRTPA. Reconciling the DNI’s authorities with those of cabinet secretaries has been a challenge that has required a great deal of interagency coordination and collaboration.

(U) The strong commitment, common vision, and good faith efforts of the ODNI and IC leadership have contributed to significant progress towards meeting the spirit and goals of the IRTPA. For example, the civilian joint duty directive and program guidance are the result of an exhaustive interagency process. Similar efforts are underway as part of our IC pay modernization effort. However, as many of the successes to date are dependent upon senior leaders who share a common vision for the IC, the basis for continued progress is fragile.

Hearing Date: September 10, 2007
Committee: HSGAC
Member: Senator Voinovich
Witness: Director McConnell
Question: 2

Question 2: (U) The numerous agencies that make up the intelligence community function under various personnel authorities. For example, those from the Departments of State and Treasury are covered by title 5 of the United States Code, the Central Intelligence Agency is exempt from title 5, and the Departments of Defense and Homeland Security are developing new personnel systems for their respective agencies. What are your short and long term goals for the workforce of the intelligence community? What do you see as the ideal framework for human capital management of the intelligence community workforce? Do you have the statutory authority to reach those goals?

Answer: (U) The Director of National Intelligence's (DNI's) short and long term goals for the Intelligence Community (IC) workforce are outlined in the DNI's Five Year Strategic Human Capital Plan (June 2006) and his 500 Day Plan for IC integration and collaboration. The long-term goal is the creation of a true "national intelligence service," integrated by shared values and a common ethos, and aligned by supporting human capital policies and systems that balance IC-wide coherence with the need for agency (and departmental) flexibility and focus. Major initiatives include:

- a. (U) IC Civilian Joint Duty Program: The crosscutting problems faced today by the IC require professionals and leaders with an understanding and awareness of the entire IC. Senior leaders need experience and established relationships beyond just a single agency. The civilian IC joint duty program is essential to the Community's transformation and to the establishment of a culture of collaboration. It responded to the IRTPA which charged the DNI with establishing "mechanisms to facilitate the rotation of personnel of the IC through various elements of the IC in the course of their careers to facilitate the widest possible understanding by such personnel of the variety of intelligence requirements, methods, users, and capabilities." As the centerpiece of the IC's leadership development strategy, this program is intended to: ensure the development of IC employees who have an enterprise-wide perspective; cultivate cross-organizational networks; facilitate knowledge and information sharing; and ultimately develop and deploy leaders who understand the scope and complexity of the IC and are able to effectively integrate the Community's resources in support of the IC mission. The ODNI issued instructions implementing the program in June 2007 with the concurrence of the cabinet-level members of the Joint Intelligence Community Council. Moreover, as a demonstration of the IC's senior leadership commitment to joint duty and to "jump start" the initiative, the major IC agencies voluntarily identified over 75 significant joint duty rotational opportunities at the GS-15 or senior executive level, and selected over 40 of their best candidates to take on these challenging positions as part of a leadership exchange and assignment pilot.

- b. (U) IC Performance-Based Pay System: Performance management and compensation policies across the IC vary widely, impede cross-agency movement, and do not consistently reward high performance, collaboration, technical expertise, and contribution to mission. These policies also lack clear linkage to strategic priorities and typically emphasize hierarchical relationships, rather than collaborative behaviors. In 2006, the DNI, with the concurrence of the IC's senior leadership, determined that the IC should proceed with the design, development, and deployment of a modern compensation "architecture" for its civilian employees that better links pay to performance and labor market competition. The 500 Day Plan calls for completing the detailed design and development of that system and beginning its implementation. The implementation of the initiative is fully funded over the next five years in the National Intelligence Program (NIP), and the overarching policy guidance is in the final stages of interagency coordination. The first directive to be issued will establish performance management system requirements, which will establish a common baseline on which to evaluate all IC civilian employees. A similar set of requirements will be issued shortly thereafter for IC senior civilian officers. In coordination with the departments and independent agencies with IC employees, we will begin its initial deployment in FY 2008. It will also be event-driven, based on the "readiness" of IC agencies and elements to implement a pay for performance system.
- c. (U) Equal Employment Opportunity Plan of Action: The ODNI has made greater diversity a mission imperative for the IC. A diverse IC workforce is a competitive advantage for the IC and effectively positions us to win the War on Terror through full inclusion of all groups. Private industry has learned, and the research shows, that diverse teams produce better results and better decisions. To that end, the DNI signed a policy statement on IC Equal Employment Opportunity (EEO) and Diversity and published the first-ever IC EEO and Diversity Cross Cutting Emphasis Area Plan that focuses on strengthening (1) leadership and accountability; (2) workforce planning; (3) recruitment, hiring, and retention; and (4) career development and advancement. This plan and the subsequent implementation plans that will be developed and implemented across the IC affirm the DNI's personal commitment to the principles of EEO and diversity.
- d. (U) Strengthen Recruiting Relationships with Colleges and Universities: In order to maintain a pipeline of diverse, talented applicants to meet our immediate long-term workforce requirements, the IC needs to reach out to our Nation's colleges and universities, especially those that produce graduates with the diversity and critical skill sets we need, and establish, maintain, and grow effective working partnerships with them. We will build upon the success of the Centers for Academic Excellence program, which provides technical and financial support to select colleges and universities, particularly those with diverse student populations, in order to improve the ability of the IC to attract the best and brightest.
- e. (U) Recruiting and Retention of Heritage Americans: The IC requires substantial numbers of employees with mission-critical language, regional, or cultural expertise. This expertise exists in our Nation's first and second generation Americans, (such as Arab-American, Korean-Americans, etc) from heritage communities whose native language skills and cultural experiences are indispensable as we face current and

future national security challenges. The ODNI is in the process of refining and executing a comprehensive recruiting and retention strategy for such first and second generation Americans, institutionalizing relationships with “Heritage Community” organizations, and partnering with colleges and universities that serve these diverse groups. We are also reviewing the security clearance policies that have historically been a potential barrier to the hiring of our newest citizens. This will expand the recruiting “pipeline” of high-quality, diverse applicants with core, mission-critical languages and regional/cultural expertise.

