S. HRG. 111–616

# SECURING AMERICA'S SAFETY: IMPROVING THE EFFECTIVENESS OF ANTITERRORISM TOOLS AND INTERAGENCY COMMUNICATION

## HEARING

BEFORE THE

## COMMITTEE ON THE JUDICIARY
## UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JANUARY 20, 2010

**Serial No. J–111–71**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

58–484 PDF WASHINGTON : 2010

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 THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware
ARLEN SPECTER, Pennsylvania
AL FRANKEN, Minnesota

JEFF SESSIONS, Alabama
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATT MINER, *Republican Chief Counsel*

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS



## WITNESSES



## QUESTIONS AND ANSWERS



## SUBMISSIONS FOR THE RECORD

# SECURING AMERICA'S SAFETY: IMPROVING THE EFFECTIVENESS OF ANTITERRORISM TOOLS AND INTERAGENCY COMMUNICATION

**WEDNESDAY, JANUARY 20, 2010**

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:10 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Kohl, Feinstein, Feingold, Schumer, Cardin, Whitehouse, Klobuchar, Kaufman, Franken, Sessions, Hatch, Grassley, Kyl, and Coburn.

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

Chairman LEAHY. Good morning. I think before we start on this hearing, every one of us has to be moved by what we have seen on television or people we have talked with during the past couple weeks in Haiti. And if I could, with the indulgence of my colleagues, wearing another hat that I have as Chair of the Appropriations Subcommittee that handles our foreign aid, I have been particularly interested in what has been happening. I have had talks with people on the ground in Haiti and others who have gone down there, and I want to begin by thanking President Obama, Secretary of State Hillary Clinton, USAID Administrator Shah, General Fraser of the U.S. Southern Command, and all the hard-working people here and on the ground in Haiti for their efforts to save lives in the aftermath of this devastating earthquake.

A number of States—I know California sent search and rescue, Virginia did, and others. My own little State of Vermont is sending down a medical team today. Recovering from this disaster is a daunting challenge for the people of Haiti, but Vermonters and all Americans have opened their hearts and are sharing generously. We will continue to do so. Any one of us just as human beings have to be moved by what we have been seeing down there.

Now to the subject of this important hearing. A terrorist intent on detonating an explosive was able to board a plane with hundreds of passengers headed for Detroit, Michigan, on Christmas Day. After Congress passed major legislation in 2004 to implement the 9/11 Commission's recommendations, and after the country invested billions of dollars to upgrade security systems and to reorga-

nize our intelligence agencies, the near tragedy on Christmas Day compels us to ask what went wrong and what additional reforms are needed.

The administration responded quickly and has already conducted a preliminary review. The President has candidly identified problems. He spoke directly to the American people about the incident, the threat, and the actions that are necessary to prevent future attempted attacks. They did not offer excuses, but instead they have taken responsible action to provide additional security measures.

I know there will be some hard questions at this hearing. We will want to know how and why we failed to successfully detect and prevent this attempted attack. How did someone who paid for an airline ticket with cash, who boarded without luggage for a winter trip to Detroit, and whose father had come to U.S. officials weeks before to warn that his son had become radicalized, how was he able to board a flight for the United States with a valid visa? Just as we now know the horrific, deadly attacks on 9/11 could have been prevented, should have been prevented, the recent White House review found that the Government "had sufficient information to have uncovered and potentially disrupted the December 25 attack." Our intelligence agencies did not adequately integrate and analyze information that could have prevented this attempt. The President called it a "systemic failure," and he is right that this is unacceptable. Just as we failed on 9/11, we failed here.

Now, I would hope that all Senators here ask whatever questions they feel they should, but I hope we proceed with the shared purpose of making America safer. No one has been angrier or more determined than the President. He did not respond with denial and obfuscation, but instead came forward to identify failures and correct them.

Let this not be a setting where we are looking for partisan advantage. We are all Americans; we are all in this together. Every one of us as members and virtually everybody in this room fly often. "Passions and politics" should not obscure or distract us. We should all do our part. As the President said recently in announcing the immediate actions he had ordered: "Instead of giving in to cynicism and division, let's move forward with the confidence and optimism and unity that define us as a people. For now is not a time for partisanship, it's a time for citizenship—a time to come together and work together with the seriousness of purpose that our National security demands."

I was here after 9/11. I saw Republicans and Democrats come together to work together with the President to find out what went wrong and to make sure it did not happen again. That is what we need to do today.

Our witnesses today are public officials. They are not adversaries. They each share with us a common purpose, as the President said, "to prevail in this fight...to protect our country and pass it—safer and stronger—to the next generation."

In the aftermath of the Christmas Day plot as well as the Fort Hood tragedy, it can be tempting to forget that it is always easier to connect the dots in hindsight. It was not our intelligence agencies that first raised the alarm about the suspect who tried to blow up the Northwest Airlines flight. It was the suspect's own father,

a Nigerian, who turned him in. Our response to the incident has to be swift but also thoughtful. It may be tempting to take reflexive actions, but to do so will only result in the unnecessary denial of visas to legitimate travelers and the flooding of our watchlists such that they become ineffective tools in identifying those who would do us harm. We want to stop real people who may do us harm, not 8-year-old children.

A "one size fits all" mentality will only ensure that we will miss different threats in the future. We cannot hunker down and hide behind walls of fear and mistrust. We should not let our response to the incident provide another recruiting tool for terrorists, and we have to be smarter than that.

Finally, this morning, the Inspector General released a report a few minutes ago detailing the misuse of so-called exigent letters by the FBI to obtain information about U.S. persons. The report describes how the FBI used these exigent letters without proper authorization to collect thousands of phone records, including in instances where no exigent conditions existed. The report also details how the FBI then compounded the misconduct by trying to issue national security letters after the fact. This was not a matter of technical violations. If one of us did something like this, we would have to answer to it. This was authorized at high levels within the FBI and continued for years. I understand, Director Mueller, that the FBI has worked to correct these abuses, but this report is a sobering reminder of the significant abuse of this broad authority. No one is above the law—no Senator and no member of the FBI. And there has to be accountability for what happened here.

Senator Sessions.

**STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA**

Senator SESSIONS. Thank you, and I would join with you in your comments about the tragedy in Haiti and hope that we in a unified effort in Congress can do all possible to assist in that tragedy.

It was on Christmas Day that America was reminded that the war on terror is still being waged and that our enemies will stop at nothing in their efforts to destroy our country. But for the bravery of passengers and crew aboard Northwest Flight 253 and a defect in the bomb, close to 300 innocent people could have been murdered.

Make no mistake, this was another act of terrorism, another act of war. And now it appears clear that our intelligence officials had gathered enough information to stop Mr. Abdulmutallab from boarding the plane. In reality, it was our enemies' poor bomb-making skills, luck, and the courage of passengers and crew that saved that flight.

The problem arose from a lack of action on available intelligence. Was it the result of policies arising from a hesitation to interfere in one person's travel plans? Or, was it a failure to connect the dots? Was it an individual failure somewhere, or a systemic failure? Perhaps all. It is clear that 8 years after September 11, 2001, there are still holes in our counterterrorism system. Al Qaeda has openly declared war on our country. They have attacked us and are still attacking us. This administration cannot wish that reality

away, and I do not think they intend to. The threat cannot be negotiated away. What we must do is acknowledge this reality and work to both interrupt the attacks and destroy the organizations that are at war with us. It is a different kind of war, but a real war nonetheless.

This hearing can help us get insight into the failures that occurred and what we need to do in the future. But until the administration and Congress fully acknowledges the reality of the enemy, I do not think we will be fully effective. The work of the 9/11 Commission unified our Nation behind the idea that preventing acts of war by traditional law enforcement techniques would not be effective. They declared we should treat this danger with a new understanding of war. The sad truth is that the administration tends to view this conflict wrongly as a law enforcement matter now, retreating from that national decision I thought we reached. Now we have a policy that presumes captured terrorists here and abroad will receive a trial in our civilian courts, be given Miranda warnings, be given court-appointed attorneys, not be subject to interrogations, and have rights to repeated court appearances and speedy trials, regardless of whether they might possess critical information concerning further deadly attacks that might be planned.

This is what civilian trials mean. This is how they are conducted. As Attorney General Holder testified, civilian trials are not required in these cases by the law or the Constitution. And I would note that in no war, to my knowledge, has any nation has ever allowed the enemy to use their own courts to further the enemy's efforts to destroy that nation. This is not a case about whether there were red flags. The terrorist's father personally went to the U.S. embassy to raise a red flag. The would-be attacker bought his plane ticket with cash. He checked no luggage. He reportedly was known to have communicated with terrorists in Yemen. According to press reports, our intelligence agencies intercepted messages referring to "the Nigerian," Mr. Abdulmutallab.

So this case is one where our own intelligence commuity had information. People at risk in the far corners of the globe got valuable information. So we have preliminary information that suggests that the authorities were aware of this terrorist and had ample cause to stop and question him and deny him the right to board that plane.

We cannot defeat al Qaeda through half steps, Miranda warnings, minimization procedures, and Inspector General reports. This is not the time for the Government to erect new barriers between the intelligence and law enforcement agencies. We understood that was a mistake before. Nor is it time to add more bureaucratic red tape, new reporting requirements, or unnecessary safeguards which do nothing more than hinder the ability to thwart the next shooting, the next bombing, the next 9/11.

We should use every lawful power and tool we have to protect this Nation. This war was declared by al Qaeda and its terrorist allies long before September 11th, before Guantanamo Bay. Guantanamo Bay did not cause these terrorist attacks. This war started long before we invaded Afghanistan, before the drone attacks and before the fall of Saddam Hussein. This is a war that began to take shape in the early 1990s when al Qaeda attacked various U.S. fa-

cilities here and abroad. Unfortunately, it is a war which will continue, I have to say, for some time, for some years. And it is imperative that our intelligence and counterterrorism professionals have what they need on the front lines to disrupt the next terror plot and thwart the enemy at every turn.

Rather than putting more bureaucratic hurdles on our intelligence agencies through a weakening of the PATRIOT Act, we should be looking to cut the red tape, strengthen their ability to stop the next airline bomber promptly before he gets a visa or is allowed to board a plane. We need to get this right. I appreciate the willingness of all the administrative witnesses to testify. I especially appreciate the presence of Director Mueller, who took a hard look 8 years ago at some of the warning signs that were missed before September 11th and address the reforms, good reforms, in the FBI. Through his testimony and experience and the testimony of Mr. Kennedy and Mr. Heyman, I hope we will be able to come to a consensus that we must give our investigators the tools and flexibilities they need to prevent further attacks on our country.

Thank you, Mr. Chairman, and I am glad we are having the hearing. I know the Homeland Security Committee, I think, is also having one, and I believe it will help the American people feel that we are responding to the concerns that I know they are feeling.

Chairman LEAHY. Well, thank you, and I think the American people also expect us to work together on responding to these issues.

I am going to ask each witness—I know you have long statements. The whole statement will be placed in the record. I am going to ask you to limit your time to the time that has been suggested to you because, as you can see, we have a lot of Senators, and I want to give every Senator the opportunity to ask the questions they want.

We will begin with Robert Mueller, the sixth Director of the Federal Bureau of Investigation. Prior to that, he had a long and distinguished record at the Department of Justice, including serving as U.S. Attorney for the Northern District of California. Please go ahead.

**STATEMENT OF THE HON. ROBERT S. MUELLER, III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC**

Mr. MUELLER. Thank you, Mr. Chairman, Senators, Senator Sessions in particular. I am pleased to be here today. And before I begin, as did you, Mr. Chairman, I would like to take a moment on behalf of the men and women of the FBI to extend our condolences and support to the people of Haiti and to all of those who have lost family and friends from the devastating earthquake last week. The FBI is providing assistance to the rescue effort, but we are also focused on making sure that fundraising efforts are not tainted by fraud and that we are doing everything possible to ensure that funds raised for the relief in Haiti are legitimately going to support the victims of the earthquake.

Now, let me turn to the subject of today's hearing, if I might. As recent events have made clear, terrorists remain determined to strike the United States. The FBI has transformed itself in recent

years to meet our responsibilities to deter, detect, and disrupt these terrorist threats. We have improved our intelligence capabilities and created the administrative and technological structure needed to meet our national security mission. We are now a full partner in the intelligence community, and we, too, must consistently collect, analyze, and disseminate intelligence to those who need it. As has often been said, today we share information by rule and withhold by exception.

Meeting these threats, however, requires continued vigilance and improvements on the FBI's part and on the part of every member of the intelligence community. Let me take a moment to address the evolving threats we have seen over the past several years.

We not only face the traditional threat from al Qaeda but also from self-directed groups not part of al Qaeda's formal structure. We face threats from homegrown extremists, those who live in the communities they intend to attack, and who are often self-radicalized and self-trained.

We also face threats from individuals who travel abroad to terrorist training camps in order to commit acts of terrorism overseas or to return home to attack America. And these threats continue to change and evolve as extremists are now operating in new sanctuaries around the world as al Qaeda and its offshoots are rebuilding in Pakistan, Yemen, and the Horn of Africa.

While the terrorist threat has not diminished, together with our intelligence community partners we have disrupted a number of plots over the past year. We have learned a great deal from these cases, both about the new emerging threats and how to stop them. Let me offer several examples.

In May, four individuals in New York, some of whom met and were radicalized in prison, were arrested for plotting to blow up Jewish synagogues and to shoot down military planes.

In July, a group of heavily armed extremists in North Carolina were arrested for making plans to wage jihad overseas after traveling to terrorist training camps.

In September, on the eve of September 11th, a Colorado resident was arrested in New York for planning to set off a bomb after having received detailed bomb-making instructions from Pakistan.

That same month, two self-radicalized loners—one in Springfield, Illinois, and one in Dallas, Texas—were arrested for attempting to bomb a Federal courthouse and a downtown office tower in those respective cities.

And weeks later, a Chicago resident was arrested for his role in planning a terrorist attack in Denmark and assisting in the deadly 2008 Mumbai attacks.

And, of course, the killing of a young Army recruiter in Arkansas in May and the tragic shootings at Fort Hood in November are stark examples where lone extremists have struck military here at home.

Last year's cases demonstrate the diversity of new threats we face. Some involve self-radicalized terrorists influenced by the Internet or their time in prison. Others receive training or guidance from known terrorist organizations abroad either in person or over the Internet. And the targets of these attacks range from civil-

ians to Government facilities to transportation infrastructure and to the military both in the United States and overseas.

On Christmas Day, the attempted bombing of Northwest Flight 253 has made it clear that the threat of attack from al Qaeda and its affiliates continues to this day, and we can and must do more in response to these threats.

As directed by the President, the FBI has joined with our partners in the intelligence and law enforcement communities to review our information-sharing practices and procedures to make sure such an event never happens again.

For the FBI, the President has directed a review of the visa status of suspected terrorists on databases at the Terrorist Screening Center and asked for recommendations for improvements to the protocols for watchlisting procedures at the TSC. Together with our intelligence community and law enforcement partners, we will learn from and improve our intelligence systems in response to the Christmas Day attack.

Now, Mr. Chairman, you mentioned the exigent letter issue, and let me address that as well. Let me start off by saying that we take the issues raised by the Inspector General exceptionally seriously, and we have since he first undertook a review a number of years ago. At the outset, it is important to understand that the records obtained were telephone toll records and not the content of conversations. And, second, exigent letters have not been used since 2006.

As I stated in 2007, when the Inspector General first reported on the FBI's use of exigent letters, the FBI had substantial weaknesses, substantial management and performance failures in our internal control structure as it applied to obtaining telephone records. And since that time we first became aware of this, we have reformed our internal controls and developed an automated program that together with changes in policy and training substantially minimizes any errors.

On this issue, I would like to insert one quote from the report that summarizes what we have done since 2006. And the IG states: "It is important to recognize that when we uncovered the improper exigent letter practices and reported them to the FBI in our first NSL report, the FBI terminated those improper practices and issued guidance to all FBI personnel about the proper means to request and obtain telephone records under the ECPA." He goes on to say that that does not excuse—and I agree with him—does not excuse the improper use of exigent letters and the ineffective and ill-conceived attempts to cover them with other NSLs.

Chairman LEAHY. Thank you, and the rest of the statement will be placed in the record. We will probably be going back to this issue during the hearing.

[The prepared statement of Mr. Mueller appears as a submission for the record.]

Chairman LEAHY. Our next witness will be Patrick F. Kennedy, who is Under Secretary of State for Management, a career minister in the Foreign Service. Under Secretary Kennedy oversees the Bureau of Consular Affairs and is the Secretary's principal adviser on management issues.

Mr. Kennedy, please go ahead, sir.

**STATEMENT OF HON. PATRICK F. KENNEDY, UNDER SECRETARY FOR MANAGEMENT, U.S. DEPARTMENT OF STATE, WASHINGTON, DC**

Mr. KENNEDY. Thank you very much. Chairman Leahy, Ranking Member Sessions, and distinguished members of the Committee, thank you for the opportunity to appear before you today.