- f. (U) National Intelligence University: IC education and training efforts are currently optimized for each agency and have limited offerings with an enterprise-wide perspective. The lack of a “joint” training facility impedes the goal of improving collaboration and integration. Without a joint facility, agency training programs are likely to continue to be narrowly focused, and they will not foster a collective identity among intelligence officers. We are developing a business case and action plan to acquire a permanent “bricks and mortar” National Intelligence University facility. We will also develop joint education and training to reinforce functional and professional competencies at the basic, intermediate, and advanced levels to strengthen IC collaboration through the development of (1) a common foundation of solid intelligence tradecraft skills to meet the IC Professional Standards, and (2) a strong joint perspective on the intelligence enterprise.
- g. (U) IC Human Resources Capabilities Catalog: The IC does not have a precise, current inventory of the skills and capabilities of its most mission-critical human resources. Such an inventory is crucial if we are to fully exploit the diverse talents of our current workforce. We must know who and where our experts are on any given intelligence topic. Making such information widely available to all IC professionals will facilitate their collaboration and information sharing. This initiative builds upon the success of the Analytic Resources Catalog, to catalog, collect, analyze, and disseminate detailed, competency-based information on the current capabilities of our analysts, collectors, scientists and engineers, acquisition professionals, and others in mission-critical disciplines, identifying the top experts on any given intelligence topic, enabling the creation of collaborative and information sharing networks, and revealing critical skills gaps. The IC Competency Catalog is also crucial to our ability to assess the quality and quantity of the skills resident in our workforce against current and future requirements, so we can target our recruiting, training, career development, and deployment strategies to close any gaps between the two.
- h. (U) A Common, Core Human Resources Information System: The proliferation of human resource information systems (HRIS) in the IC prevents the sharing of critical personnel information and results in costly inefficiencies, both in IT infrastructure and in human resources (HR) service delivery. These “stove-piped” systems impede lateral information flow, require burdensome data calls to support the development and oversight of IC-wide human capital strategies and policies, and sub-optimize increasingly scarce human and financial resources. A common HRIS platform would realize efficiencies through enterprise software licensing agreements, common IT support structures, and shared HR service delivery. The DNI is beginning to integrate the HR information systems of the six largest IC elements (FBI, CIA, NSA, NGA, DIA, and NRO), starting with (1) the design and development of an IC-wide HR

“data repository” that will eventually encompass the IC Capabilities Catalog, described above; (2) the identification of common HR business processes and functional requirements to be met by a common HRIS platform; and (3) development of a plan for migration to a common HR software platform. An IC HR data repository, as the first step in developing and deploying a common, integrated HRIS, will support cross-Community strategic HR planning, collaboration, and career paths – all key elements of an IC culture that values and reinforces collaboration. It will also provide significant savings in IT infrastructure and serve as the platform for far more efficient “shared” HR service delivery.

- i. (U) Civilian Employment Plans: The DNI, in coordination with the IC agencies and elements, has developed an initial set of Civilian Employment Plans (CEPs). These plans will identify and evaluate current and projected civilian requirements by major mission area, take into account the strategic threat environment, model the demographic variables that may impact those requirements (such as estimated accessions and attrition), account for the necessary infrastructure (facilities, IT) and administrative support, and describe the human capital strategies that we intend to employ in closing mission-critical skill gaps. The CEPs are developed under the oversight of the Civilian Employment Oversight Board, which brings together the human capital and financial management leaders within the IC. The next steps are to require all IC elements to submit CEPs on an annual basis. Furthermore, an overall IC-wide CEP will be crafted, derived from individual agency plans, to complement the FY 2009 budget submission.
- j. (U) Integrating Military and Contractor Personnel: One of our goals is to build an “all-source” workforce that integrates and optimizes our mix of civilian, military, and contractor personnel. We have partnered with Under Secretary of Defense for Intelligence to begin development of a military manpower annex to the strategic human capital plan that will provide a framework for establishing requirements and metrics for military personnel assigned to NIP components. We have also completed the first-ever inventory of “core” contractor personnel who work in direct support of the IC, and now require IC elements to collect and report data on those contractors annually. At the same time, we are exercising better oversight of our contractor workforce by establishing guidelines and accountability mechanisms to ensure contractors are employed appropriately. We are also seeking legislative relief from civilian end-strength ceilings, insofar as those ceilings have forced us to contract for work more effectively done by U.S. Government civilians.
- k. (U) Senior Leadership Accountability: While there are mechanisms in place to align agency strategic and performance plans with National Intelligence Strategy (NIS) objectives, there was no process to hold the heads of those agencies personally accountable for achieving them. To remedy that, the DNI has begun requiring each of the heads of IC elements to sign a Personal Performance Agreement with him, describing specific results that are demonstrable and measurable, contribute to the overall NIS, and represent a “stretch” for senior leaders. In addition, the DNI has asked the heads of IC elements to review and revise as necessary the annual performance plans for their senior executives and professionals to ensure that they too align with the NIS.