As Secretary Clinton stated following the attempted bombing of Flight 253, "we all are looking hard at what did happen in order to improve our procedures to avoid human errors, mistakes, oversights of any kind...and we are going to be working hard with the rest of the administration to improve every aspect of our efforts."

We acknowledge that errors were made and that processes need to be improved. Here are the steps we have already taken.

The Department of State misspelled Umar Farouk Abdulmutallab's name in a Visas Viper report. As a result, we did not add the information about his current visa in that report. To prevent this, we have instituted new procedures that will ensure comprehensive visa information is included in all Visa Viper reporting that will call attention to the visa application and issuance material that is already in the databases that we share with our national security partners.

Chairman LEAHY. With the forbearance of my colleagues, why can't you have something—if you go on a Google search or you go on a Yahoo search and you type in a name, the computer will automatically ask you, "Did you mean . . .?" and it will put three or four other ways of spelling it. Why wouldn't that be a relatively simple thing to do?

Mr. KENNEDY. That is correct, Senator. When an applicant appears before us, we already have that software installed on our application screening process. If we put in the name Kennedy and we misspell it, it will come back K-E-N-N-E-D-Y, K-E-N-E-D-Y, K-N-N-D-Y. We had not loaded that software into the database to check on already issued visas because we were looking for a specific known commodity. We are in the process of changing that.

We have also evaluated the procedures and criteria used to revoke visas. The State Department has broad and flexible authority to revoke visas, and we regularly use that power. Since 2001, we have revoked 51,000 visas for a variety of reasons, including over 1,700 for suspected links to terrorism.

In an ongoing effort with our partner agencies, new watchlisting information is continually checked against the database of previously issued visas. We can and will revoke visas without prior consultation in circumstances where an immediate threat is recognized. We can and do revoke visas at the point of people seeking to board an aircraft, preventing their boarding. In coordination with the National Targeting Center, we revoke visas under these circumstances almost daily. We are standardizing procedures for triggering revocations from the field, and we are adding revocation recommendations to our Visa Viper report. We have scrubbed our databases and reviewed information in coordination with our partner agencies.

In our data scrub since December 25th, we have reviewed the names and all prior Visa Viper submissions. We have re-examined information in our Consular Lookout database on individuals with

VerDate Nov 24 2008 12:43 Oct 12, 2010 Jkt 058484 PO 00000 Frm 00012 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\58484.TXT SJUD1 PsN: CMORC

potential connections to terrorist activities or support for such activities. In these reviews, we have identified cases for revocation and have also confirmed that substantial numbers of these individuals hold no visas and few ever did. And for the few who did, many were revoked prior to the current review.

We recognize the gravity of the threat and are working intensely with our colleagues from other agencies to ensure that when the U.S. Government obtains information that a person may pose a threat to our security, that person does not hold a visa.

At the same time, expeditious coordination with our national security partners is not to be underestimated. There have been numerous cases where our unilateral and uncoordinated revocation of a visa would have disrupted important investigations that were underway by one of our National security partners. They had the individual under investigation, and our revocation action would have disclosed the U.S. Government's interest in that individual and ended our colleagues' ability, such as the FBI, to pursue the case quietly and to identify terrorists' plans and co-conspirators.

We will continue to closely coordinate our revocation processes with our intelligence and law enforcement partners. Information sharing and coordinated action are foundations of our border security systems put in place over the past 8 years.

We believe that U.S. interests in legitimate travel and trade promotion, as the Chairman mentioned, and educational exchange are not in opposition to our border security agenda and, in fact, further that agenda in the long term. We will continuously make enhancements to the security and integrity of the visa process. As we continue to do this work, we take a comprehensive review.

The Department has close and productive relationships with our interagency partners, and particularly the Department of Homeland Security, which has authority for visa policy. The State Department brings unique assets and capabilities to this partnership. Our global presence, international expertise, and highly trained personnel bring us singular advantages in supporting the visa function throughout the world. We have developed and implemented an extensive screening process requiring personal interviews and supported by a sophisticated global information network. This front line of border security has visa offices in virtually every country staffed by highly trained, multilingual, culturally aware personnel of the State Department. We have embraced a multilayered approach to border security which gives multiple agencies an opportunity to review information and require separate reviews at both the visa and admission stages. No visa is issued without being run through security checks against our partner databases, and we also screen applicants' fingerprints against U.S. databases as well. We take our partners' consideration into every effort that we make. We fully support the visa security program of the Department of Homeland Security and work closely with them in a dozen countries.

This multi-team effort to which each agency brings its particular strengths results in a more robust and secure process with safeguards and checks and balances. It is based on broadly shared information and is a solid foundation on which to build our border security future. We are past the era of stovepiping data, but there

is clearly more work to be done. We are doing that work now and planning future improvements as we continue our review.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Kennedy appears as a submission for the record.]

Chairman LEAHY. Thank you very much, Secretary Kennedy.

David Heyman is the Assistant Secretary for Policy at the Department of Homeland Security. He previously served as Director of the Homeland Security Program of the Center for Strategic and International Studies, also served as a senior adviser to the U.S. Secretary of Energy, the White House Office of Science and Technology Policy.

Secretary Heyman, thank you for being here. Please go ahead, sir.

**STATEMENT OF HON. DAVID F. HEYMAN, ASSISTANT SECRETARY FOR POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC**

Mr. HEYMAN. Thank you, Chairman Leahy, Senator Sessions, and distinguished members of the Committee. I appreciate the opportunity to testify.

Let me just start by echoing the sentiments regarding the tragedy in Haiti. This tragedy is of epic proportions, and the men and women at the Department of Homeland Security, Coast Guard, FEMA, and across the Department are working around the clock to support the international effort for the people of Haiti.

As President Obama has made clear, we are, all of us, determined to find and fix the vulnerabilities in our systems that allowed this attempted attack to occur. Our country's actions against terrorism require a multiagency, multinational effort to include the intelligence community, the Defense Department, DHS, the agencies here today, as well as efforts of our international allies.

Our aviation security relies on partnerships among the U.S. Government, the airline industry, and foreign governments. These partnerships must all come together when an individual seeks to travel to the United States. To board a plane, there are effectively three key requirements: An individual must retain proper documentation to include a passport, visa, or travel authorization, a ticket and boarding pass. That individual must pass through checkpoint screening to ensure that he is not concealing a weapon or other dangerous material on his person or in his baggage. And, third, the individual must be cleared through a pre- flight screening process that seeks to determine if that individual poses a threat and, thus, could be denied permission to fly.

Within that travel process, let me briefly describe the DHS role.

First, to accomplish pre-flight screening, the Department of Homeland Security is one of the principal consumers of the terrorist watchlist, which includes the no-fly list. We check against it and use it to keep potential terrorists from boarding flights and to identify travelers who should undergo additional screening.

Second, within the United States, to prevent smuggling of weapons and other dangerous materials on planes, DHS performs the physical screening at airport checkpoints and provides further security measures in flight.

VerDate Nov 24 2008 12:43 Oct 12, 2010 Jkt 058484 PO 00000 Frm 00014 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\58484.TXT SJUD1 PsN: CMORC

Outside the United States, DHS works with foreign governments and airlines to advise them on required security measures for flights bound to the U.S. as well as on which passengers may prove a threat. TSA does not, however, screen people or baggage at international airports.

I have submitted a longer written statement describing the various DHS programs that work to keep terrorists from boarding planes, but regarding the attempted attack on December 25th, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with explosives. The interagency process to fix the vulnerabilities highlighted by this attack is well underway. As a consumer of the watchlist information, DHS welcomes the opportunity offered by this process to contribute to improving the Federal Government's ability to connect and assimilate intelligence, and we are working with the FBI, ODNI, and NCTC on that.

We are also focused on improving aviation screening and expanding international partnerships to guard against a similar type of attack. I have just personally returned from a 12-day trip of consultations with key partners abroad.

In terms of the DHS role, though, the bottom line is that Abdulmutallab was not on the no-fly list, which would have flagged him to be prevented from boarding; nor was he on the selectee list, which would have flagged him for secondary screening. Furthermore, the physical screenings that were performed by foreign authorities at airports in Nigeria and in the Netherlands failed to detect the explosives on his body.

Immediately after the attack, DHS took a number of immediate steps to secure incoming and future flights to include directing FAA to alert 128 incoming flights of the situation, increasing security measures at domestic airports, implementing enhanced screening for all our international flights coming to the U.S., and working with State and local air carriers to provide appropriate information.

In the report to the President regarding this attempted attack, the Department has outlined five key areas of action that we are now addressing.

First, as the incident underscores, aviation security is increasingly an international responsibility. That is why Secretary Napolitano dispatched Deputy Secretary Lute and myself and other officials to meet our international counterparts on this issue. Today Secretary Napolitano is traveling to Spain to meet with her European counterparts for discussions on how to strengthen international aviation security measures.

Second, DHS has created a partnership with the Department of Energy and its National Laboratories to use their scientific expertise to improve screening technology at airports.

Third, DHS will move forward in deploying enhanced security screening technologies like advanced imaging technology and explosive trace detection machines to improve our ability to detect the kind of explosives we saw on the 25th.

Fourth, we will strengthen the capacity of aviation law enforcement, including the Federal Air Marshals Service.

And, finally, as mentioned earlier, we will work with our interagency partners to re-evaluate and modify the way the terrorist

watchlist is created, including how names are added to the no-fly and selectee list.

As the President has said, there is, of course, no foolproof solution, but there are many steps we can and are taking today to strengthen international aviation security. We face an adaptive adversary as we develop new screening technologies and procedures. Our adversaries will also seek new ways to evade them, as shown on Christmas Day. We must always be thinking ahead to innovate, improve, and adapt to the new emerging security environment, and I look forward to your questions to discuss this further.

Thank you.

[The prepared statement of Mr. Heyman appears as a submission for the record.]

Chairman LEAHY. Thank you.

I still remain concerned, and, Secretary Kennedy, the State Department did not realize the suspect in the Christmas Day attempted bombing possessed a visa until after he initiated this action on the flight. The consular officer sent the first notice that was given to the National Counterterrorism Center, initially misspelled the name, as we have talked about. But within days, an amended notice was sent to NCTC with the corrected spelling. Why did the consular office not check the visa status of the Nigerian national at the time the second notice was sent?

Mr. KENNEDY. He did not do that, Mr. Chairman, because——

Chairman LEAHY. I know he did not do it, but why not?

Mr. KENNEDY. Because the second message was launched from another source.

Chairman LEAHY. But why wouldn't—it may have been launched from another source, but why wasn't it checked?

Mr. KENNEDY. I cannot—because we did not have access at the embassy to that other reporting, Mr. Chairman, and we had entered his name in the incorrect spelling into the database that is our watchlist database, which was disseminated to all the appropriate agencies. We slipped up. I have no statement other than that, sir.

Chairman LEAHY. Thank you.

Before I go into the Christmas Day attack, just to go back, Mr. Mueller, to some of the things you talked about, the Justice Department Inspector General report on the national security letters, the FBI essentially told those companies that got these letters that there was an emergency so that the company would give the records voluntarily, as we would expect them to do. And the letters they were given said a subpoena would follow. Of course, the subpoena did not follow. Often there was no emergency. And this goes beyond being a technical violation. These are records of Americans being obtained improperly, 2,000 telephone records.

Has or will any FBI official be sanctioned or punished for these violations of the law?

Mr. MUELLER. Let me start by saying yes. This process started back in, I think it was, 2006 and initial reports were issued by the Inspector General. As a result of those reports, they were reviewed for discipline, and individuals have been disciplined for their participation in these series of issues. In this particular case, the re-

port will go through our process, and we will look at the conduct and assign discipline as warranted.

Let me also say I share with you the concern that this is information on American citizens that we had without following the appropriate protocols, in some cases where there was not an emergency, and we have put in place a process to go through every one of those numbers and determine whether we had a valid legal basis to retain that number, and where we did not, it was purged from our system.

Chairman LEAHY. Please let this Committee know what action is taken. I would note for the record you nodded yes on that.

Mr. MUELLER. Yes.

Chairman LEAHY. Now, what I worry about is the overinclusion of names on the no-fly list. You want to have the right names on there, but if you put every single possible name, in effect you have no names. You have such things as we saw last week in the New York Times, an 8-year-old boy who was on this list from the time he was an infant. He has been subjected to physical searches and patted down so much that the family does not want to fly. As his mother said, he may be a terrorist at home, but he is certainly not on an airplane. And it would be humorous except for what it causes to that family, but also what it says of the whole system when, complaint after complaint, the name stays on there. It is the same as the late Senator Kennedy, who was stopped numerous times because he was on the list. And even the President of the United States, President Bush, called him to apologize. He said it was not the President's fault. He just wanted to know how to get off the list, and he still did not get off the list for some time. I think we have to be looking first and foremost at our analysis and say what puts somebody on there.

How do we go about, No. 1, making sure we have the right person on there but, second, that we now do not so overinflate the list that legitimate travelers, business people, students, just the average American suddenly finds themselves on a list and unable to travel?

Mr. MUELLER. Well, it is, on the one hand, a delicate balance. As we have seen in the Christmas Day plot, a name can be misspelled by one letter, and you will miss them.

On the other hand, there are basically two precautions that are taken to assure we have the right person. For almost all of these lists, particularly the ones where it results in a stopping at an airport or at a no-fly list, it requires not just the name but an identifier, date of birth, something else that identifies it, as opposed to just the name.

Second, the other aspect of it is there is a redress process. If a person is no-fly, there is a redress process that DHS maintains so that——

Chairman LEAHY. Let me interrupt that. A date of birth, this 8-year-old first went on there when he was about a year old. Somebody looking at the list would say he is on there, he was born last year, and he is now on a terrorist watchlist. I mean, somebody——

Mr. MUELLER. I cannot explain what happened with the 8-year-old any more than I could have explained to Senator Kennedy how he had gotten stopped.

Chairman LEAHY. I am sure. But, you know, I told him it was because he was Irish and they all know him. But you heard what Secretary Kennedy said. You have a list over here and you have a list over here. Who determines which agency carries the primary responsibility for a lead that touches several agencies? You might have input from State, NCTC, DHS, and other agencies?

Mr. MUELLER. Well, when it comes to international terrorism, the contributions, nominations on international terrorism go to the National Counterterrorism Center. It can be an international terrorism case developed by the CIA, DIA, NSA, or even ourselves. It goes to the National Counterterrorism Center. The National Counterterrorism Center makes the determination as to which lists the individual will be nominated to, whether it be the no-fly, the selectee, or the Terrorist Screening database.

For domestic terrorists, it is the FBI that makes the recommendation to the Terrorist Screening Center as to who should go on that list. It is screened by both. The contributing agency and the National Counterterrorism Center screens it. Then the National Counterterrorism Center screens it itself. Then finally the Terrorist Screening Center does a follow-up screening to assure that there is sufficient identifying data and that the information putting the person on that list supports the criterion for being placed on that list.

Chairman LEAHY. I have gone over my time. I obviously have a lot more questions, and I do not want to interrupt others. We will go through these questions, and you and I may want to spend some time later in the week. And I am showing a list of testimony that I am going to submit for the record, a long list, and that will be submitted for the record. I am showing it to Senator Sessions.

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

Chairman LEAHY. Senator Sessions, over to you.

Senator SESSIONS. Thank you.

Briefly, I guess, Mr. Mueller, I will ask you, the NCTC, the center that maintains the list, do you think we can do better about getting people off the list? I heard somebody on a talk show the other day who said he was born here, his family is from Lebanon, but he keeps getting stopped.

Mr. MUELLER. Yes, in some sense, yes. If you have got people who do not belong on the list, they should be gotten off the list for a variety of reasons. It interferes with their right to travel——

Senator SESSIONS. And who would be responsible for that? Is that the NCTC?

Mr. MUELLER. NCTC in terms of international terrorism, yes. But also DHS in terms of the redress process. When somebody files a complaint that they should not be on the list, it is then handled principally by DHS. But generally you want to have on those lists—as many persons who meet that criterion should be on that list because it is protection against terrorist attacks in the United States.

Senator SESSIONS. I could not agree more, and people in this world have—a lot of people have the same name, and it is difficult to know. And one of the reasons we are here complaining is because somebody did not get on the list.

But, Mr. Heyman, I think you should look to see how a person who can prove that they may have the same name as a dangerous person can somehow not be given as much burdens at the airport as otherwise would be the case.

Mr. HEYMAN. Senator, there is a one-stop-shop website that was developed for redress purposes, www.dhs.gov/trip, and anyone who has concerns that they are inappropriately on a watchlist should go there. There is an adjudication process. The Department through the interagency process has adjudicated 56,000 people at this point.

Senator SESSIONS. I don't think—I just would say I do not think we need to have proof beyond a reasonable doubt that a person is a terrorist before they go on the list. What is the burden normally we would have there? It should not be too high.

Mr. MUELLER. It is reasonable suspicion that the person is either assisting, participating, or supporting terrorists.

Senator SESSIONS. Are you satisfied that is the sound standard?