- i. (U) Employee Climate Survey: To measure the pace of progress and reform in the IC, the DNI now conducts annual IC-wide employee climate surveys; beginning in 2005, and again in 2006 and 2007, those surveys gauge the quality of our work environment and the morale of our workforce. Based on results of the 2006 survey the “state” of the IC workforce is positive. Overall job satisfaction is high – higher than the average for the rest of the federal government – but there is still room for improvement. For example, most IC employees have trust and confidence in their supervisors, but look for stronger leadership from senior leaders. Based on these survey results, the DNI is addressing a number of issues identified by our employees (such as quality of leadership and supervision, information sharing, and performance management), and each IC agency head has been directed to take additional concrete steps to address specific concerns raised by their own employees. In addition, we developed and implemented a standard exit survey for all IC employees to learn about their experience in the IC and their reasons for leaving.
- m. (U) Corporate Recruiting: We have established a centrally-funded IC “corporate” recruiting strategy, executed annually by multi-agency recruiting teams that travel to target campuses, professional conferences, and other events to reach high-quality candidates. We have also deployed an IC recruiting Web site that is being upgraded with resume intake capability. In addition, for the first time, we established an IC-wide resume-sharing database that allows all IC agencies and elements to share and consider highly qualified applicants, even though they only may have applied to a single agency.
- n. (U) IC-wide Benefits Programs: Competitive benefits are an important part of the IC’s recruiting and retention equation. We must do everything we can to provide our employees with benefit options that address our unique requirements and build a sense of community. Last year, the DNI extended the CIA’s innovative Compass Rose health insurance program to all IC civilian employees, as well as access to Compass Rose’s complementary life, accident, income replacement, and long-term care coverage plans this year. This year we extended to all IC civilian employees the FBI’s Special Agents Mutual Benefits Association Health Benefits Plan, as well as a number of their supplemental insurance plans, and additional supplemental insurance programs provided by NSA’s Government Employee Benefit Association.
- o. (U) The National Intelligence Reserve Corps: The DNI now has a program for retaining critical knowledge and talent in the IC. Pursuant to Section 1053 of IRTPA, we established the National Intelligence Reserve Corps (NIRC) that allows us to re-employ retired IC professionals, without financial penalties, to augment the workforce. Normally, re-employed annuitants suffer a financial penalty, and as a consequence, most come back to us as independent contractors.

(U) There had never been---until the ODNI’s creation---a comprehensive, IC-wide human capital strategy vectoring all of the IC’s agencies and elements in a single direction, nor has there ever been a coordinated, cohesive set of common program and policy initiatives designed to achieve the ambitious goals outlined in that strategy. There is a clear consensus amongst the IC’s senior leadership that an integrated, IC-wide approach to human capital management can leverage scarce financial and human resources, while still accommodating the unique needs and interests of the separate components comprising the IC.

(U) The various personnel authorities (and resultant personnel systems) across the IC do pose a challenge. For example, it is very difficult to foster a sense of community through such initiatives such as civilian joint duty when pay and benefit systems may be substantially different. However, we believe that the initiatives described above, once fully implemented, will provide the necessary framework for managing the IC workforce.

(U) The statutory DNI personnel authorities are limited and ambiguous. It has been through the strong commitment, common vision, and good faith efforts of the current ODNI leadership and the IC that we have been able to make significant progress towards meeting the spirit and goals of the IRTPA. However, as many of the successes to date are dependent upon senior leaders who share a common vision for the IC, the basis for continued progress is fragile.

Hearing Date: September 10, 2007
Committee: HSGAC
Member: Senator Voinovich
Witness: Director McConnell
Question: 3

Question 3: (U) Having held four hearings on improving our security clearance process, I was encouraged by your inclusion of security clearance reform within your 100 Day Plan. Reform of the security clearance process has been on GAO's High-Risk List since 1990 because it severely limits the ability of our national security agencies to meet their mission requirements. Despite the reforms enacted as part of the Intelligence Reform and Terrorism Prevention Act, our current system remains broken, with individuals waiting an average of 203 days for their clearance. Director McConnell, when will individuals awaiting clearances begin to see the results of your recently announced plan?

Answer: (U) The 100 Day Plan improvements issued by the Office of the Director of National Intelligence focused on both the high-risk applicant programs and broader security clearance reform across the Intelligence Community (IC) and at the national level.

(U) In evaluating our high-risk applicant programs, our goal was to improve the process for people who probably would not be considered for clearances under the existing system, to include first and second generation Americans. While many of the long-term recommendations were carried forward into the 500 Day Plan, several short-term recommendations are expected to have near-term benefits. One such recommendation includes a policy change for those individuals with immediate family members who are not U.S. citizens. Under the current system, those individuals require a waiver, while the new policy will leverage the existing decision process for foreign influence issues. We fully expect the short-term outcome of this policy change to result in more applications from high-risk applicants, a more streamlined security clearance process, and a more robust mission capability within the IC.

(U) The broader security clearance process improvements cited in the 100 Day Plan provide for a new, validated proof of concept proposal for the development of an alternative security process. This alternative process concept was developed by the Joint Security Clearance Process Reform Team, and approved by the Under Secretary of Defense for Intelligence and myself on August 28, 2007.