Mr. MUELLER. We are looking at the standards and seeing their application across various potential threats. But it has worked well in the past, and at this point, without further discussion, I am satisfied with that. I believe it is a low enough standard——

Senator SESSIONS. We are not putting them in jail. We are just simply confronting them before they get on an airplane.

Mr. Mueller, after being dispatched by an al Qaeda affiliate in Yemen to blow up hundreds of civilians in an airline bombing, Umar Abdulmutallab was charged via a criminal complaint within 24 hours of the landing of Northwest Flight 253. He was reportedly given Miranda warnings shortly after being arrested, including being advised he had the right to remain silent and he was entitled to a lawyer.

First, who made the decision that Abdulmutallab was going to be treated as a criminal rather than an enemy belligerent?

Mr. MUELLER. Well, let me preface this by saying, as I am sure you are aware, this is in litigation, but I think I can talk generally about what happened and not interfere with the ongoing litigation.

Abdulmutallab was arrested on the plane after these incidents. There was no prior discussion. He was handed over, I believe, by the personnel on the plane to CBP, who originally had custody of him. He was taken to a hospital in which the FBI took custody of him. And it happened so fast that there was no time really at that point where the transfer was made very quickly given the moving circumstances to determine whether alternative arrest could or should be made.

Senator SESSIONS. Well, who made the decision that he would be treated as if he were a criminal to be tried in civilian courts and be provided Miranda warnings? Who?

Mr. MUELLER. Well, the decision was to arrest him, put him in criminal courts. The decision was made by the agents on the ground, the ones that took him from the plane and then followed up on the arrest——

Senator SESSIONS. Well, this is a very big issue. So the decision was made by agents on the ground based on some protocol or some policy that they understood?

Mr. MUELLER. Based on an ongoing, very fluid situation in which they were trying to gather the facts and determine what culpability

this individual had. But as important as determining the culpability of this individual is what other threats were out there that needed to be addressed.

Senator SESSIONS. Well, surely you recognize—I know you do—that there are great differences between trying a person in military commissions. In fact, I was able to work on legislation and get language in that said anyone "a part of al Qaeda at the time of the alleged offense was per se an unprivileged criminal combatant, enemy combatants, subject to military commissions and indefinite detention" as long as we have a conflict with al Qaeda. And so this was a big decision. Immediately, I assume, the lawyer advised his client not to talk.

Mr. MUELLER. Well, without getting too much into the details, in this particular case the agents interviewed him for a period of time for any information relating to ongoing and other threats.

Senator SESSIONS. Before or after a Miranda warning was——

Mr. MUELLER. Before Miranda warnings were given.

Senator SESSIONS. Well, that is pretty dangerous because anything he said during that time is not admissible in a civilian court, is it?

Mr. MUELLER. That is correct.

Senator SESSIONS. So if he confessed——

Mr. MUELLER. Well, I take that back. I take that back. As I am sure you are aware, there is a limited exception for emergency situations in the case called *Quarles* where——

Senator SESSIONS. But with regard to your agents, it seems to me you have a policy that these kinds of individuals will be tried in civilian courts rather than military commissions. That has ramifications because it is going to reduce, I think you would agree, the likelihood of intelligence being gathered. One of the things we learned from the 9/11 Commission is that intelligence saves lives, and we need to gather intelligence. That is not the motive of the criminal justice system generally in America. It is to prosecute criminals. So I think this is a serious matter.

Are you satisfied that you have a clear understanding, a national policy about how these people should be treated once they are apprehended?

Mr. MUELLER. Well, I do believe——

Senator SESSIONS. It sounds to me like the guys on the ground just made a decision on the fly.

Mr. MUELLER. There are decisions made whether or not to arrest somebody, and our arrest powers are dependent upon——

Senator SESSIONS. Arrest powers, that is not a problem. Were you contacted about whether or not this individual should be treated as an unlawful enemy combatant——

Mr. MUELLER. No.

Senator SESSIONS.—or a civilian criminal?

Mr. MUELLER. No.

Senator SESSIONS. So the decision was made below your level.

Mr. MUELLER. Well, that does not mean the decision can be taken—that does not mean the decision can or should not be taken later if one wants to go otherwise. But in this particular case, in fast-moving events, decisions were made, appropriately, I believe, very appropriately, given the situation——

Senator SESSIONS. I do not think you can say it is appropriately. We do not know what that individual learned while he was working with al Qaeda, and we may never know because he now has got a lawyer that is telling him to be quiet.

Chairman LEAHY. Senator Sessions, for one thing, let him finish answering the question. The fact is, of course, if you are talking about him going to a military commission, he would have been given a lawyer in a military commission. Military commissions had, I think, three convictions. The courts have had hundreds of convictions of terrorists.

Senator SESSIONS. I do not think they are given lawyers who tell them to remain silent initially. If they are going to be tried in a trial by a military commission, they are given a lawyer.

I think this is a matter of serious import. I do not think we have clarity of rules, and I believe we have got to get it straight. And I believe these people will be better tried in a military commission for a lot of reasons, one of which is the gaining of intelligence.

My time is up, Mr. Chairman.

Chairman LEAHY. I might say to the distinguished Senator from Alabama, he, like I, was a prosecutor. Do you think any prosecutor is going to have to worry about what was said by somebody who tried to ignite a bomb and was stopped by several eyewitnesses? I do not think they are going to have to rely too much on a confession from them.

Senator SESSIONS. Well, just in response to your question——

Chairman LEAHY. Let us be serious for a moment.

Senator SESSIONS. In response to your question to me, it is not just the ability to prosecute this individual, but whether if he were properly interrogated over a period of time we may find out that there are other cells, other plans, other Abdulmutallabs out there boarding planes that are going to blow up American citizens.

Chairman LEAHY. Senator Kohl.

Senator KOHL. Thank you, Mr. Chairman.

Director Mueller, how many people are on the no-fly list, approximately? Is it being expanded now? What is the——

Mr. MUELLER. We are generally hesitant to give the full numbers. I would say several thousand.

Senator KOHL. And are you anticipating——

Mr. MUELLER. Hesitant to give it in open session. That is what I am saying.

Senator KOHL. I understand that. Are you anticipating that list is going to be expanded?

Mr. MUELLER. There are discussions, and there have been some expansions, yes.

Senator KOHL. All right.

Mr. MUELLER. And, again, that can be part of a briefing as to what activities have taken place, particularly since Christmas Day.

Senator KOHL. All right. Director Mueller, clearly there are flights into the United States from hundreds of airports all around the world, and these airports are under the direction and supervision of other governments. I assume some of them do a better job, some of them do not do as good a job. For example, according to what we hear, in Israel they do a terrific job of screening people before they board flights.

What kind of a problem is dealing with other countries to be sure that their security measures at their airports originating flights into the U.S. are sufficient?

Mr. MUELLER. I would be happy to try to answer, but I actually think my colleague Mr. Heyman from DHS would be more familiar with this than I am.

Senator KOHL. All right. Mr. Heyman, go ahead.

Mr. HEYMAN. Thank you, Senator. The standards by which international airport security are the ICAO standards, which is the international body for developing security regimes for aviation across the globe. Countries are required to meet ICAO standards for the last point of departure to the United States. TSA does audit those countries to ensure security standards are met. But you are absolutely right, the ability to meet those standards varies from country to country, and I think as we look forward, one of the things we are looking at in terms of discussions with our international partners is the ability to help build the capacity around the globe for the right level of security.

Senator KOHL. Well, it seems to me that is a crucial element of this whole discussion we are having, how well do they do their jobs in other countries and at other airports. I would not be surprised that there may be airports around the world that should not be allowed to originate flights into the United States because of their lack of proper security implementation. Wouldn't you imagine that might be true?

Mr. HEYMAN. Well, in order for a carrier to travel from a country abroad, from a last point of departure abroad to the United States on a direct leg to the United States, they have to meet the ICAO standards, and they have to meet TSA audit requirements. And the Department audits last points of departure—there are about 245 of them—to the United States every year, and if an airport or carrier do not meet the standards, they are given an opportunity to address those concerns, or the flights are discontinued.

Senator KOHL. I have never heard about an airport that has been cited and disallowed from originating flights into the United States because of lack of proper security observations, and I would suggest that there must be some serious issues relating to airports that are not doing the proper job of screening prior to originating flights into this country. My common sense tells me that that is very possibly true. What do you think?

Mr. HEYMAN. I can tell you that of the 245 last points of departure to the United States, the TSA has audited them on a regular—does audit them on a regular basis to ensure the safety and security of flights emanating from those points of departure. Other cities that may be interested in direct flights to the United States would have to go through the ICAO standards and the TSA review, and if they were not able to meet them, they would not be permitted flights.

Senator KOHL. I would like to hear a little bit from you all about body scanners, their use, their effectiveness, and plans to expand them. What are some of the issues that we are dealing with, Director Mueller?

Mr. MUELLER. That is a little bit out of my bailiwick as well. Again, I would defer to DHS.

Mr. HEYMAN. I would be happy to answer that question, Senator.
Senator KOHL. Go ahead.

Mr. HEYMAN. There are a number of different ways in which we provide security at checkpoints here in the United States and that are considered abroad for screening passengers who may be trying to conceal weapons or materials. The standard use of a walk-through metal detector is what is the predominant security feature around the world. In the United States, we have a number of layers of defense, layers of security, to include behavioral observation, canines, explosive detection devices as well as other technologies. We are in the process of deploying whole-body imaging, enhanced image technology. That technology has the advantage of detecting non-metallic substances such as powders or liquids, such as what was found on Abdulmutallab on Christmas Day. So we are moving forward rapidly to deploy additional scanners around the United States on that.

Senator KOHL. I would like to get back to my question about different airports in different countries. What is it about the Israeli airport security system that has attracted as much praise as it has over the years?

Mr. HEYMAN. Senator, that is one of the countries I just visited and, in fact, did take a tour of their airport, Ben Gurion Airport, and had briefings from security officials there. They have addressed their security concerns through a number of layers, including things that we do in the United States, such as behavioral observation, the way that they interview—the interview is critically important to passengers—and the number of layers of screening, of targeting potential terrorists as well as screening of baggage that may be on board.

They also live in a very different environment, and I would not compare their targeting necessarily to the United States. I think they have a very different environment that they live in and, thus, not necessarily transferable. But their layers of defense is something that we have also adopted in the United States and is what a lot of people talk about.

Senator KOHL. Finally, I would just make the observation again that this is a worldwide issue, clearly, and I am troubled by the thought that rating security, airport security in different countries, if it were done very critically, would probably disclose wide variances between the security effectiveness implemented in different countries. And until we do a better job of trying to coordinate as a world the security systems in different countries, we will continue to be at great risk. Would you agree with that?

Mr. HEYMAN. Senator, I do agree. I think one of the key things we learned from this is that access to any airport in the world gives you access to the entire international system. This individual bought a ticket in one country, traveled to a second country, transited through a third country to target a fourth country. There were somewhere near two dozen individuals, two dozen nationalities represented on that plane. They traveled across a number of different countries. This is an international problem, and that is why Secretary Napolitano is heading to Europe tonight to meet with European counterparts for discussions on enhancing international security. There will be additional—the President has

tasked the Department to expand international cooperation in this realm.

Senator KOHL. Thank you.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator Grassley.

Senator GRASSLEY. Thank you, Mr. Chairman.

I will start with Secretary Kennedy. The State Department has indicated that it could not provide this Judiciary Committee with a copy of the Christmas Day bomber's visa application prior to this hearing because it was part of "an interagency DOJ review process." However, the Justice Department indicated to my staff yesterday, just yesterday, that the State Department had not even provided a copy of the application to the Justice Department yet. I do not understand why the State Department would tell us that it was being reviewed by the Justice Department if the Justice Department says they do not have it. So since I do not want to trust just executive branch opinion about what is on this and what process it ought to go through, I want to know for myself what information did this bomber put on his visa application. Why shouldn't we conclude that the State Department is simply trying to hide behind the Justice Department criminal process in order to avoid or delay a full accounting of how this terrorist got into this country on your watch? But my big question is, second: When will we get a copy of this application?

Mr. KENNEDY. Senator, we are by no means attempting to hide behind this whatsoever.

Senator GRASSLEY. OK. Well, then, when will I——

Mr. KENNEDY. I promise you that I will return to my office and I will have our staff contact the Department of Justice immediately, and if it is in, we will proceed from there, sir. We are not attempting to hide behind the Department of Justice. We carefully coordinate all our activities with the Department of Justice, and we will get back to you, sir.

Senator GRASSLEY. But they have got to have it in order to review it, and you told me it is being reviewed. I do not say you did, but the people in the agency said it is being reviewed.

Mr. KENNEDY. We will check with the Department of Justice this afternoon, sir.

Senator GRASSLEY. I would think the first thing to do would be to walk it over there so that they can have it.

I would like to go on to another issue with the FBI Director. On January the 7th, President Obama directed the FBI to "conduct a thorough review of Terrorist Screening database holdings and ascertain current visa status of all known and suspected terrorists, beginning with the no-fly list."

This directive implies that there is a concern that the State Department may have issued visas to individuals who are known or suspected terrorists. However, the Christmas Day bomber was not labeled a known or suspected terrorist. Instead, he was given a lesser classification by the State Department as what they referred to as a P3B, meaning he was a possible or probable terrorist.

Has the FBI reviewed all records in the State Department's CLASS system for individuals designated P3B, meaning possible or

probable known or suspected terrorist, to determine if any of these individuals were issued a visa?

Mr. MUELLER. My understanding, Senator, is that we have taken the no-fly list and assured that the persons there do not have visas. We have taken the selectee list and determined that persons there do not have access to visas. And then with regard to the much larger Terrorist Screening database, we are going through that and making certain—at this time we are going through that database and assuring that those persons do not have visas.

It is from the Terrorist Screening database that the CLASS system is populated with information on particular individuals. So we feel that this way we are looking at the databases which are handled by the Terrorist Screening Center, and what we are doing will be redundant to what is being done by the State Department as well as by the NCTC.

Mr. KENNEDY. Senator, could I, with your——

Senator GRASSLEY. Well, just a minute, and then I will be glad to have you do that. Just in case you answered my question, but I do not know for sure if you answered it, have you reviewed P3Bs, then? And if you have not, do you intend to do so?

Mr. MUELLER. I am not personally familiar with P3Bs, Senator, but I would be happy to——

Senator GRASSLEY. Well, they are the possible or probable terrorists.

Mr. MUELLER. Is that a definition for—I am a little bit lost. Is that a definition for populating a particular list?

Senator GRASSLEY. It is my understanding it is. But now maybe I ought to let Secretary Kennedy speak.

Mr. MUELLER. He may be more versed in that.

Senator GRASSLEY. Maybe you could have solved this for me, but go ahead.

Mr. KENNEDY. Yes, sir, Senator. Thank you. If I could just give 1 second of context, every visa applicant who comes into a United States embassy and applies for a United States visa, his or her name is run against a complete database that includes entries from the FBI, entries from Homeland Security, entries from the Terrorist Screening Center, entries from DEA. We take entries in from all these agencies daily and load them into our database, and so no one who applies for a visa, no one is issued a visa without a complete scrub against the full interagency database. And, additionally, they are also scrubbed against the complete DHS and FBI fingerprint sets of individuals who are of concern to those agencies.

So we run this complete screen. Then anytime someone is moved up, so to speak, on the screening list from either of our partners within the national security community, that information is immediately transferred to us. We then run that new information against our list of issued visas to see if those agencies have obtained new information that they had not been made available to us earlier, and then we run that. And if someone has moved up on that list, we then move to revoke those visas immediately.

Last, on your question, sir, about the P3B, the P3B is a category, when someone comes to our attention, we have concerns about them, but it is not conclusive. We then immediately send that information to our partners in the intelligence and law enforcement

community, but we put this P3B code in so that no State Department officer at that post or anywhere else in the world will issue that visa without doing a double-check with our partner agencies.

After December 25th, we rescrubbed that with our partners in the intelligence community and have canceled seven visas.

Senator GRASSLEY. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman. I would like to just make a couple of comments and then some questions.

I think it has become pretty clear now that the airplane remains a major explosive device. I think it is very clear that there are going to be more attempts. This attack took place over United States soil. I think the handling by the FBI is entirely appropriate. And I would like to bring to this Committee's attention the fact that the FBI has done excellent interrogation in the past. A Subcommittee on which Senator Kyl and I have participated has had former FBI agents testify going back to the 1993 New York City bombings where the interrogation done by the FBI really brought about convictions of a number of people, including the blind sheikh, people who are serving time in prisons in the United States who were part of trials here in the United States. So I believe the handling of Mr. Abdulmutallab is entirely appropriate, and I think people should understand that.

I am concerned about the no-fly list. I believe the definition of who would go on the no-fly list is highly convoluted. It takes a Philadelphia lawyer to interpret. And I have been told by Director Blair that it is being reassessed and hopefully will be redone.

PETN is becoming the explosive of choice. I suspect we are going to have more attempts using this explosive, and hopefully it will not be perfected soon.