(U) The Security Clearance Reform team is currently executing a series of demonstration projects to validate the key innovations that comprise the transformed process. The primary innovation driving the transformation is the use of new technologies that significantly reduces processing times across the security clearance lifecycle by eliminating manual, time-intensive processes. Given the importance of the security clearance process in controlling access to information that affects national security, the demonstration projects will assess these new technologies for their ability to reduce processing times without compromising rigorous standards for those who hold security clearances.

(U) The demonstration projects will be conducted through March 31, 2008 after which we will incorporate the results of the demonstrations and adjust the process accordingly. In parallel with the demonstration projects, the Security Clearance Reform team is identifying and recommending relevant policy, statute and executive order changes to enable the transformed security clearance process. I am confident that sufficient executive commitment exists to ensure these changes will be made to enable full deployment.

(U) Once the policy changes are in place, we expect components of the new process to start benefiting applicants as soon as 2008, with full end-to-end implementation across the U.S. Government to follow. The joint team will make every effort to deploy improvements as they become available, but understand that end-to-end transformation will take time across the Government.

Hearing Date: September 10, 2007
Committee: HSGAC
Member: Senator Voinovich
Witness: Director McConnell
Question: 4

Question 4: (U) In January, the Subcommittee on Oversight of Government Management held a hearing to assess the federal government's ability to recruit and train skilled translators and linguists to meet our national security needs. What do you believe is the chief obstacle to achieving a higher level of foreign language proficiency in this country, particularly in critical, less commonly taught languages? I read with great interest the description in your written testimony of the work your office is doing to recruit individuals with critical language skills. Could you share with me the number of critical language positions you have filled?

Answer: (U) The chief obstacle to achieving a higher level of foreign language proficiency in the United States, particularly in critical, less commonly taught languages, is the lack of adequate financial, institutional, and social support for foreign language education in our schools and colleges. In addition, skills in many such languages are not seen as a marketable commodity, since there are relatively few jobs for these skills, even in the Intelligence Community. In general, translators and linguists are not generally viewed as a high-prestige, high-wage professions, especially considering that achieving high levels of language proficiency requires many years of continuous study. Much of the available instruction is provided in private weekend schools for heritage speakers, children of immigrants, who want to learn the languages of their ancestors.

(U) Moreover, for critical, less commonly taught languages, there is a severe shortage of qualified teachers, curricula, standards, teaching materials, and standardized tests. In addition, there are few states which have certification programs for teaching these critical languages, making it very difficult to place teachers in schools at the pre-college level. It is extremely difficult for even an experienced teacher from overseas to achieve certification to teach in U.S. schools, because we have so few certification programs. This is true even in major languages such as Chinese and Arabic, which are beginning to draw larger numbers of students.

(U) To address the immediate need for critical language skills, the Intelligence Community (IC) is focusing on increasing recruitment of native and heritage speakers, through enhanced outreach to heritage communities and streamlining security practices to ease the clearance process. We also support such programs as the National Security Education Program, including the National Flagship Language Program, and English for Heritage Speakers program. These programs have been successful in training U.S. students and heritage speakers to high levels of proficiency in critical languages, and improving the English language skills of highly-educated native speakers.

(U) To address the long-term need to improve foreign language proficiency in critical languages in the United States, the major national program underway is the President's National Security Language Initiative (NSLI), launched in 2006. In this effort the Office of the Director of

National Intelligence (ODNI) is partnering with the Departments of Education, State, and Defense to expand existing programs and develop new programs that will greatly expand education in critical languages. For example, the ODNI-sponsored STARTALK program, a new initiative under NSLI, began its pilot program this year, which provided training to 448 teachers and 872 high school students in Chinese and Arabic in summer programs in 21 states and the District of Columbia. Most of the teacher participants were high school teachers, who typically have 100-150 students, so the total impact of this pilot year would be improved instruction to as many as 40,000 students in the coming years. Pending programmed funding, STARTALK is expected to grow to a nationwide program in all 50 states by 2011, and will expand to include students from K-16 in a broader range of critical languages.

(U) In addition, ODNI will be launching a new program of funding hiring of persons with critical language skills on temporary billets in 2008 in order to retain top talent and get them into the system while awaiting clearance or availability of a permanent billet in an appropriate agency. Up to 30 new hires may be hired in the pilot program this year.

Hearing Date: September 10, 2007
Committee: HSGAC
Member: Senator Voinovich
Witness: Director McConnell
Question: 5

Question 5: (U) How are you coordinating with other federal agencies on best practices for recruiting, training, and retaining language proficient individuals? What challenges remain?

Answer: (U) The DNI Foreign Language Program Office (FLPO), leading a collaborative interagency team under the Foreign Language Executive Committee (FLEXCOM), has written a comprehensive Foreign Language Human Capital Plan for the Intelligence Community (IC). This plan has more than 60 action items and addresses recruiting, training, career development, retention, and other relevant subjects, as well as gathering requirements, planning, and development of performance metrics from a community perspective. The plan includes establishment of an integrated team approach to recruiting which maximizes resume sharing, and use of technology to improve resume sharing, hot-linking to component Web sites and language screening tests for applicants. The plan also calls for strengthening training and career management plans for personnel with linguistic and regional expertise, and establishing a foreign language component of the IC career development framework to improve retention. The plan is in the final stage of formal coordination and the key elements of the plan have already been endorsed by all IC agencies.

(U) Although the Foreign Language Human Capital Plan has not been formally implemented, collaborative recruiting and resume-sharing efforts are already underway. About 1,300 resumes obtained in diversity-themed recruiting events and through direct applications in FY 2007 were made available to recruiters in all the IC agencies for review and potential hiring on a password-protected website. About 82 of those resumes were designated as possible language analyst or linguist candidates. Additionally, a significant number of the other resumes obtained from these recruiting activities indicated native language speaking ability, language coursework and/or study abroad experience.

(U) In addition, the IC Chief Human Capital Office hosted a Heritage Summit in June 2007 with broad IC participation, to share best practices and develop recruiting strategies for Americans from heritage communities who have critical language skills. The DNI is also modernizing security clearance processes to speed up the hiring process, which should ease accession of those from heritage communities with critical languages skills as well as those who have spent significant time overseas.

(U) The DNI CHCO actively works with the National Security Education Program, which sponsors students in study abroad and language-intensive training, to showcase their programs at meetings of the Intelligence Community Recruitment Subcommittee composed of recruiters from all the IC agencies.

(U) Building a qualified workforce with the linguistic skills needed by the IC requires a long-term commitment. Hiring by itself does not always keep up with attrition or rapid changes in target sets, particularly in the least-commonly-taught languages. This is largely due to the difficulty of identifying and recruiting appropriate applicants with the required skills. Where hiring does not keep pace with attrition, NSA re-balances the language workforce through cross-training or pursues other options, such as contracting or resource-sharing with partners, to acquire adequate capability.

Hearing Date: 10 Sept. 2007
Committee: SHSGAC
Member: Sen. Lieberman
Witness: VAdm Scott Redd

Question: Much of your testimony focused on the National Implementation (NIP) for the War on Terrorism, describing how it has been implemented and adopted over the past year. Testimony from the hearing attested frequently to the importance of state and local law enforcement in fighting terrorism; FBI Director Mueller testifying that “local police officers on the streets are the frontline of the war on terrorism.” Does the National Implementation Plan address the responsibilities of state and local law enforcement? If so, would it be possible to develop an unclassified version of the NIP, to allow these key non-federal stakeholders to become familiar with parts of the plan that are relevant to their work?

Answer: The National Implementation Plan (NIP) does provide strategic direction with an implicit role for state and local law enforcement but assigns lead responsibility for such tasks at the Federal level in order to leverage the existing working relationships between Departments/Agencies and state/local partners and avoid any duplicative process that might result in unclear or conflicting objectives. To that end, we understand the vital role performed by state and local law enforcement and must continue to formally evaluate the efforts of Departments/Agencies to ensure the relationships between all elements of the CT community are helping achieve the objectives outlined in the NIP.

Although the decision to provide an unclassified version of the NIP to key non-federal stakeholders resides with the White House, we expect Departments/Agencies to share relevant parts of the plan with state/local partners at an appropriate level of classification.

Hearing Date: 10 Sept. 2007
Committee: SHSGAC
Member: Sen. Lieberman
Witness: VAdm Scott Redd

Question: In describing the U.S. government's efforts in the battle of ideas, you testified that "Countering Violent Islamic Extremism" (CVIE) is one of the four "key pillars" in the National Implementation Plan (NIP) for the War on Terrorism. Your written testimony states that the planning phase of the NIP is complete, and is now in the process of implementation across the interagency. In response to a subsequent request for a briefing on CVIE, NCTC indicated that the NIP as a whole is currently under review. Please explain the current status of development for the CVIE portion of the NIP. Has CVIE been fully developed to the level of detail whereby specific tasks are assigned to government agencies and departments for implementation? Does the NIP identify the need for a counter-narrative to the extremists' message, and if so, what is that counter-narrative? In addition to the Department of State, which you testified is responsible for 30% of the tasks, does CVIE assign tasks to agencies with domestic responsibilities? Please describe the status of the implementation of this strategy at the agencies who have been assigned responsibility, as well as the status of measures to assess the success of the strategy.

Answer: The CVIE portion of the NIP has been developed to the point that tasks are assigned to government agencies for implementation. This month, NCTC began its internal effort to consider possibilities for refining and updating those tasks so that interagency coordination and synchronization of USG counter-radicalization activities under the NIP's CVIE pillar might be better integrated. These activities are wide-ranging, often multi-faceted and sometimes neither wholly domestic nor entirely international. This process of refining and updating might also consider how to associate measures of effectiveness with tasks. The Department of State-led Counterterrorism Communications Center (CTCC) dynamically develops and promulgates counter-narratives to extremist messages. Domestic agencies do have NIP responsibilities for countering radicalization within the United States. In response to the direction of the NSC and the HSC, NCTC has identified a need to coordinate, integrate, and synchronize the efforts of the USG, particularly the FBI and DHS, to reach out to community leaders of religious and ethnic minorities across the nation, and to foster a dialogue of mutual understanding. NCTC has worked with DHS and FBI to develop and propose mechanisms to accomplish this objective, and these proposals are ready for NSC/HSC approval.

Hearing Date: 10 Sept. 2007
Committee: SHSGAC
Member: Sen. Tester
Witness: VAdm Scott Redd

Question: Admiral, your testimony refers to the establishment of an NCTC-run electronic library. Is this information accessible to intelligence analysts in countries that are friendly to the United States? Do the documents in this library include multi-media documents such as video, audio and cached Internet websites?

Answer: NCTC has not established an electronic library such as is being created by the ODNI. NCTC maintains within its NCTC On-Line (NOL) system a significant collection of critical electronic records relating to counterterrorism. This collection of over 8 million documents contains classified information of direct and significant relevance to the Counterterrorism Community. The system is fully capable of supporting and storing multi-media content.