So let us go for a moment to the visas, and, Mr. Kennedy, let me ask you: Were you saying in your testimony that there will be an automatic revocation of visas for subjects of a Visa Viper cable or a Terrorist Identities Datamart Environment, the TIDE, entry? The answer is yes or no.

Mr. KENNEDY. The answer is no for the reasons outlined in my testimony, Senator. We receive information that causes us great concern as the first line of national security. We send that information to our partners in the FBI, our partners in other law enforcement agencies, and our partners in the intelligence community. We have been requested on numerous occasions by those agencies not to revoke the visa because there is an active investigation——

Senator FEINSTEIN. Well, let me stop you there because I know all about that, and I have some questions about that, but that is for another Committee, and we will be taking that up on Thursday. But those are not many, and I know the number of people on the no-fly list. It seems to me that we ought to have a process which assured revocation of a visa, and what I have learned is that essentially it is very difficult to revoke a visa.

Mr. KENNEDY. Senator, it is not very difficult to revoke a visa. If the FBI, Homeland Security, any other member of the law enforcement and intelligence community comes to us—and we get in-

formation from them every day which we run against our records. If they come in and say that this individual is a danger to national security, we revoke the visa immediately.

Senator FEINSTEIN. So that is automatic. And where does it have to come from, the automatic?

Mr. KENNEDY. The Terrorist Screening Center at the FBI, the NCTC, from the Department of Homeland Security. We receive information from all our partners, and if they provide us with information that says that this individual is a danger to national security, we revoke that visa immediately.

Senator FEINSTEIN. All right. I am happy to hear that.

As you know, Mr. Abdulmutallab was issued a multiyear, multiple-visit tourist visa in June of 2008. Do you believe it is in the United States' security interest to issue visas that allow entries over several years or more than one visit to the United States?

Mr. KENNEDY. Senator, because we receive information every day from our law enforcement and intelligence community partners, we are able to revoke and cancel visas on any given day if new information comes to our attention that says an individual who was not a threat when we ran his or her application against our partners' databases. If those circumstances change and we are notified by the intelligence community or law enforcement that this individual's circumstances have changed, we then immediately revoke his visa.

Senator FEINSTEIN. All right. It just seems to me we still have a lot of learning to do. This Committee had the consular officers before it who gave visas to certain of the 9/11 hijackers, and those visas should not have been issued, in my view. And I think we have really got to batten down the hatches of who we give visas to. And I am about to go into the Visa Waiver Program because, in my view, that is the soft underbelly of this country, Mr. Heyman.

Mr. KENNEDY. Senator, if I could add one thing with your permission.

Senator FEINSTEIN. Sure. Go ahead.

Mr. KENNEDY. You are entirely correct. Before 2001, we were not—we, the State Department, were not receiving sufficient information from our intelligence community and law enforcement colleagues. Since 2001, the number of data elements given to us from our partners is up 400 percent. We now have a 27-million-name list from the intelligence community, writ large, from the law enforcement community, and from our own sources that every single visa applicant's name is run against that database as well as run against fingerprint databases from the FBI and Homeland Security.

So there has been an absolute change from the point that you spoke of in 2001 where we were not getting sufficient information in order to have a data set to run against. We now have that. As I said, it is up 400 percent since 2001.

Senator FEINSTEIN. I appreciate that, and I thank you for it.

Mr. Heyman, as you will probably know, I am not a fan of the Visa Waiver Program. We now have 16 million people from 35 different countries who come in without a visa, and we do not know if and when they leave. I believe it is the soft underbelly of this

country. I believe that if Mr. Abdulmutallab, who went to school in Great Britain, in the U.K., became a naturalized citizen of the U.K., he could have had a visa waiver and come into this country without one. And I think that is a real, real problem.

So let me ask you: What checks do we have that someone who is denied a visa but is not put on a terrorist watchlist can come into this country at a later date through the Visa Waiver Program?

Mr. HEYMAN. Well, just to clarify, in the Visa Waiver Program you do not need a visa, but there is a travel authorization that is required, an advance travel authorization that runs the same checks basically that a visa check would do. It is also done—the same kind of cursive review of the watchlist and things like that to revoke or refuse authorization is done. And I understand your concerns about it, but let me just say that the Visa Waiver Program includes a number of additional enhanced opportunities for cooperation and information sharing to include reporting of lost and stolen passports, standardized passports, sharing of terrorist screening information, sharing of criminal data information, and recurring auditing or review that we have with these countries to evaluate overall security, which we do not have with non-visa waiver countries.

So there are a number of enhanced security measures that actually supplement security in the VWP programs, and so I am not sure I would agree with the characterization, but I understand your concerns.

Senator FEINSTEIN. Yes, and I am not sure I would agree with what you said, so perhaps we can debate this or discuss it separately.

Chairman LEAHY. This debate could go on, and I am sure it will. We are going to do—Senator Feingold is going to be next. Then Senator Cardin is going to chair the hearing. I have to go on the floor on a judicial nomination.

I have been making notes here. I think all of you are probably going to be getting calls from me or my staff in the next few days. There are an awful lot of follow-up things.

Senator Feingold.

Senator FEINGOLD. Thank you, Mr. Chairman.

Thank you all for being here. I join all members of this Committee in my horror at what happened on Christmas Day on the Northwest flight from Amsterdam to Detroit. While the attempt did not end in the tragedy that it could have, we must understand how and why the bomber was able to board that flight and what steps we can take to prevent the next such attempt. But we must also approach our task calmly and thoughtfully and not treat this as an opportunity to score political points. Congress needs to work with the executive branch to find the right answer to these questions and not just lay blame or take actions that are politically expedient but ultimately ineffective.

By all accounts, the President was right to characterize this as a systemic failure, and I agree with him that some very tough questions must be asked to repair and improve the counterterrorism systems that are now in place. This is not the time for excuses, nor is it the time for pointing fingers. It is time to fix the problem, and that is exactly what will make us safer.

Mr. Chairman, I would just ask that my full statement be placed in the record.

Senator CARDIN. [Presiding.] Without objection.

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

Senator FEINGOLD. Thank you, Mr. Chairman.

First, I am concerned that the policy of enhanced screening for all nationals from 14 countries will potentially harm our relations with governments and populations that can be allies in defeating al Qaeda and its affiliates and may not be an effective use of limited resources. Can any of you tell me whether a formal intelligence analysis has been conducted assessing the value of blanket screening of all people who are traveling from or through or are nationals of particular countries, either generally or specifically with respect to the recently designated 14 countries? Somebody.

Mr. HEYMAN. Sure. The designation of the countries was a determination in consultation with the Department of State and the Department of Homeland Security, as well as an assessment of new and emerging threat information. Their recommendation includes not just the enhanced screening of a number of foreign nationals, but, in fact, the majority of any individual traveling to the United States, to include U.S. citizens. So it is not, in fact, a blanket across specific nations per se, but enhanced screening for all individuals coming to the United States.

Senator FEINGOLD. Mr. Heyman, my question was whether there was a formal intelligence analysis that had been conducted as a part of this.

Mr. HEYMAN. The threat information was included in the analysis for determining the enhanced screening procedures.

Senator FEINGOLD. I am not certain that is the same. Could you provide that analysis to Congress? Formal intelligence analysis that led to these determinations.

Mr. HEYMAN. I will have to get back with you. I was not a party of the discussions, but I will be able to follow up with you after.

Senator FEINGOLD. OK. Secretary Kennedy, what role did the State Department play in helping to determine which countries should be on the list? And how did the State Department handle the responses it received from those countries once they were notified?

Mr. KENNEDY. Thank you, Senator. The Department of Homeland Security presented the State Department right after the events of Christmas Day with a list of countries that they said that they believe that these areas needed enhanced screening. We reviewed that list. There were a couple of countries we asked questions about. The list was then approved by the State Department because Homeland Security felt on the basis of the information, as Mr. Heyman said, was sufficient that as an interim step that needed to be taken immediately in order to safeguard not only American citizens but nationals of other countries boarding those aircraft as well. And so I know from discussions that have taken place that the Department of Homeland Security is continuing reviewing that list to determine the best way to provide safe and secure aviation movement because of the boarding—let us call it the boarding process, if I could, Senator.

Senator FEINGOLD. How did the State Department handle the response it received from those countries once they were notified that they were in this group?

Mr. KENNEDY. We shared that information with the Department of Homeland Security, and we are in discussions with them. Our Office of Counterterrorism at the State Department works very, very closely with the Department of Homeland Security, as does the Aviation Division of our Economic and Business Bureau. Those discussions are ongoing, but the primary responsibility, as Mr. Heyman said in his earlier testimony, for surveying airports and determining whether or not that airport is safe to launch aircraft to the United States is the last——

Senator FEINGOLD. But what I would like to be able to have access to is the information about what happened when these countries were notified and what their response was. This is very relevant to the value and wisdom of doing this.

Mr. KENNEDY. Senator, I will——

Senator FEINGOLD. So can we get a briefing on it, classified if necessary?

Mr. KENNEDY. Yes, sir. We will be in contact with your staff this afternoon to set something up for you.

Senator FEINGOLD. Thank you.

Director Mueller, we have heard criticism this morning for the decision to try Abdulmutallab in Federal court, and I am, of course, a little mystified by this reaction given the similarity of this case to the attempt by Richard Reid who was prosecuted in Federal court by the prior administration, now serving a life sentence. Some have argued the decision has compromised our ability to obtain useful intelligence. But as I understand it, and as Senator Feinstein touched on, there are quite a few examples of people who have been charged with terrorism-related crimes in Federal court and who have cooperated with the U.S. Government.

Do you see any reason to treat this case differently from the Richard Reid case? And has it been your experience that alleged terrorists charged with crimes in Federal court often cooperate with the Government and provide useful intelligence?

Mr. MUELLER. Well, in a direct answer to the question, we have had a number of cases in which, through the process, the criminal justice process of the United States, individuals have decided to cooperate and provided tremendous intelligence. That is not to say that there may not be other ways of obtaining that intelligence, but, yes, in answer to your question, the criminal justice system has been a fount of intelligence in the years since September 11th.

Senator FEINGOLD. Thank you for that answer. Director, I cannot finish without telling you how concerned I am, as I am sure you know, about the new Inspector General report that came out this morning, which you talked about, detailing rampant illegality at the FBI with regard to obtaining phone records. I know you have taken a number of steps previously to address those issues, but the IG recommends much more, and DOJ and the FBI need to provide Congress today with the new OLC opinion that states what legal authorities the FBI has to obtain phone records. Will you make sure that that happens?

Mr. MUELLER. I am trying to understand exactly what you want.

Senator FEINGOLD. The new OLC opinion that states what legal authorities the FBI has to obtain phone records.

Mr. MUELLER. If it ia an OLC opinion, it really is in the hands of the Department of Justice. It is up to the Attorney General. But I see no reason why you should not have it, but it is not my decision to make.

Senator FEINGOLD. OK. I thank all of you.

Thank you, Mr. Chairman.

Senator CARDIN. Well, first let me thank all of our witnesses for the work that you do for our National security.

In my role as Chairman of the Subcommittee on Terrorism and Homeland Security, we held a hearing last year in which we went over whether we are sharing information among the U.S. intelligence agencies as effectively as we need to in order to protect homeland security. At that hearing, Ms. Baird and former Senator Gorton testified, and they have submitted testimony for the record in regards to this hearing in regard to the concerns they have about the culture of sharing information within our Federal agencies. Without objection, I am going to ask that their testimony be made part of this record.

[The information appears as a submission for the record.]

Senator CARDIN. I guess my first question is: There has been concern as to the operational roles and responsibilities in regard to making the decisions concerning who is to be stopped at our airports, how we share the appropriate information, and the President has asked for a review. Is there currently in the works any recommendations for change as to the sharing of information and the respective roles of the different agencies in making these decisions?

Mr. MUELLER. Why don't I try to address that? The President has directed us to look at the criteria that are utilized to put persons in various levels of the terrorist watchlist. That is one aspect of it.

The President has also asked us to look and Admiral Blair is looking at other mechanisms utilizing information technology which will enhance our ability to better connect pieces of information from various databases. That has been an ongoing process since September 11th, and it is an ongoing process as new technology becomes available and we have new data sets.

But I would say just as a comment that the sharing is—it is a new world since September 11th in terms of our desire to share with every other agency. Not a one of us, sitting at this table or otherwise, does not understand that we have an obligation to share that information to prevent the next terrorist attack. So the motivation is there. The will is there. A lot has been done. There is still work to be done, particularly when it comes to utilizing information technology to make our jobs easier.

Senator CARDIN. And also how we connect the dots. Let me get to Mr. Abdulmutallab for one moment. Information became available last year to the State Department from his father, and as I understand, that information was reviewed as to whether there was a visa outstanding in regard to that individual, and because of the misspelling of the name, it did not pop up on your data search. Is that correct?

Mr. KENNEDY. That is correct, Senator. As I said earlier, we made—if I could add two points quickly. We did, though, put the name correctly into our lookout system, and the lookout system went to all the agencies in Washington, and a longer classified message describing more in-depth conversations with his father went in with the correct spelling, and the two were married up in a single file in Washington. And so the misspelling, our error, was obviated by the second message that paired up with it, sir.

Senator CARDIN. But it never gave you the information at the time that a visa was outstanding. If it did, if it would have shown that he had been issued a visa in 2008, was there sufficient information available for you to take action in regard to that visa?

Mr. KENNEDY. No, sir. There was not sufficient information from his father, nor do we take preemptive action because, as I mentioned earlier, we always consult with our law enforcement and intelligence community partners before we revoke a visa to make sure the individual is not a subject of investigation and we would compromise their investigation.

Senator CARDIN. So let me make sure. Are you saying that even if it would have popped up that he had a visa outstanding, you would have not taken any action to revoke that visa?

Mr. KENNEDY. There was insufficient information to immediately revoke the visa, and also following the protocols that have been in place since 2001, we check with our partners in the intelligence and law enforcement communities to make sure that our revoking that visa does not tip him off that he is under surveillance by one of our partners in the national security community, and, thus, our action would have compromised their ability, let me hypothetically state, to roll up a larger terrorism ring.

Senator CARDIN. So in this particular case, we do not know what would have happened if you made that inquiry.

Mr. KENNEDY. We did notify—we did put his name, correctly spelled, into our database that was available to law enforcement and the intelligence community personnel.

Senator CARDIN. And no dots were connected from that, that we are aware of prior to Christmas Day.

Mr. KENNEDY. Sir, that is something that is outside——

Senator CARDIN. He did not go on any watchlist, did he?

Mr. KENNEDY. No, sir. If the intelligence or law enforcement communities had come back to the State Department and said, "We have other information on this individual in addition to the information you, the State Department, has provided us; we are putting him on one of the lists," we would have potentially—we would have revoked that visa in coordination with law enforcement and intelligence.

Senator CARDIN. So DHS had the information prior to Christmas Day, but did not have any reliable information to act. Is that where we are?

Mr. HEYMAN. He was neither on the watchlist nor a no-fly list nor a selectee list, and so there was—no check against those lists would have come up with anything.

Senator CARDIN. But whose responsibility was it to look into that information and determine as to whether he was actively involved in al Qaeda in Yemen? There is information that he was there. It

seems to me that there was significant information linking him to potential terrorist activities that was put into our data bank. Whose responsibility was it to follow up to see whether action should be taken to at least alert agencies of a risk factor, but also to investigate whether there is further reason to suspect that an act of terrorism might be taking place? No one seems to want to answer that.

Mr. KENNEDY. Senator, that is a subject outside the jurisdiction of at least the State Department. I can describe our process. Any information that comes to the attention of the State Department that says there is a potential terrorist, we send it in to the national——

Senator CARDIN. You send it in. You type it in. It is sent in. You did not think he had a visa outstanding. If he had one, you would not have acted without further information from other agencies. And this point, I guess, Director Mueller, I was referring to originally as to responsibility. Whose responsibility was it to take that information and try to connect the dots?

Mr. MUELLER. I think the President's—the report identified by the President would say that the information goes into the National Counterterrorism Center where the lists are maintained from which you then put the person on no-fly or the——

Senator CARDIN. Someone has to develop the——

Mr. MUELLER. And so the information is developed. It is developed by NSA. It is developed by CIA, developed by the State Department, goes into the NCTC, the National Counterterrorism Center for determination as to whether that person should be on which watchlist. And to the extent that there is follow-up, it is done generally there when it comes to international terrorism.

Senator CARDIN. I would just make the observation there was information that was put into the data bank, and it appears like before Christmas Day no one acted on that.

Mr. MUELLER. Well, there is some information that did get to NCTC. There is other information that did not get to NCTC before then. And so it was a question of—I think it is fair to say some person should have passed information into NCTC that did not end up there, and the database, the ultimate database where you have the information that leads to putting a person on either the selectee or the no-fly list for international terrorism generally goes through that process.

Senator CARDIN. I guess my concern is that it is not clear as to whose responsibility it was to take that information and to develop it, whether it is a serious enough link not only to protect America against that individual but to use that information to try to determine whether there is active terrorist plots against America. And I hope that is being corrected because there was information there that was just sitting there, and obviously it could have been a very serious situation against this country.

Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. Let me thank all the witnesses for being here.

My first question is for Mr. Kennedy from the State Department. It is about multiple-entry visas. One of the main criticisms that has been leveled in this matter was that Abdulmutallab's multiple-

VerDate Nov 24 2008 12:43 Oct 12, 2010 Jkt 058484 PO 00000 Frm 00033 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\58484.TXT SJUD1 PsN: CMORC

entry visitor visa issued to him by our embassy in London in June 2008 was not revoked once his father warned our Nigerian embassy about his extremist activity. This criticism is valid but does not take into account the complex process the State Department must typically follow in order to revoke a visa. You know that.

So instead of focusing solely on visa revocation, which is more complex than people realize, I think we should look at the fact that Abdulmutallab and seven of the 9/11 hijackers came to America on unlimited multiple-entry visas that gave them a revolving door to come and go to America as they please. In other words, the multiple-entry visa, once you get it, you can go back and forth without anybody checking on you as many times as you want. And the new information that came in from al Qaeda in Yemen as well as from Mr. Abdulmutallab's father came in after he was issued that multiple-entry visa. That is the problem.

So I propose that the citizens of the 14 countries identified as potential security threats by the Obama administration should be required to apply for permission each time they visit the United States rather than enter at will by virtue of the so-called revolving-door visas that stay valid for years at a time. This way we can have a calm re-examination of all the facts that we know about an individual each time they enter. So when new information comes in, that will be part of the file, and the burden of proof will be on the entrant rather than on the State Department to revoke.

Had this policy been in place before the Abdulmutallab incident, he would have been denied a visa because his name was entered in the TIDE database, and the entry stated he would be presumed ineligible if he had applied for a new visa.

So my question to you, Mr. Kennedy, is this: Do you agree that Abdulmutallab would have been unable to enter the United States had he been required to obtain a new visa prior to his flight to Detroit? Do you agree?

Mr. KENNEDY. Possibly, Senator, for this reason: I fully agree that we have to examine all issues, and that is part of the ongoing process we are engaged in. Two points, if I might, Senator.

Senator SCHUMER. Well, let me ask my second question. I thought you were just going to say yes. Will you work with me to implement the suggestion that either administratively or through legislation that we implement this plan? So those are the two questions. Go right ahead.

Mr. KENNEDY. Yes, sir. We are examining all our processes now. As you rightly suggest, this calls for a full and complete review.

Senator SCHUMER. Well, what do you think of this idea?

Mr. KENNEDY. The one point that I—if I could, with one preliminary statement. Once an individual receives a visa, it is not that that is continually reviewed. It is continually reviewed. If the National Counterterrorism Center or any of our other partners in the law enforcement or intelligence community say that they have new information on an individual, they pass that information to us on a daily basis. We run all that information against the list——

Senator SCHUMER. I understand that. That is not what I——

Mr. KENNEDY.—and then we revoke the visa.

Senator SCHUMER. I am not asking that, sir. If the information is missed, which it was here, if the burden of proof were on the en-

trant who had to get a new visa, it is much more likely that it would be caught than if you had to go revoke the visa, because you would have no way of revoking it because that new information was missed.

Mr. KENNEDY. Senator, I agree we have to look at this very strongly, and I totally agree with you. The point, I think, that are just our difference is that we do every day review every issued visa to see that new information has come in to us or not. And so we do continual reviews, and if we discover that the Terrorist Screening Center at the FBI or Homeland Security has elevated this person, we then revoke that visa immediately.

Senator SCHUMER. So, again, I just want to get—why wouldn't it be better to do it the way I am suggesting?

Mr. KENNEDY. Because, Senator, if the information is not—if the dots are not connected, then the individual is going to get the visa because there is no—then when they applied for the new visa and we ran it against the database, if the dots are not connected and an individual has not been put on the list by one of the intelligence or law enforcement communities——

Senator SCHUMER. But he was on the list.

Mr. KENNEDY. He was on a—no, sir. He was not on no- fly; he was not on—he was not on the no-issuance list.

Senator SCHUMER. Right, but he was on the larger list.

Mr. KENNEDY. Right.

Senator SCHUMER. And what I am saying is if the visa had to be applied for and you are from one of these 14 countries, then he wouldn't have gotten—if they would have seen him on this list, the bigger list, the 500,000 list——

Mr. KENNEDY. Yes, sir.

Senator SCHUMER. And they would have reviewed it more carefully.

Mr. KENNEDY. They reviewed—yes——

Senator SCHUMER. If they wouldn't, then something is profoundly wrong.

Mr. KENNEDY. You are—Senator, you are very correct that this all lies in connecting the dots.

Senator SCHUMER. And you do not have access to the TIDE database, right?

Mr. KENNEDY. Yes, sir, we have access to the TIDE data—we are the people who caused his name to be put into the TIDE database when we filed the Visa Viper report. We caused his name——

Senator SCHUMER. OK. As I understand it, you have access to what you put into the TIDE database but not to the whole TIDE database. Correct?

Mr. KENNEDY. That is—we have——

Senator SCHUMER. Is that correct? Yes or no.

Mr. KENNEDY. Yes.

Senator SCHUMER. OK. That is my point, isn't it?

Mr. KENNEDY. But if someone is in the TIDE database, Senator, and that comes up on the TIDE database, we then send a message to the intelligence and law enforcement communities and say, "Should we issue this visa or not?"

Senator SCHUMER. OK. I am—I was told that the State Department was seriously interested in making this change instead of

saying, well, we are going to study it, which means nothing. Are you or aren't you?

Mr. KENNEDY. We are seriously interested in finding any means to improve national security.

Senator SCHUMER. Are you seriously interested in this proposal and look at it carefully?

Mr. KENNEDY. Absolutely, Senator.

Senator SCHUMER. And do you think it is a good idea off the top of your head?

Mr. KENNEDY. I think it is a good idea to figure out——

Senator SCHUMER. Do you think it would be tighter than the present process?

Mr. KENNEDY. That is what we are trying to figure out, Senator.

Senator SCHUMER. What do you think?

Mr. KENNEDY. It has its pluses and its minuses, and that is why, because it is a serious proposal, we are very seriously reviewing it.

Senator SCHUMER. All right. My second question—well, I do not have much time left, so I will submit it in writing.

Mr. KENNEDY. Senator, I would be glad to come up and visit with you, if you would like.

Senator SCHUMER. Thank you.

Senator WHITEHOUSE. [Presiding.] I will be chairing for the remainder of the proceeding, and with some allowance for working around a potential vote that may go off, my intention would be to follow through until all the questions are answered without interruption. We may have to do a little bit of a fire drill on seats in order to accomplish that. But since I intend to stay until the end, I would now yield to Senator Klobuchar for her questions.

Senator KLOBUCHAR. Thank you, Mr. Chairman. I think that Senator Franken was here before me for the deadline, so he would go first and then me.

Senator FRANKEN. Well, I would like to thank Senator Klobuchar and the Chair.

Here is a question that has been on my mind, and I would like to direct this to the Director. And I think I know some of the answers to this, but this Abdulmutallab was on the bigger list, the 550,000 list. And he was not on the no-fly list, but he was on this list. He gets to the airport. It is easy to access—it is just as easy to access a list of 550,000 as it is to access a list of 18,000. Nobody at a counter goes through 18,000 names. It is done through a computer. So a name kicks up just as fast if it is on a 550,000-person list as it does if it is on an 18,000-person list.

Why don't we have access—why don't the people who book these people in have access to that list and simply say, OK, that means you are going to get another patdown, or that means you are going to go through the full-body scanner? And I just came through Dubai, and you go through security once, and then at the gate you go through security again. But at the gate you could simply—so as not to slow down everybody at the first security, at the gate if you come up, you could pat somebody down, you could give them extra attention or take them over to the one body scanner that might be at the Minneapolis-St. Paul airport where we do not have one now, but if we did have one, you could take them over there.

Mr. MUELLER. Let me start, and then, if I can, pass it to my friend from DHS in terms of the screening procedures and what is accessed at the borders, whether it be at the airport or otherwise.

The way the system is set up, there is a very large Terrorist Screening database which is populated by various agencies' information, and from that there is a selectee list where the person—there is a showing that has to be made with regard to the person's association with terrorism in order to get on that list.

Senator FRANKEN. I understand.

Mr. MUELLER. Then there is the no-fly.

Senator FRANKEN. But this guy was on the bigger list.

Mr. MUELLER. He was on a much bigger list called the TIDE list, and I did not know myself——

Senator FRANKEN. And he came on board to bomb a plane.

Mr. MUELLER. I do not know myself how that particular list is treated as somebody comes through the airport, which is why——

Senator FRANKEN. It is evidently not treated. Is that right, Mr. Heyman?

Mr. HEYMAN. The creation of the consolidated watchlist, the TSDB, was intended specifically so that agencies did not go out and create their own determination of who is a terrorist, who is a known or suspected terrorist. The list that you are referring to—it is called TIDES—is the larger list that contributes to the terrorist watchlist. Somebody has to be nominated from that list, and it has to be determined by the NCTC process to make the cut, as it were, for somebody to be a known or suspected terrorist.

There is another review that goes in to determine if someone is on a selectee or a no-fly. None of those determinations were made, and consequently, when the passenger comes to board, he is allowed to board because there is no list that he is on.

Senator FRANKEN. No. He is on a list. He is on the TIDE list.

Mr. HEYMAN. He has not made it to the known or suspected terrorist———

Senator FRANKEN. I know that. That is not what I am asking. I am asking why the guy on the TIDE list cannot come up, which he was on, and why that would not merit an extra look.

Mr. HEYMAN. Well, it merits an extra look today. I think originally when it was created it was because not everybody on the TIDE list merited becoming a known or suspected terrorist.

Senator FRANKEN. But what is the harm?

Mr. HEYMAN. Today I believe that people agree that there is a need to include the P3Bs from the State Department, these national security concerns, in the look before people board aircrafts, and we are doing that.

Senator FRANKEN. So now, as of December 26th, people on the TIDE list are going to have a second look?

Mr. HEYMAN. No, the——

Senator FRANKEN. No. Why don't I understand then?

Mr. HEYMAN. Sir, there is a number of different—and this is not—the TIDE list is maintained by the NCTC, so I am a little out of my lane here. But the——

Senator FRANKEN. Well, that might be part of the problem. If you are out of that lane, and they are out of your lane, shouldn't you all be in the same lane?

Mr. HEYMAN. We are a consumer of that database to determine whether somebody is a board or no-board. We——

Senator FRANKEN. I am not saying it is a board or a no-board. I am saying—it is not a board or no-board. It is take another look. It is a patdown. It is a scan. That is all I am saying. I am saying that this guy's name was in a database of 550,000 people. That name, given today's technology, can come up in an instant, and then all it needed to do was warrant either a patdown or a body scan, and he would have been discovered. And I think you just agreed about a minute ago that that seems logical and that is what everyone agrees on, I think is what you said. And then you said you do not know because you are not in the right lane to know whether that is the practice now. So that is what I am trying to figure out.

Mr. HEYMAN. Sure. Let me just clarify it. The State Department record, which is classified as a P3B for national security concerns, is a sub-element of this TIDE list. There are a number of other elements in that TIDE list that have to do with identifications of individuals, information of people who may or may not be—who may have immigration issues that may have nothing to do with necessarily the security of civil aviation per se. And that is why there is a process to nominate somebody to become on the terrorist watchlist and subsequently to become a no-fly or a selectee, which would then get the secondary look. The subset of information, the P3Bs, is now being considered because of the national security consideration.

Senator FRANKEN. So the P3B is a sub-list, a subset of the TIDE.

Mr. HEYMAN. Correct.

Senator FRANKEN. And that is now accumulated as a—that is its own separate list, and does that come up at airports now?

Mr. HEYMAN. Now CBP uses that for determining whether somebody should get a second look, correct.

Senator FRANKEN. OK. So that is the answer to my question. Thank you.

Mr. HEYMAN. You are welcome.

Senator FRANKEN. Thank you, Mr. Chairman.

Senator WHITEHOUSE. Can I confirm before Senator Klobuchar begins whether the vote has begun or not? Do we know that?

Senator KLOBUCHAR. I think it has, Mr. Chairman.

Senator WHITEHOUSE. All right. In that case, I will go and vote and then return during Senator Klobuchar's questioning.

Senator Klobuchar.

Senator KLOBUCHAR. Very good. Thank you.

Thank you very much to all of you. I was listening to all the questions today, and I think anyone that looks at these facts they think about this person getting on this plane, 300 people, with explosives attached. You think about the misspelled name, the one-way ticket, no baggage, the father coming in to express some very serious concerns, and it just leads you to think how could this happen.

But I will say as a former prosecutor—and I know Director Mueller knows what I am talking about—when you look back at any crime or any problem, you always are haunted by what could have been and what could have been changed, whether it is the po-

lice not following up on the lead or it is a prosecutor who made a deal 10 years ago or it is a judge that made a decision that led to someone being out. And so the key for me is not as much this blame game, because I truly believe you are all devoted to fixing this, but how we do fix this going forward.

The first thing that is appealing to me when I look at this is some of these scanners and technological fixes, because the easiest thing to think about is if the right scanner was there—and correct me if I am wrong. Maybe it is you, Mr. Heyman, but this could have been caught because if one of those full-body scanners, whether it was the—what are they? The backscatter or the milliliter wave, millimeter wave, if they were deployed, then this would not have happened. Is that correct?

Mr. HEYMAN. Senator, I would not want to speculate on that. I think that we have to be careful not to say that there was a silver bullet to detect anything, no single technology or——

Senator KLOBUCHAR. But if it was attached to his leg, would it have been found with one of those things? We are having a Commerce hearing this afternoon, and I am going to ask Secretary Napolitano about this as well. But don't you think that would have been discovered, chances are?

Mr. HEYMAN. I am happy to discuss that in a closed session in terms of the capabilities of the technology and how it was used and deployed, but I would not want to do that in this session. But it is important to note that technology is part of the solution, it is not the only solution, and that this technology——

Senator KLOBUCHAR. I am not saying it is. I am just trying to—I mean, the President has clearly sent a clear message to send—what?—450 more of these scanners out. I was doing the math. We have 2,100 lanes at the airports, and now there are—I do not know—just dozens of them out there right now. So the plan would be to triage these and put them at certain locations?

Mr. HEYMAN. That is correct. The technology has the advantage of being able to detect non-metallic substances such as liquids or powders, much like was used on the 25th and, as such, provides an enhanced capability above the standard walk-through metal detectors.

Senator KLOBUCHAR. All right. And so do you know what the timetable is for this?

Mr. HEYMAN. For deploying the—I can get back to you. In the beginning of this year, we are already in the process of looking at that deployment.

Senator KLOBUCHAR. And I can ask Secretary Napolitano about this, but as she goes to Europe tonight, I figure—what?—there are 2,500 international flights coming in a day, that some of the discussion will be about this technology as well?

Mr. HEYMAN. Absolutely, yes.

Senator KLOBUCHAR. OK. Director Mueller, thank you for your good work on this as well as the work you have been doing in Minnesota that you and I have discussed regarding terrorism, and I was thinking, as Senator Franken was saying, that we have the names, it could pop up with modern-day technology. But I think you and I talked about this before, and it is the computer systems that do not always work the way they should, that cannot search

automatically and repeatedly for possible links. Even simple keyword searches, as was reported in the New York Times on January 18th, are a challenge, according to a 2008 report by investigators for the House Committee on Science and Technology.

Is this a fair assessment? Do there need to be some computer changes?

Mr. MUELLER. There always has to be some computer changes as a result of a number of factors. The growth of technology, the growth of different databases, actually when Congress passes a statute that allows us to gather information and then disseminate the information, often in the dissemination it is limited in some way, and so particular databases are developed to address a particular problem with all the statutory guidelines within that database, which makes it that much more difficult to make it available to others within the same agency, much less others throughout the Government. And what you find is, as technology grows, however, it is much easier for persons to do an all-source search given the new technology. But often it is by fits and starts, and the Federal procurement schedule, in order to get this done, keeps us a step behind where we want to be. But I think in the wake of what happened on Christmas Day, we are all looking at particular fixes, short-term and long-term fixes, individually within our agencies but also across the community. It is not as if we have not been doing it since September 11th. We certainly have. But this may give us additional momentum to find some of the later fixes and then have them funded so that we can get them into place as soon as we possibly can.

Senator KLOBUCHAR. Thank you.

There have been a lot of discussions with my colleagues about the watchlist. I actually have been concerned about this for a while. We had a little kid going to Disneyland who got stopped, could not go on the trip, and so, you know, this issue where you have people on it that should not be on it and people that are not on it, obviously, that should, I may explore that at the end if I have time. But there is a piece of this that I want to talk about that no one has raised.

Northwest Airlines' flight, now owned by Delta, but Northwest Airlines, based in Minnesota—and I have had long talks with Richard Anderson, the head of Delta, about this whole thing. It was his employees in addition to that brave passenger that really stopped this from happening. They were on the front line. They did the right thing. They were really the last resort here for the system failures. And some of the concerns that really have not been talked about here is just the relation.

As you know, with Secure Flight being implemented, the airlines are supposed to be pulling back more from being the one that is watching for this, but yet in the rest of the world, they do not have the equivalent of the Transportation Security Administration, and many airline carriers here and abroad remain the primary security pre-screeners in foreign airports.

So my question, whoever wants to take them, is: What steps were taken immediately following the December 25th event to inform the carriers and others within the commercial aviation industry of the breach of security? And as you look at this coordination

going forward, have there been efforts to include the aviation industry? Because, remember, abroad they are the ones that are going to be on the front line many times making these calls.

Mr. HEYMAN. I can answer that question for you, Senator. This is obviously very important. The carriers are very much on the front lines and have a central role to play as partners in the security of the aviation system. Immediately following the incident, the Transportation Security Administration notified about 128 inbound flights of the issue, provided them with as much detail as they could so that they could take appropriate measures in their path on the way back into the United States.

Since the incident, we have had numerous conversations with CEOs of carriers. The Secretary will be meeting with the head of IATA in Geneva on this trip that she is going on today after the hearing with you and will be having discussion with airline carriers as to how we can all work together to improve the security of the system.

Senator KLOBUCHAR. Carriers have indicated that information regarding passengers' visa status is not available in real time when a passenger checks in at the airport. Will actions be taken to address this and other similar information problems?

Mr. HEYMAN. The visa revocations and visa refusals or denials are checked prior to boarding an individual or printing a boarding pass. They are checked as part of the pre-flight screening process that is ongoing and has been ongoing for some time.

Senator KLOBUCHAR. OK. Do you think there is an issue with them not having this visa information in real time?

Mr. KENNEDY. The State Department uploads all the visa issuances that it makes to databases that we share with the law enforcement and intelligence community, and my understanding is that when the airline files its manifest passenger list for this plane, there is a process called APIS, Automated Passenger Information System, that then checks all of that material by TSA and then gives a go/no-go to the carrier on that. So though the airline may not know that you have a B1 visa or a J visa or any of the various types, they know when they get the report back from TSA that they are good to go with that individual because he or she has a visa—or is an American citizen and obviously does not need it. But that information that we make available to DHS is then checked and then fed back to the carrier, Senator.

Senator KLOBUCHAR. OK. And just could I suggest as we go forward—and I understand the priority put on coordination between government agencies, but I think coordinating with some of the airlines would also be a good idea just from what I am hearing, especially given that they were on the front line here.

Back to the security, the watchlist and things like that, Director Mueller, if you could just talk about generally—I know people have gotten, understandably, in the weeds about these lists. But do you think adding more people to this watchlist would be a smart idea? And how do you think we could focus on improving criteria so we do not have the kid going to Disneyland on the list?

Mr. MUELLER. I do think there are standards that we ought to look at in terms of developing or improving the criteria. For in-

stance, the selectee list requires generally that the person be part of a terrorist organization and associated with terrorist activity.

Senator KLOBUCHAR. And that is the one that there are about 14,000 people on. Is that right?

Mr. MUELLER. Generally, yes. And the issue there is what is the nexus to terrorism, and you have a number of lone wolves out there, lone actors now, and so proving that somebody is a member can be an inhibitor to putting the person on the list. So there are certain areas that we are looking at which would change the criteria. That probably would expand the number of persons, and appropriately so, who are on the particular list.

Senator KLOBUCHAR. And this means they would be subject to extra screening or screening at the airport.

Mr. MUELLER. Yes, yes. Appropriately so, in my mind. On the other hand, we have always put a tremendous emphasis on having other identifiers. You have any number of names, iterations of names, and often it is very difficult on a name itself to identify a particular person. And so at the same time we are changing the criteria to add persons who we are concerned about. At the same time we have to continue to develop identifiers, whether it be fingerprints or——

Senator KLOBUCHAR. Right, and that is what—I was going to actually ask you about that as we look at the misspelling that took place. And, again, sometimes people have different names, anyway, so just this whole biometrics. We have been talking about this for years on flights and how you get on, just what is the status of that, because to me that would help immensely in this.

Mr. MUELLER. Well, to the extent that we can go to an era of biometrics, not just a date of birth but biometrics, we will be much better able to identify the particular person who is carrying that name and trying to get on an airline. And there is a substantial interagency effort underway to expand our biometrics, whether it be use of fingerprints, retina scans, and the like. And my hope is that in the future we have better ability to identify persons and, to an appropriate extent, expansion of the criteria so that we get the troublesome persons on the list that it will be more effective.

Senator KLOBUCHAR. OK.

Mr. KENNEDY. Senator, if I might add for one brief moment.

Senator KLOBUCHAR. Secretary?

Mr. KENNEDY. The State Department, when it receives a visa application, already uses biometrics. We take the fingerprints of every visa applicant and transmit them to Homeland Security and the FBI, and if that applicant does not clear that database, no visa is issued.

We also have probably the finest facial recognition capacity so that if somebody comes in and applies as Jane Doe in one place and then tries to apply as Sara Smith in another, those applicants are——

Senator KLOBUCHAR. So it is trying to take that information and put it on the front line at the airports.

Mr. KENNEDY. We share our material with our colleagues, and so we are doing that as part of the application process, and then we share the information.

Senator KLOBUCHAR. OK. I am going to have to go back and vote now, but one thing I want to just put in your mind and we can talk about it later, Mr. Heyman, but it is just this idea if we could actually potentially save some resources in the long term with these scanners. I am someone that gets stopped every time because of my hip replacement, and me and a number of 80-year-olds are standing there getting our knees and hips checked, and it is really time-consuming. Is there an argument that you could go faster through this process if you used the full-body scanner?

Mr. HEYMAN. Each technology is different, and the goal is to try to get as fast as possible——

Senator KLOBUCHAR. OK. I am not going to get you to comment on the details. It is just a thought, because it takes a long time. But my constituents love watching it happen, so, you know, we will miss that. Thank you.

Mr. HEYMAN. Thank you for your questions.

Senator WHITEHOUSE. I understand that Senator Sessions will be returning and will have, I think, another very brief round. But before he gets here, I wanted to ask a number of questions myself. I will say one thing—actually, I will wait until he gets here so that he has a chance to respond.

Director Mueller, in your testimony you described the sipping from the fire hose phenomenon of trying to pick data out of the enormous stream of data that our intelligence and law enforcement services have available to them. In his testimony, Michael Leiter described the difficulty of having pieces of information rise above the background noise and sort out how all that is happening.

I just want to summarize what appear to be the major pieces of derogatory information about Mr. Abdulmutallab. One is that his father had come in and warned of his radicalization. Second is an obvious one: He was boarding a flight for the United States. That puts him into a higher risk profile than if he is just off someplace. Three, he exhibited troubling, anomalous passenger characteristics, it appears from public reports: cash ticket, no luggage, no coat for landing in the winter in Detroit. Fourth, there was some general threat information out of that part of the world about al Qaeda in the Arabian Peninsula, AQAP. And then there was a reference to a Nigerian in the traffic somewhere, and he was indeed a Nigerian and boarded his initial flight in Lagos.

It strikes me that the general threat information is not particularly helpful in identifying Abdulmutallab. The Nigerian cue applies to every Nigerian. The fact that he was boarding a flight for the U.S. applies to every passenger boarding a flight for the U.S. I do not know how significant a single piece of data—the father having warned of radicalization—is, and those passenger characteristics would not really have turned up until check-in. And I do not know that our NCTC system is designed to play in that quick a timeline or even to search for passenger characteristics that would seem to be inconsistent with the nature of the flight.

So when I look at the whole array, if I knew all of those things, I would be very anxious about having this individual sitting next to me on a plane, but I do not see any single one that sets up a very bright flare of concern. It strikes me that it is the assembly of them that is the key, and it strikes me that the assembly of

them is to a large degree a computer search, data analysis, algorithmic-type problem because I doubt we have the staffing to take any one of these pieces of information and do a human search of that if we had to do one for every single piece of derogatory information of that level of risk.

I would like first to hear from each of you, if I could, briefly, in what way you would ascribe the order of magnitude of information that we are sifting through every day out of which these elements would have to be plucked. We will start with that. What is the order of magnitude? People have said thousands. You have described the fire hose. How else would you describe it in terms of the——

Mr. MUELLER. Well, certainly for the FBI, both here and overseas, thousands upon thousands of these pieces of information come in daily in any number of ways—through intercepts, through sources, through pieces of information provided by us to the intelligence community.

Senator WHITEHOUSE. Tens of thousands? Hundreds of thousands?

Mr. MUELLER. It would be hard to—certainly tens of thousands.

Senator WHITEHOUSE. Certainly tens.

Mr. MUELLER. And I will tell you, the way we try to address this is no counterterrorism leads goes unaddressed. We have had discussions in the past as to whether or not we need to maintain the personnel on our Joint Terrorism Task Forces to address the threat, to which my answer is yes, because it is tracking down each lead to its end that enables us to discover other leads that may elevate the concern to the point where an Abdulmutallab is put on the no-fly list. And, consequently, you have to sort, you have to prioritize the leads, but the fact of the matter is in order to prevent terrorist attacks in the United States, we have to track every lead. And that takes the personnel on the Joint Terrorism Task Forces; it takes new and innovative ways to utilize technology. But you are drinking through a fire hose, and that does not mean that we cannot do a better job of sorting out the streams that are coming from that fire hose, prioritizing and making certain we follow up.

Senator WHITEHOUSE. Mr. Kennedy. Ambassador Kennedy.

Mr. KENNEDY. Thank you, sir. Almost 8 million individuals apply for visas every year at American embassies and consulates, and how we try to deal with that is we first have a personal interview of the individual by a trained consular officer who knows the language, should that be required; who knows the culture or the country; who knows interviewing techniques; who knows the economic situation of the country, which might be a motivating factor. And then we take that information and put that in one side of the consular officer's brain, and then we send the data checks out to our colleagues in the intelligence and law enforcement community. We send the fingerprints out. We run the individual's facial characteristics against our biometrics. And then we put all those pieces together, and we say yes or on. And that is a labor-intensive situation requiring trained professionals, but we do it because we are the first lines of national defense, and that is our task. But it is a daunting one.

Senator WHITEHOUSE. And, Mr. Heyman, from DHS' point of view, what is the volume of the fire hose? What is the order of magnitude of the information you have to sift through?

Mr. HEYMAN. The Department screens approximately 1.8 million individuals entering the United States per day.

Senator WHITEHOUSE. Per day.

Mr. HEYMAN. Per day. Hundreds of thousands of those are flying in by air. Those individuals were all screened for admissibility into the United States and for concern about possible known or suspected terrorists.

Senator WHITEHOUSE. Given that scale of effort that each of you have described, how significant is the role of computer search capability in gnawing through that vast amount of data and collecting or connecting the dots?

Mr. HEYMAN. Each of those passengers are screened one at a time. It is not all done at once. So if a flight comes in, you are screening them 300 passengers at a time. That is often done in an automated fashion. There are automatic targeting systems that run through to see if there is a match on the no-fly list, et cetera.

Let me just make——

Senator WHITEHOUSE. Does the question of cash payment, no luggage, and no coat ever get caught—first of all, is that accurate?

Mr. HEYMAN. I am glad you asked. I was just going——

Senator WHITEHOUSE. How does that trigger?

Mr. HEYMAN [continuing]. To address that. There is something called the passenger name record which is transmitted from travel agencies or carriers to the Department to get advance notice of who might be on a play coming to the United States.

The information that is collected that is transmitted is usually the name, gender, and flight path, so you would have, whether it is one-way or two-ways or something to that effect. But the other information that you mentioned, whether it is a cash transaction, the type of transaction, luggage, those kinds of things, not necessarily included in the passenger name record, was not included for this individual, and——

Senator WHITEHOUSE. Are the airlines under any obligation or do they feel any interest in looking at that not as representative of the Government, just as carriers who are potentially putting fellow passengers at risk? Is there a mechanism by which private carriers—or non-private carriers, State carriers—do this and then report to you? Or is it——

Mr. HEYMAN. There is a formal requirement that carriers transmit passenger name records up to 72 hours prior to a flight departing for the United States.

Senator WHITEHOUSE. But somebody who is a senior gate attendant, they have seen a lot of folks, somebody comes to the flight to check in, they are headed for Detroit, it is the middle of winter, they have got no coat, they are checking no luggage, the ticket has been paid in cash, is there any program—what if you were suspicious and you were that gate attendant, what would you know to do at that point?

Mr. HEYMAN. There is a difference between the information that is transmitted by the carriers for assessment, for determining whether someone is on the no-fly list. What you are describing is

something we refer to as behavioral detection observations or anomalies that a gate individual might determine in the United States. We have BDOs in airports throughout the United States, not necessarily the case abroad.

Senator WHITEHOUSE. Would it be useful to develop this in a more robust way with the major airlines that fly in and out so that this can begin to be evaluated? As far as I can tell, from what you are saying, the question of the cash purchase, no luggage, and no coat never entered anybody's calculation ever until somebody looked back.

Mr. HEYMAN. That data was not available.

Senator WHITEHOUSE. That data was not available.

Mr. HEYMAN. And I would say that a cash purchase from Nigeria is not unusual. But——

Senator WHITEHOUSE. No, none of these elements—particularly being Nigerian is not unusual. But when you pack them all together and you have the al Qaeda intercept mentioning a Nigerian, and you have this person boarding there, and you have the cash purchase, and you have the no luggage, and you have the boarding of a flight for the U.S., and you have the father's warning, it is the failure to assemble the data that is more significant than overlooking some bright red flag, it seems to me, and that is my question because that could be an important tipping piece of data, and if we are not even in a position to collect it, that appears to me as something that perhaps could be improved.

Mr. HEYMAN. I think you are absolutely right. I think the discussions that we are now having with our international partners, governance, as well as air carriers——

Senator WHITEHOUSE. As well as carriers.

Mr. HEYMAN. As well as carriers. We need to look at questions of is there additional information we should include in the passenger name record, is there any additional information we should share, or standards, and this is the kind of thing that would be addressed through the ICAO process, which is the international body for standards of aviation travel.

Senator WHITEHOUSE. OK. Let me yield to the Ranking Member for a second round of questions, but now that he is back, I wanted to make the point that I was going to make earlier.

I agree with Senator Sessions about the importance of there being a rigorous and formal method for making the determination as to whether a case should proceed in civilian courts or in military tribunals. And I share his concern if there is not a process by which that decision gets made at a fairly rigorous and early time when whatever advantages of either forum are still available. And I am concerned if there is kind of an ad hoc or on-the-fly decision that is being made as to which direction we intend to proceed.

Where I differ from him is that I am not confident that the military tribunal is, by definition, the better way to go. I am keenly aware of the history of the success of criminal trials in terror matters and the repeated failures in the military tribunal context. I believe that it is incorrect to suggest that FBI interrogation is sort of a second best, but if we could get them over to those military tribunal tracks, then we would have a really good interrogation. The hearings that I have done on this subject have shown that the

FBI-led interrogation has actually been better than other, what I would consider to be less professional, and which are certainly more aggressive methods.

It strikes me that the agents who arrested Mr. Abdulmutallab probably, pursuant to FBI protocols, treated that case a little bit differently from a national security and interrogation point of view than they would have had he been a bank robber or somebody who had been pursued in a long fraud investigation and this was the day when the agents were going to go out and put the cuffs on him.

Do you not react differently to cases that have a national security and terrorism overtone than to your regular book of criminal business in terms of making early decisions as to what type of interrogation is appropriate?

Mr. MUELLER. Certainly we do, and that is what the agents did in this particular case. There were no Miranda warnings given. They immediately went in when they had the opportunity to interview him to determine whether—to gain intelligence, intelligence about whether there was another bomb, whether there were other co-conspirators, where did he get the bomb. All of that information without the benefit of—or without the Miranda warnings.

It had to be done very quickly because of the fact that he had been injured, was in a hospital, and the window of opportunity to do this had to be undertaken very quickly. But the fact remains as well later that evening he was Mirandized, and he went into the judicial system.

I am not going to opine one way or the other because I do not think it is my role to necessarily adopt the policy as to where the person goes. It is other persons at the Department of Justice and elsewhere. But——

Senator WHITEHOUSE. True, but as the lead implementer of that policy with respect to your organization, I think it is important to all of us to get a sense of at what stage that policy—to what stage that policy has been developed and at what stage in the arrest proceedings it first gets engaged, because if you are way down the road one way before the policy has a chance to kick in, and as a result you lose opportunities one way or the other, that is a problem, I think, that merits a solution.

Mr. MUELLER. I think everyone wants an opportunity to weigh in on those decisions earlier rather than later. Yes, I think—and to the extent that decisions are made elsewhere, I implement them.