NOL is available at multiple levels of classification, with the appropriate documents for that level of classification being available on each network. While these documents are accessible and searchable by personnel with the appropriate clearance levels, NOL does not have the full capability provided by the enhanced library services such as those proposed under the ODNI National Digital Intelligence Library Program. NCTC does electronically share NOL information with friendly foreign partners.

Hearing Date: 10 Sept. 2007
Committee: SHSGAC
Member: Sen. Voinovich
Witness: VAdm Scott Redd

Question: How are you coordinating with other federal agencies on best practices for recruiting, training, and retaining language proficient individuals? What challenges remain?

Answer: NCTC is in constant contact with other federal agencies to include the CIA, State Department and the ODNI to learn and then share the best practices for the following:

- Selecting language training candidates who are most likely to succeed.
- Continually monitoring progress in language training programs.
- Ensuring that the instructors use established rigorous teaching methods.

Further, NCTC's Directorate of Intelligence is nearing completion of the creation of an on-site pilot program in both Arabic and Persian (Farsi as well as Dari, the Persian dialect spoken in Afghanistan). The program is designed to offer part-time basic language and cultural familiarization training for employees assigned to NCTC. NCTC is planning to have native-proficiency language instructors available to maintain and improve capabilities of persons at NCTC who have had formal training in their home agency or other language experience.

To recruit individuals with heritage language skills, NCTC Training has established a relationship with Georgetown University's *English for Heritage Language Speakers* --a program that immerses heritage language speakers into English instruction --writing, speaking, reading, and listening--six hours a day--five days a week-- for six months. Students who have completed the program have averaged a 3+ in English in all the skills, which would enable them to be significant contributors as Intelligence Community employees.

The ODNI has implemented a Foreign Language Incentive program to reward employees who have foreign language skills at the 3 level of proficiency. A number of NCTC analysts have also registered for sponsored external language training to maintain their skills.

The biggest challenge that remains is implementing a cost effective dual-track language training program--one to establish language skills, the other to maintain the high level of skill some of our employees currently have.

**Responses of the Federal Bureau of Investigation
Based Upon the September 10, 2007 Hearing Before the
Senate Committee on Homeland Security and Governmental Affairs
Regarding “Confronting the Terrorist Threat to the Homeland:
Six Years After 9/11”**

Responses to Questions from Mr. Mueller

Questions Posed by Chairman Lieberman

1. In your testimony, you acknowledged that the US does have a problem of homegrown Islamist radicalization. What programs has the FBI initiated or plans to initiate through the Office of Law Enforcement Coordination or through another office to assist state and local law enforcement with addressing the problem of homegrown Islamist radicalization? In addition, how receptive have state and local law enforcement agencies been to offers of assistance to address this problem?

Response:

The FBI has a total of 59 Community Outreach Specialists in the Community Outreach Program (COP). This includes 30 full-time and 29 part-time professional support employees, 5 percent of whom have relevant foreign language skills. The COP also includes four FBI Special Agents who serve as Community Outreach Coordinators in support of the COP. The COP is overseen by a unit in the FBI’s Office of Public Affairs that has a funded staffing level of nine.

Each of the FBI’s 56 FBI field offices has a COP responsible for developing close working relationships with the state and local law enforcement agencies in their territories, and state and local partners frequently participate in the FBI’s outreach programs. In addition, there is a Joint Terrorism Task Force (JTTF) in each FBI field office. These JTTFs, which include representatives from state and local law enforcement agencies, consult those in their COPs for guidance regarding various ethnic and minority cultures.

In addition, the FBI participates in four Federal inter-agency working groups that are collectively addressing the spread of Islamist extremism in the United States.

- The FBI, the Federal Bureau of Prisons, others in the Department of Justice (DOJ), the Department of Homeland Security (DHS), the

Department of the Treasury (Treasury), and the Department of State (DOS) participate in an inter-agency Federal working group that meets monthly to discuss the spread of Islamist extremism in the United States and how to counter it.

- Along with DHS, DOS, Treasury, the United States Agency for International Development, and the Department of Health and Human Services, the FBI participates in a Domestic Engagement working group that meets regularly to identify strengths, weaknesses, and best practices for each government agency's community engagement efforts.
- An Incident Management team, consisting of the FBI, DOJ, DHS, and national leaders from the Arab-American, Muslim, Sikh, and South Asian communities, was established to resolve issues that arise in the aftermath of incidents in local communities. The group convenes by way of telephone conference call after an incident and, if an incident warrants, meets in person.
- DOJ's Assistant Attorney General for the Civil Rights Division hosts an interagency meeting with community leaders approximately every two months to address civil rights concerns and to connect leaders with the agencies able to help remedy problems.

These working groups are an excellent means of offering and receiving guidance and advice regarding the effectiveness of community outreach programs. In addition, there is a constant dialogue and information flow among government agencies regarding issues that arise to ensure the efforts of the relevant Federal agencies to address these communities' concerns are not in conflict. For example, the FBI has consulted with DHS to address concerns raised by the American-Arab Anti-Discrimination Committee regarding delays in processing name checks, has worked closely with DOJ's Civil Rights Division regarding post 9/11/01 civil rights violations, and has involved Treasury in meetings with Arab-American community leaders regarding Islamic charity fund raising.

FBI Headquarters (FBIHQ) conducts outreach on the national level and provides guidance to the field to assist them in their outreach on the local level. This guidance allows field offices to adapt their programs to address the demographics of their territories, and it is the responsibility of the Special Agent in Charge to ensure the field office is engaging in appropriate community outreach. Each field office is encouraged to establish relevant advisory committees and to conduct

other outreach activities, such as Citizens' Academies, Community Relations Executive Seminar Training (CREST), town hall meetings, and youth programs.