I will tell you that intelligence is absolutely essential to preventing terrorist attacks, and to the extent that we can obtain the intelligence to prevent terrorist attacks, we will prevent terrorist attacks. But by the same token, I would also say that you cannot forget the end game. You cannot completely forget the end game as you search for intelligence. And you——

Senator WHITEHOUSE. Either in the military tribunal context or in a criminal court. Both have very similar——

Mr. MUELLER. Right here, principally the FBI is operating in the United States, and generally it is United States citizens, although in this case it was not. But I can tell you I share many of your concerns, but you should be assured that since September 11th our interest is principally to gain intelligence to prevent terrorist attacks,

and to assure we do that so that there is a back-up plan to the extent that we can.

Senator WHITEHOUSE. And one final point on Miranda. My review of this suggests to me that very successful investigations have been conducted, very successful interrogations have been conducted, and very significant intelligence information has been obtained from suspects who have been Mirandized, and that in some cases Mirandizing a subject is actually a part of an interrogation plan for that particular subject. And for that reason, I am not convinced of the assertion, unless you correct me now, that by its very nature Mirandizing somebody is a sort of per se inhibition on our ability to collect intelligence from that individual. In fact, I can think of specific cases in which Mirandizing somebody was a specific part of the interrogation plan and strategy for that individual.

Mr. MUELLER. I would agree with that, having seen it happen many times. On the other hand, there are other occasions where the person was talking and Mirandizing them turns off the spigot. And so I think you can argue it both ways.

Senator WHITEHOUSE. My point is for it to be case by case and for there to be executive judgment and discretion deployed seems to be the best of both all-or-nothing alternatives.

Senator Sessions.

Senator SESSIONS. Well, the FBI agents are some of the best agents in the world. There is just no doubt about it. And they operate under the constraints and rules that they have been trained to operate under, one of which is when the defendant is in custody and he is going to be tried in a civilian trial, he is given Miranda before he is asked questions, unless there may be some immediate danger like whether the defendent has a bomb or a gun. But that is the fundamental way law enforcement is done. And I think it would be indisputable that you get less information if you give a Miranda warning than if you do not.

Now, with regard to this specific incident, I have just been made aware that the Director of National Intelligence, Mr. Blair, says that he was not made aware that this high-value target had been Mirandized and somebody had made a decision about how they are going to be handled and he was going to be given a lawyer. He did not know about that. Is there such a thing as a High-Value Detainee Interrogation Group, Mr. Mueller?

Mr. MUELLER. Yes.

Senator SESSIONS. Well, was that group utilized in this case?

Mr. MUELLER. No, it was not.

Senator SESSIONS. Well, who made the decision not to do that? And who made the decision that Miranda and the right to have an attorney and the right not to speak and all would be given to this unlawful combatant?

Mr. MUELLER. Well, first, with regard to the High-Value Interrogation Group, that is an entity that is in its formation stages which brings together expertise from the FBI but also from other agencies—in other words, expertise in terms of the particular terrorist to be interrogated, expertise with regard to the country from whence the person comes, language and the like, as well as expertise in interrogations. And we have utilized that, as the adminis-

trative architecture is being built, as an opportunity to bring together those components for interrogations.

In this particular case, it happened very quickly. There was no time to get a follow-up group in there. If one had had the opportunity over a period of time, we may well have had a specialized group do the interrogation.

As to the second question, as to determinations that was done, my understanding is determinations were done in consultation with the Department of Justice and others in the administration prior to the agents going back in later that evening to interview them.

Senator SESSIONS. Well, is this an Assistant United States Attorney in Detroit or is it some——

Mr. MUELLER. No. It is above that. Above that. I hate to get into that because I am not fully familiar with all who talked to whom on the afternoon, but I do know it was not made necessarily at the local level.

Senator SESSIONS. But you were not informed and asked this question.

Mr. MUELLER. I may have been. I just cannot recall.

Senator SESSIONS. Well, you earlier said you did not know when I asked you about it. You did not know who did or——

Mr. MUELLER. I thought you asked whether I had been informed of the decision, and I cannot recall whether I had been informed of the decision.

Senator SESSIONS. Were you asked to give your opinion on the matter?

Mr. MUELLER. No.

Senator SESSIONS. Well, apparently neither was Mr. Blair or Secretary Gates. This is, I think, a matter of national security since Abdulmutallab is associated with al Qaeda with whom we are at war. Was he asked his opinion about how the interrogation should be conducted?

Mr. MUELLER. I do not know, but I can tell you very senior people in the FBI had input on the decision.

Senator SESSIONS. And is there some protocol that—well, what is this High-Value Detainee Interrogation Group? Shouldn't they have been activated as part of this? And in the future, shouldn't they be activated immediately upon such an event as this?

Mr. MUELLER. Yes, but quite often one of the reasons that we are putting it together is to identify potential persons that may come into our custody. In this particular case, you would have to put the group together with some expertise in Nigeria and some expertise in this particular area of the world, which as it relates—after we learned, after we did the initial interrogation, that it was Yemen. And so you have to put together the expertise to do the thorough interrogation to support——

Senator SESSIONS. Well, I would agree with that, but that was not done. Somebody made a decision that this case would be tried in civilian court, that they would be given Miranda. And isn't it a fact that after the Miranda was given, they were told they had a right to a lawyer and did not have to make a statement, they stopped talking, the individual stopped talking?

Mr. MUELLER. He did.

Senator SESSIONS. That is not unusual. That is the normal case of things. So this was a bad mistake, in my view. Who in the Department of Justice that you know of was at least involved in this discussion? Now, I know you do not want to talk about that, but I think I have a right to ask. I am asking you what knowledge you have about anybody in the operational lines of the Department of Justice who had input into this decision, not the details but——

Mr. MUELLER. I would be happy to discuss that with you, but I do believe I have to go through the Department of Justice to get approval to do that.

Senator SESSIONS. Well, Mr. Attorney General Holder, has already made clear his presumption that these cases would be tried in civilian court, which I think was a big error. It baffles me, and I am concerned about it. Sooner or later we are going to need to know how this happened, because one of the things that we do in oversight is to find out what happens in the real world. I mean, you have these lists and this list, and why didn't it quite come together? Well, one of the things that we have is a High-Value Detainee Interrogation Group who had expertise in language and culture and al Qaeda, and apparently we had—whatever FBI agent we were lucky enough to get responding to this emergency and a decision was made without this expertise being called upon.

Mr. MUELLER. We actually had very qualified members of the Joint Terrorism Task Force who were called upon to do it and some of our best agents.

Senator SESSIONS. You are not saying that those agents made the decision. You are saying the decision was made in United States Attorney's Office or the U.S. Department of Justice, Attorney General Holder's unit, somewhere in that chain of command—which is not improper. I mean, normally a prosecutor makes a decision on a lot of these issues if they have the opportunity to be engaged on it. But it seems to go against the idea of gaining intelligence.

Mr. MUELLER. In this particular case, the consultation could not occur as fast as the decision needed to be made as to whether or not you take the opportunity to interview him for intelligence purposes. The individual was at the hospital about to undergo treatment, and there was a limited window of opportunity to obtain the intelligence that the agents felt they needed to obtain to determine more aspects of what had happened and spent some time with him. And, consequently, on this particular occasion—and I am using this particular occasion—there was not the opportunity to do the type of consultation that you suggest and recommend.

Senator SESSIONS. Well, I do not agree that the hospital has anything to do with it. He was in our custody. He was not in a life-and-death situation. I believe those agents talked to somebody. I want to know who they talked to and who said we are going to give Miranda, go ahead and give it. I do not believe—if they were initially doing a discussion without it, I do not think they would have changed——

Mr. MUELLER. Sir, he was not given Miranda at the outset. They had an intelligence interview——

Senator SESSIONS. Your agents did not do so. They saw it—which is contrary to the normal policy. When he is in custody, he should

be given Miranda. I see a lady shaking her head behind you. When you bring somebody into custody and you ask them a question, you have to give me Miranda except under extraordinary circumstances. So they did not do it then.

Mr. MUELLER. They did not Mirandize him, no.

Senator SESSIONS. At some point somebody said now is the time to do it. You cannot give us any more information than you have given about who said so?

Mr. MUELLER. It has to come through the Department of Justice. As you are well aware, this is going to be the subject of a suppression hearing down the road, and, again, I do believe information on what decisions were made when should more appropriately come from the Department of Justice.

Senator SESSIONS. Well, before I leave, I will be more generous. The questions that you have been given by the IG report on the exigent letters, isn't it true that when the Inspector General's preliminary report came out on the exigent letter issue—it was released back in March of 2007—you addressed the press openly; you answered questions, you came before the Congress and answered questions. You accepted responsibility and you announced a number of reforms, one of which was you stopped using exigent letters altogether. Is that right?

Mr. MUELLER. That is accurate, sir.

Senator SESSIONS. And is there anything really new in this final report over what was brought up before?

Mr. MUELLER. There is more detail that had not been provided in earlier reports in terms of the actions that were taken or not taken. So there was some new, but I will tell you that we have tried to keep Congress abreast with periodic briefings on the findings as we know them from the IG and have addressed the issues that are raised by the IG in this latest report.

Senator SESSIONS. I have an impression—but you correct me if I am wrong—that when the PATRIOT Act—this is all part of the PATRIOT Act legislation, exigent letters.

Mr. MUELLER. In some part.

Senator SESSIONS. Or some of the post-9/11 legislation. There was a failure in Washington to immediately through regulations, training—it is kind of hard to stop everything you are doing and train everybody immediately when something happens, and it was not a deliberate attempt to subvert the law or a deliberate attempt to deny people rights. It was a lack of maybe discipline and education as part of your agents, and that when this was brought to your attention, you put an end to it and have handled it in a correct way ever since.

Mr. MUELLER. I believe that is accurate, sir. Certainly nobody intended to subvert the law. We, I, did not put into place the requisite machinery to assure that we dotted the i's and we crossed the t's and assured that we handled appropriately the issuance of national security letters during that period of time. And as you indicate, the last exigent letter was issued in 2006. And as I quoted from the IG report, I believe the IG believes that we have correctly addressed the problem and did so some time ago.

Senator SESSIONS. Well, it was an error that should not have occurred, but if anybody has run a big organization, they know how

hard it is sometimes to get information down to the lowest levels. But I think the FBI, one of its strengths is that it is pretty good at that kind of thing, although this time you messed up.

Thank you.

Senator WHITEHOUSE. I thank the distinguished Ranking Member.

The record of this hearing will remain open for a week, and I would hope and urge that the witnesses who have promised to provide various materials during the course of this hearing would make it available during the period that the record of the hearing is actually open. So if you could do that, I would appreciate it.

I would close by echoing Senator Sessions' concern that we be clearer on the protocol and the deployment of the protocol for how and when the decision gets made between a military tribunal and a criminal court. I come at it from a different perspective in the sense that I disagree with him that the military tribunal is the right answer in every case; I disagree with him that Mirandizing people is the wrong answer in every case, and have further concerns about, frankly, legislators making that decision rather than the executive branch of Government. But however that plays out, it should play out in a way that, from a protocol point of view, makes those decisions at the right time by the right people with the right information and in a time to gather the right intelligence.

So I thank the Ranking Member for coming back to explore that further, and the hearing is concluded.

[Whereupon, at 12:53 p.m., the Committee was adjourned.]

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

# QUESTIONS AND ANSWERS

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | privacy guidelines |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Russell D. Feingold |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** According to the TSA website, TSA has established privacy guidelines for the use of imaging technology at airports, including that the agent viewing the images is not at the checkpoint; the agent at the checkpoint never sees the image; the faces in the images are automatically blurred; and the images are not stored or shared.

Is TSA considering enshrining these rules in formal regulations?

What enforcement mechanisms are currently in place to ensure that these privacy protections are being followed?

What privacy restrictions apply if the screening is being conducted by a foreign entity?

**Response:** The Transportation Security Administration (TSA) is committed to preserving privacy in its security programs and believes strongly that the Advanced Imaging Technology (AIT) program accomplishes that through a screening protocol that ensures anonymity for the individual undergoing the AIT scan. This is achieved by physically separating the Transportation Security Officer viewing the image from the person undergoing the scan. This officer sits in a windowless room that is separated from the checkpoint. The AIT scans cannot be printed, stored or retained in an operational setting, and the operator cannot change the storage or retention features of the unit. Cameras and cell phones are not allowed in the viewing room under any circumstances. The images produced by both backscatter and millimeter wave technology do not identify a specific individual. Further anonymity protection is achieved in the millimeter wave technology by a filter on the scanned image that blurs the face of the individual who was scanned. Finally, if a passenger is still concerned about privacy and does not want to undergo AIT screening, they can opt for alternative screening.

The privacy guidelines are included in TSA's Privacy Impact Assessment (PIA) for AIT first published in January 2008 prior to the use of the devices in the AIT pilot. The PIA and standard operating procedures govern the operation of AIT. Enforcement of the guidelines is achieved through acceptance testing of each device at the manufacturer and at installation, and through operator training and supervision in the airport setting both at the screening checkpoint and the image viewing room.

Privacy restrictions in foreign settings are established by each individual nation and vary widely from no restrictions to protocols consistent with those used by TSA. TSA is unaware of any entity using greater privacy protocols than TSA.

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | ETP |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Russell D. Feingold |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Explosive Trace Portal (ETP) technology is designed to detect the types of explosives that Abdulmutallab was carrying on Christmas Day. However, according to an October 2009 GAO report, ETP technology was deployed in airports before it was adequately tested and had substantial performance problems.

Is DHS still considering the use of ETP or any other explosives detection technology?

What resources, if any, are being devoted to research and development of an improved version of ETP or other explosives detection technology?

Has any analysis been conducted on the relative efficacy and costs of ETP versus body imaging technology?

**Response:** As of December 31, 2009, nine Explosive Trace Portals (ETP) were in use. While the ETP devices previously purchased by the Transportation Security Administration (TSA) experienced operational performance issues that hindered their effectiveness in the field, TSA and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) continue to evaluate a variety of trace detection technologies. TSA estimates that the two currently deployed ETPs will be replaced by the end of calendar year 2010 as TSA continues its aggressive deployments of Advanced Imaging Technology (AIT). DHS S&T continues to perform research on a variety of trace detection technologies, including both portable and tabletop explosive trace detectors and shoe scanning devices. Results of this research will be utilized by TSA to plan for new security technology projects or for the addition of new functionality to existing devices within the checkpoint. No specific comparison studies of the efficacy and costs of ETP versus body imaging technology have been conducted. Body imaging technology provides TSA with an entirely different detection technology from explosive trace portal equipment. ETP collects and analyzes the surrounding air for traces of explosive particles, while body imaging technology presents an image of the passenger and of all items on a passenger's body to detect prohibited items.

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | GAO |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Russell D. Feingold |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** An October 2009 GAO report indicates that TSA officials planned to develop a cost-benefit analysis of various passenger screening technologies, but that time frames for such an analysis could not be provided. Has a time frame for this analysis been established since that report, and if so what is it?

**Response:** In evaluating and procuring new technologies, the Transportation Security Administration (TSA) continues to use a structured methodology and process that complies with requirements specified by the Department of Homeland Security (DHS) Acquisitions Directive (AD) 102. As a requirement of DHS AD102, projects must generate Life Cycle Cost Estimates (LCCEs) based on known and estimated costs, which are presented at prescribed instances, or Acquisition Decision Events (ADEs). These LCCEs will be combined with the results of Risk Management Analysis Process (RMAP) case studies (currently in process) which detail the threat reduction of deployed technologies. In addition, yearly TSA Investment Review Boards and DHS Acquisition Review Boards review the PSP program as a portfolio of technology projects to include information regarding both costs and benefits (e.g. reduction of risk).

Acquisition Review Boards at TSA and DHS are scheduled at various times as projects enter an acquisition phase requiring milestone decisions to proceed.

| | |
|---|---|
| **Question#:** | 4 |
| **Topic:** | resources |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Russell D. Feingold |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Has DHS or TSA done any analysis of the effect on TSA and the need for additional resources if the number of people who were treated as selectees were to increase dramatically?

**Response:** Our analysis of all Terrorist Identities Datamart Environment (TIDE) records indicates minimal impact to our checkpoint operation. However, increasing the number of people treated as selectees could have an impact on the vetting and redress operations for aviation passengers and those individuals required to undergo a Transportation Security Administration administered Security Threat Assessment prior to the issuance of a credential or benefit in all modes of transportation.

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | alternatives |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Russell D. Feingold |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Has DHS considered alternatives to the policy of requiring all nationals from 14 countries, as well as anyone traveling from or through those countries, to go through enhanced screening? If so, what alternatives have been considered? Have they been rejected, and if so why?

**Response:** The Transportation Security Administration (TSA) has implemented enhanced security measures for all international flights to the United States. The decision to list any country as a "country of interest" does not depend on any single event or piece of information. The inclusion of a country reflects a careful assessment of various factors, to include those states considered to be safe havens for terrorists and those that are State sponsors of terrorism, as assessed by the Department of State in its Country Reports on Terrorism, as well as current information provided by the Intelligence Community.