Each field office must submit to FBIHQ a detailed semi-annual accomplishments report identifying the types of community outreach conducted in the past six months. The report uses a detailed question and answer format and requires a list of existing and newly developed partnerships with various ethnic and minority organizations and community leaders. The report also discusses the various outreach activities that occurred during the evaluation period, such as Citizens' Academies, CREST, town hall meetings, and youth programs, all of which strengthen community relations, improve the trust between the FBI and the community, and ultimately contribute to the FBI's overall mission success. In response to the semi-annual accomplishments report, FBIHQ replies to the Special Agent in Charge, recognizing field office accomplishments, identifying any areas of concern, and recommending ways to improve the COP, if appropriate.

2. Important strides are being made in creating the capacity for information sharing between levels of government. The FBI has its Joint Terrorism Task Forces and the Field Intelligence Groups; DHS is spurring the development of state and local Fusion Centers; numerous ports have maritime interagency operations centers; and states have their own Emergency Operations Centers. What is the FBI doing to ensure that all these efforts are collaborative and integrated, rather than duplicative, or worse - disconnected? What role is the federal government playing in ensuring that each entity has discrete roles and responsibilities, and is receiving the information it needs to perform its functions within the overall Information Sharing Environment?

Response:

On 11/14/06, the Office of the Director of National Intelligence (ODNI) submitted to Congress the Implementation Plan Report for the Information Sharing Environment (ISE), which serves five communities: intelligence, law enforcement, defense, homeland security, and foreign affairs. For information sharing at the Federal level, the ISE Implementation Plan calls for greater coordination so that strategic and time-sensitive threat information gets to those who need it. Key elements are a national management structure, architecture, and standards. FBI roles include the following.

- The Assistant Director for the FBI's Directorate of Intelligence (DI) is a full member of the ISE Information Sharing Council, which is chaired by the ISE Program Manager (PM).

- The FBI's Office of the Chief Information Officer (OCIO) develops and implements plans for the ISE Enterprise Architecture Framework and Common Terrorism Information Sharing Standards, consistent with the DOJ and Intelligence Community (IC) architectures and standards.
- The FBI's National Security Branch (NSB) combines the FBI's intelligence, counterterrorism, counterintelligence, and weapons of mass destruction resources, making the FBI a preeminent domestic intelligence agency. The NSB shares information with the other U.S. intelligence agencies through secure communications and the Intelink network.
- The FBI has assigned Special Agents and analysts to the National Counterterrorism Center (NCTC), which analyzes all intelligence pertaining to terrorism. The FBI's Counterterrorism Division is co-located with the NCTC and the CIA's Counterterrorism Center.

For information sharing with state, local, and tribal governments, the ISE Implementation Plan provides for a network of state and regional fusion centers that communicate, cooperate, and coordinate with each other and with the Federal government. In 2006, the FBI provided the ISE PM with an enterprise architecture report on 39 FBI programs related to the ISE (29 Unclassified, 10 Secret). The FBI followed up with briefings by senior representatives of the FBI's NSB, the Science and Technology Branch, the OCIO, and PMs of numerous programs related primarily to the ISE Implementation Plan.

The Field Intelligence Groups (FIGs) are the FBI's primary component for receiving and disseminating information. They complement the JTTFs and other squads and task forces. The FIGs play a major role in ensuring that we share what we know with our IC and law enforcement partners, sharing information with law enforcement partners through fusion centers. State Fusion Centers and other Multi-Agency Intelligence Centers have become a focal point of information exchange and relationship building, and the FBI is committed to participating in these centers as resources permit. We have identified 42 states with designated State Fusion Centers in varying stages of development, some of which are co-located with the FBI's FIG and local JTTF. A total of 260 FBI personnel are assigned to 32 of these centers, and we are assessing the remaining 10 centers for the assignment of FBI personnel. In addition to supporting the State Fusion Centers, the FBI is also participating in 10 select Multi-Agency Intelligence Centers throughout the country.

In addition to these efforts, the FBI shares classified intelligence and other sensitive FBI data with Federal, state, and local law enforcement officials who participate in the JTTFs, which are important force multipliers in the fight against terrorism. Since 9/11/01, the FBI has increased the number of JTTFs from 35 to 102 nationwide. We have also established the National Joint Terrorism Task Force (NJTTF) at FBIHQ, staffed by representatives from 38 Federal, state, and local agencies. The mission of the NJTTF is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of counterterrorism operations.

In August 2007, the FBI's Counterterrorism Division hosted the fiscal year 2007 JTTF National Training Conference in Dallas, Texas, which was attended by approximately 550 Federal, state, and local JTTF members representing 40 Federal and 80 state and local agencies. The FBI continues to increase representation on the NJTTF; as of September 2007, the NJTTF consisted of 44 Federal, state, and local representatives.

Questions Posed by Senator Voinovich

3. How are you coordinating with other federal agencies on best practices for recruiting, training, and retaining language proficient individuals? What challenges remain?

Response:

The Chief of the FBI's Language Services Section serves as the FBI's Senior Language Authority (SLA) and is a member of the ODNI's Foreign Language Executive Committee (FLEXCOM). The FLEXCOM's SLAs formulate the strategic direction of the ODNI's Foreign Language Program and routinely collaborate on best practices and foreign language/cultural challenges facing the IC. FBI experts also participate in the four groups of experts that report to the FLEXCOM: Training, Testing, Operations, and Technology. These four groups meet regularly to enable subject matter experts from each IC component to exchange ideas and brainstorm responses to complex foreign language issues.

The IC foreign language community routinely shares resources. Through liaison efforts, the FBI has gained translation and interpretation support, foreign language training and testing, and other assistance, while providing similar support to other agencies.

The recruitment of qualified language applicants has resulted in an 81% increase in our Language Analysts and Contract Linguists since 9/11/01 (from 784 to 1419). The FBI is working with ODNI to address recruiting and retention challenges to ensure that the FBI's recruitment and retention programs and incentives offer parity with others in the IC.

4. I know that your agency has developed a program called the Intelligence Officer Certification Program, to train and certify intelligence professionals. Acknowledging that this program is relatively new, could you describe benefits noticed by your agency and any changes you see in the future to strengthen training? Is there any ability to allow analysts from other components within the Intelligence Community to train in your programs?

Response:

The FBI's Intelligence Officer Program was established in 2004 to develop intelligence professionals in the FBI. Through this program, the FBI and other IC members provide to FBI participants a wide variety of opportunities, addressing the FBI's special responsibilities while aligning with the larger IC's Intelligence Officer Program. Among the benefits recognized to date are the following: 1) increased interest in obtaining intelligence training; 2) increased desire to broaden intelligence experiences through temporary duty assignments and joint duty assignments, both domestic and international; and 3) the development of a pool of recognized intelligence professionals available to mentor, teach, and provide their expertise as needed. A planned comprehensive review of the purpose and implementation of this program will assess how well the program meets the needs of both the FBI and the larger IC.

Although the FBI's Intelligence Officer Program is currently designed specifically for FBI employees (those in other agencies cannot seek certification as FBI Intelligence Officers), FBI-sponsored courses are available to other IC personnel through the Intelligence Community Officer Training Program. Examples of courses offered to other IC members include the following.

- Intelligence Basic Course (IBC) - In collaboration with the FBI's Training Division, our DI is currently redesigning the entry-level course for new analysts. The IBC emphasizes the three tradecraft skills (thinking, expository writing, and briefing) critical to an analyst's professional success. The FBI piloted this course in June 2007 and has recently run this course a second time. The curriculum has been constructed in modules that can be used in various combinations to provide tailored training to

field offices or groups of field offices. The FBI anticipates allowing IC participation in the next IBC course offered.

- Managing Analysis Course - In coordination with the Training Division, the DI piloted this course in August 2006 and has continued to offer it throughout 2007. This course was developed to enhance the effectiveness of those responsible for supervising analysts, many of whom are not analysts themselves. Feedback continues to be positive, and we are making adjustments to optimize the value of the course. Since its inception, we have offered this course to our Federal, state, and local partners.
- Advanced Analyst Program - This series of classes is an IC program designed for analysts with four or more years of experience. The curriculum is designed to deepen tradecraft skills and advance the profession of intelligence. As developed, this program requires that 25% of the seats in each class be reserved for analysts from other IC agencies.

Questions Posed by Senator Domenici

5. Director Mueller, as you know, my constituents have to deal with the daily problems associated with the international border that include drug smuggling, destruction of property, and the like. In July, new concerns were raised in New Mexico when news outlets alleged the existence of a human smuggling operation in my home state of New Mexico that focused on smuggling individuals from the Middle East into the United States through Mexico. I am proud of our recent efforts to improve border security by putting thousands of new border patrol agents on the ground as well as providing new border security technologies and other border assets, but I found this news story extremely alarming. At this time, can you provide us with any information about this matter?

Response:

For several years now the FBI has received reports about illegal operations in the southwest, alleging that alien smuggling organizations are smuggling individuals from the Middle East into the United States. Often such reports are passed from agency to agency, resulting in circular reporting. The information you refer to can best be described as "raw intelligence," which forms the basis for additional inquiry but is not sufficiently verified or developed to form the basis for responsive action.

This past summer, the FBI received information alleging alien smuggling activity in southern New Mexico. The FBI's Albuquerque Division properly disseminated this intelligence in the form of an Intelligence Information Report (IIR), which was then distributed by FBIHQ to numerous governmental agencies. Unfortunately, this IIR was subsequently "leaked" to a press outlet, resulting in the exaggerated media attention you described.

The FBI takes all such allegations seriously and has initiated a criminal investigation to assess the accuracy of the intelligence, as well as the reliability of the information. The FBI's Albuquerque Division is working closely with DHS in southern New Mexico to ascertain the facts so appropriate responsive action can be taken.

6. This news story was based on a purported FBI intelligence report. What effect do leaked intelligence reports have on ongoing FBI investigations?

Response:

The "leaking" of FBI intelligence to the media can adversely affect ongoing criminal investigations, resulting in the loss of potential evidence, exaggerated media attention, the possibility that Special Agents, witnesses, and sources may be compromised or endangered, and the possibility that subjects of the investigation may flee before arrest. In addition, if intelligence is "leaked" and the FBI later determines that there was no factual basis on which to open a criminal investigation, the leak can permanently damage the reputation of the individual or group that was the subject of the leak.

7. What do you need from Congress to further the FBI's efforts to end human smuggling and secure our nation's borders?

Response:

The administration worked with Members of Congress last year in an attempt to pass comprehensive immigration reform. That package included new statutory tools that would have enhanced our enforcement efforts.

These responses are current as of 10/26/07