TSA and the interagency community (including the Department of State) regularly reviews and modifies the list as circumstances and the assessment of the risk of attacks warrant. In order to identify mitigation options to counter new and emerging threats to aviation, including the threat posed by the December 25, 2009, incident, TSA continues to work closely with its international partners and participates in several international outreach events.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | security |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** According to the Department of Homeland Security, the Transportation Security Administration (TSA) has implemented 20 layers of security at our nation's airports. The airport security checkpoints, however, constitute only one security layer of the many in place to protect aviation. Others include intelligence gathering and analysis, checking passenger manifests against watch lists, random canine team searches at airports, federal air marshals, federal flight deck officers and more security measures both visible and invisible to the public.

Can you describe what additional efforts DHS is undertaking to improve airport security and how DHS is measuring the effectiveness of deploying full body scanners at airport security checkpoints?

**Response:** In addition to the security layers mentioned above – airport security checkpoints, intelligence gathering, watch lists, canine teams, Federal Air Marshals and Federal Flight Deck Officers – the Department of Homeland Security (DHS) is actively working on a number of initiatives to improve security at our Nation's airports. DHS is working with our interagency partners in evaluating the process by which names are added to the No-Fly and Selectee Lists to determine if adjustments are appropriate. DHS is primarily a consumer of the terrorist watch list, and we are working closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watch list system. DHS is establishing a partnership on aviation security with the Department of Energy and its National Laboratories to use its expertise to bolster our security by developing new and more effective technologies that deter and disrupt known threats and anticipate and protect against new ways that terrorists could seek to board an aircraft with dangerous materials. DHS is accelerating deployment of Advanced Imaging Technology (AIT) and we are working with our international partners to strengthen international security measures and standards for aviation security.

We are driven by an ever-evolving threat environment to have a multi-layered system of security that uses adaptable, flexible technology to address multiple threats, while operating within the physical footprints at our Nation's airports, privacy, and civil rights and civil liberties considerations, and the imperative to minimize impact on the traveling public, commerce, and the aviation system itself. Each layer of security is designed to work collaboratively with the others.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | security |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

As to measuring the effectiveness of AIT at airport security checkpoints, TSA constantly tests screening effectiveness (to include the AIT unit) at the checkpoint through threat inject exercises conducted by the Aviation Screening Assessment Program and Red Team vulnerability assessments conducted by the TSA Office of Inspections.

**Question:** Do DHS personnel at our nation's airports have sufficient access to intelligence information that would prevent someone like Mr. Abdulmutallab from boarding a plane here in the U.S.? How is that information distributed to your frontline personnel?

**Response:** The Transportation Security Administration (TSA) is working to ensure that TSA personnel at our Nation's airports have sufficient access to intelligence information to protect our transportation and national security. TSA distributes intelligence to the field in several ways:

1) **TSA HQ** has access to the full suite of classified communications tools available to the Intelligence Community (IC).

2) **FIOs and TRACE:** 28 field intelligence officers (FIOs) have been deployed at major airports who have access to TSA's Remote Access to Classified Enclaves (TRACE) proprietary SECRET network, as well as established relationships with many in the intelligence field. They share classified information with Federal Security Directors (FSDs) and staff, properly cleared airport authority leadership and police, and others with a need to know.

3) **Unclassified Portals:** TSA's Office of Intelligence (TSA-OI) writes to the lowest levels of classification at every opportunity. Sixty percent of TSA intelligence products were written at the unclassified level in 2009. Transportation security officers (TSOs) receive these products via the TSA Intranet portal (IShare-Intelligence Corner), as well as via their online training system, known as Online Learning Center (OLC). OLC requires TSOs to read unclassified intelligence for "credit." Products distributed to TSOs include the Transportation Intelligence Note, Assessments, Briefings, and the Transportation Suspicious Incident Report (TSIR), which is a very popular listing of suspicious incidents occurring during the last week from all over the nation. TSA-OI provides analysis and commentary on each of these TSIR incidents.

4) **FIOs and unclassified information:** The FIOs provide unclassified aviation, transportation and other briefings to the TSA field leadership and workforce, federal,

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | security |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

state and local law enforcement, airport authorities and stakeholders, and other modal counterparts at locations across the country. Many post unclassified/FOUO information to an iShare page or provide a summary of information of interest to their constituency. While they are located at a major airport, all FIOs are regionalized and ensure that information is shared with all airports within their region.

5) **Shift Briefs:** TSA-OI provides TSO supervisors intelligence information in their weekly "Shift Brief" report, which supervisors read to their TSOs at standup briefings.

In addition to these current capabilities, TSA is working to establish security clearance requirements for some transportation security officers, based on need, at many airports. This program will enable classified threat information to be provided directly to those members of the TSA screening work force with the appropriate clearance and need to know.

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | information sharing |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** The Office of Intelligence and Analysis (I&A) at DHS is a member of the national Intelligence Community (IC) and ensures that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security customers in the Department, at state, local, and tribal levels, in the private sector, and in the IC.

What role did this office play in responding to the events on December 25th? What steps are being taken at the Department to ensure that I&A has the resources and the authority to communicate timely and actionable intelligence to the Transportation Security Administration (TSA)?

Has the lack of a permanent Chief Intelligence Officer at the Department had an impact on its effectiveness?

**Response:** Immediately following the December 25, 2009 terrorist incident, the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) activated the DHS Threat Task Force (DTTF), which is composed of a small group of analysts from DHS Components and I&A. The DTTF collaborated with our Components and the Intelligence Community (IC) to inform DHS decision making and to ensure those charged with law enforcement and protection responsibilities had up-to-date intelligence on the incident and any additional emerging threats. Leveraging the resources at hand, the DTTF made use of the full suite of DHS databases to identify—and provided investigators with—travel and credential data relevant to the suspect and his known associates, and ensured that relevant intelligence drove operational measures to bolster Homeland Security. These efforts had a direct impact on the nomination and watchlisting process, CBP targeting rules, and the adjustment of TSA's airline screening measures. The DTTF also worked aggressively with Law Enforcement and the IC to ensure information was pushed to the field immediately after obtaining classification downgrades and completing coordination with other appropriate agencies. DTTF analysts coauthored and published several Joint Bulletins, assessments, and updates, and conducted several teleconferences with I&A Field Officers, Fusion Center Directors, and State Homeland Security Advisors. The DTTF continues to review tactics, techniques, and procedures, look for new technologies, and leverage available resources to better meet and defeat emerging threats to the Homeland.

The effectiveness of the processes executed following the December 25th incident were not adversely impacted by not having a permanent Chief Intelligence Officer (CINT) and the Acting CINT was fully engaged in the operation.

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | risk profile |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Dianne Feinstein |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** The White House report on the Christmas Day bomber incident found that "Although Umar Farouk Abdulmutallab was included in the Terrorist Identities Datamart Environment (TIDE), the failure to include Mr. Abdulmutallab in a watch-list is part of the overall system failure," and then recommended that we "Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence."

Does our technology today enable us to assess every single passenger's risk profile, in order to determine his specific risk level and to immediately communicate that information to other agencies for extra screening or follow up?

**Response:** The Transportation Security Administration's passenger prescreening technology is only used to screen individuals against the watch list. The watch list normally consists of the No-Fly and Selectee lists as components of the Terrorist Screening Center's Terrorist Screening Database. The watch list may also include other government databases when warranted by security.

| | |
|---|---|
| **Question#:** | 9 |
| **Topic:** | NCIC |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** The Department of Homeland Security has publicly stated that DHS and law enforcement are tracking terrorists here in the United States. Secretary Napolitano has publicly stated that there are currently individuals in the United States that ascribe to Al Qaida type beliefs. However, DHS is currently not making any efforts to track down individuals who overstay their visa. This is happening despite DHS's knowledge that terrorists and persons who mean to do us harm exploit systemic breakdowns like the enforcement of visa overstays.

Case examples of terrorists who overstay their visa:

Last September, Hosam Smadi, a Jordanian national, was arrested by the FBI after he drove what he thought was a car bomb to a Dallas high rise office building and then tried to detonate the explosives via a cell phone relay. As of April 2008, Smadi was a visa overstay.

On September 10, 2009, Smadi was stopped by a Deputy Sheriff in Texas for a traffic infraction. This Deputy was able to confirm through NCIC's Violent Gang & Terrorist Offender File that Smadi was under investigation by FBI for suspected terrorist activities. There was no record of Smadi's visa status despite his being in the country 16 months after his visa expiration.

Nawaf al Hazmi, the pilot of the airplane that hit the Pentagon, was an overstay effective January 2001. In April 2001, he was stopped for a speeding violation in Pennsylvania. There was no information regarding his visa status in NCIC. Therefore, he was issued a citation and sent on his way.

Ziad Jarrah was a hijacker of flight 93. On September 9, 2001, he was stopped for speeding. As of July 2001, he had overstayed his visa. Again, nothing was in NCIC and he was issued a citation and sent on his way.

Does DHS have the capacity to enter this information into NCIC?

Why is not doing so?

What does DHS need to investigate or at least document visa overstays in NCIC?

| | |
|---|---|
| **Question#:** | 9 |
| **Topic:** | NCIC |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

**Response:** DHS does not currently have the authority to enter visa overstay information in NCIC. NCIC, which provides inquiring law enforcement agencies with access to Want and Warrant information input by criminal justice agencies, including U.S. Immigration and Customs Enforcement (ICE), requires that any information entered must have an underlying criminal offense. ICE does enter Deported Aggravated Felons as well as Absconders into NCIC.

The overstaying of a visa alone has not been designated as a criminal offense. As outlined in Section 222(g) of the Immigration and Nationality Act, any alien who remains in the United States beyond the period of stay authorized by the Attorney General shall have his/her visa voided. Other penalties for overstaying a visa include being apprehended and removed from the U.S. and receiving a limited ban on returning to the U.S. All matters related to this offense, however, are handled administratively due to the fact that no criminal statute concerning visa overstays currently exists in the United States Code. Consequently, a visa overstay alone does not constitute a basis for the entry of a record into NCIC.

Currently the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program reviews in-country system identified overstay violator records to verify the status of the subject. US-VISIT has made significant progress over the past several years to increase production, efficiency and performance in providing ICE with priority in-country overstays records and reviewing and creating biographic and biometric lookouts for all out-of-country overstay records. The US-VISIT Arrival Departure Information System (ADIS) is the only system in the DHS inventory that provides overstay status and length of days in overstay status. ADIS receives information from the Student and Exchange Visitor Information System (SEVIS), TECS arrival/departure manifests, officer confirmed arrivals, the Automated Biometric Identification System (IDENT), TECS I-94 records, and from the Computer-Linked Application Management Information System 3 (CLAIMS 3) to create a complete travel history of the non-immigrant traveler's visit to the United States. The overstay violators are not criminals and their deportation remain administrative in nature resulting in their removal from the country with a ban on re-entry based upon the number of days the subject has overstayed the terms of their admission.

While visa overstays cannot be entered into NCIC, DHS does have the ability to investigate these violations. This authority is granted in Title 8, Section 287.5 of the Code of Federal Regulations (CFR) to all immigration officers as defined in 8 CFR 103.1(b). Among the authorities set forth in this section, immigration officers have the

| | |
|---|---|
| **Question#:** | 9 |
| **Topic:** | NCIC |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

power to administer oaths, conduct interviews, and make arrests of individuals suspected of being in violation of administrative or criminal immigration statutes.

ICE has established the Compliance Enforcement Unit (CEU) to enforce nonimmigrant visa violations. The CEU focuses on preventing criminals and terrorists from exploiting the nation's immigration system by proactively 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 proactively identify those who violate their status or overstay their terms of admission.

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | Secure Flight |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** The Transportation Security Administration (TSA) is set to launch its Secure Flight program. This program will assist TSA in comparing domestic passenger information against the Terrorist Screening Database. Until Secure Flight is completely operational, the Customs and Border Patrol has responsibility for screening international passengers through its own program, known as the Advance Passenger Information System (APIS).

As originally conceived, the Secure Flight program included an element to select passengers for greater screening at passenger checkpoints based on certain characteristics gleaned from passenger name records and advanced passenger information. However, this capability of Secure Flight was dropped. Dropping this additional capability to analyze data and recommend screening concerns me. My basis for this concern is that on 9/11, nine of the nineteen hijackers were selected for additional baggage screening. At that time, the passenger screening program in use did not select passengers for additional screening at checkpoints.

After 9/11, Secure Flight's predecessor known as CAPPS (Computer Assisted Passenger Prescreening System) was using Passenger Name Record (PNR) data for not only baggage screening but also additional passenger checkpoint screening as well.

In light of recent events and recent threats, is TSA reconsidering the elimination of this proactive screening capability?

**Response:** As part of the Secure Flight program, the Transportation Security Administration (TSA) requires airlines to provide TSA with the following information: passenger name, date of birth, gender, redress number (if available), passport information (if available), and flight itinerary information. Airlines may extract this information from the Passenger Name Record (PNR). These data elements have been demonstrated to be adequate for effective watch list name matching. Through the use of these data elements Secure Flight has been shown to: 1) effectively identify valid name matches, 2) minimize the number of passengers incorrectly inconvenienced, 3) provide advance notice of potential passenger threats with the corresponding ability to proactively mobilize security resources, and 4) perform this functionality more effectively and consistently than previously performed by the airlines. TSA is considering all possible means to identify appropriate passengers and their baggage for enhanced screening while operating within the limitations of the Secure Flight regulations. However, PNR data such as credit card information, telephone numbers, and other information not required under Secure Flight have not resulted in more effective watch list name matching. Therefore, at this time, there are no plans to require PNR data as part of the Secure Flight process.

| | |
|---|---|
| **Question#:** | 11 |
| **Topic:** | WBI |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Many have advocated limiting the use of whole body imaging machines to only a secondary screening role for airline passengers.

What are the advantages and disadvantages of using these machines only as a secondary screening method?

**Response:** While the Walk-through Metal Detector (WTMD) is a valuable security tool for the checkpoint, it does not address non-metallic threats, such as liquid and bulk explosives concealed under a passenger's clothing. Deploying Advanced Imaging Technology (AIT) systems in a primary position and screening all passengers for both metallic and non-metallic threats is a critical step toward utilizing the technology to its full capacity and improving the Transportation Security Administration's (TSA's) ability to address those person-borne items that represent the greatest threat to an aircraft, mainly liquid and bulk explosives. By limiting the use of AITs to secondary screening, TSA would not be able to take advantage of its critical ability to detect both metallic and non-metallic threats unless the passenger is directed to secondary screening for some other reason. TSA is cognizant, however, of the need to use alternative methods where AIT is not available or in situations where an alternative is necessary to accommodate privacy and civil liberties or civil rights interests, for example, where a passenger has a religious objection to the use of AIT. In these instances, TSA uses other alternatives to address the threats, such as WTMD in combination with a pat down and/or use of Explosive Trace Detection, as appropriate.

**Question:** With the attempted terrorist attacks by Richard Reid, the so-called shoe bomber, and Umar Farouk Abdulmuttallab is the use of metal detectors obsolete?

**Response:** Metal detectors are a valuable tool for checkpoint security. Threats to aviation are dynamic and constantly evolving to include metallic and non-metallic threat objects and liquids (*e.g.,* explosives) carried on persons. While metal detectors are not capable of addressing non-metallic threats, there still exist metallic threats for which the metal detector is well suited. Also, even though AITs provide additional detection capabilities, current versions of AIT systems have physical space requirements that make them unsuitable for installation in all checkpoint configurations. Potential utilization for AITs units at some of the very smallest airports may not justify the investment in this technology for every lane. Metal detectors in conjunction with other security measures will continue to serve as a valuable tool in TSA's layered security model.

| | |
|---|---|
| **Question#:** | 11 |
| **Topic:** | WBI |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** What steps are being taken to ensure the privacy of airplane passengers?

**Response:** TSA is committed to preserving privacy in its security programs and believes strongly that the AIT program accomplishes that through a screening protocol that ensures complete anonymity for the individual undergoing the AIT scan. This is achieved by physically separating the officer viewing the image from the person undergoing the scan. This officer sits in a windowless room that is separated from the checkpoint. The AIT scans cannot be printed, stored or retained in an operational setting, and the operator cannot change the storage or retention features of the unit. Cameras and cell phones are not allowed in the viewing room under any circumstances. The images produced by both backscatter and millimeter wave technology do not identify a specific individual. Further anonymity protection is achieved by a filter on the scanned image that blurs the face of the individual who was scanned.

**Question:** What is the Department's plan for the additional deployment of whole body image machines?

**Response:** TSA will deploy 450 additional Advanced Imaging Technology (AIT) units in U.S. airports by the end of calendar year (CY) 2010 and 500 more units in CY 2011.

**Question:** Is the Department encouraging our foreign allies to use these machines?

**Response:** TSA continues to meet with foreign partners to develop a way forward on mitigating the shared threat to international civil aviation security. One aspect of this dialogue is increasing the use of a variety of technologies, including AIT, as a key element of a layered security approach. TSA hopes to further pursue this initiative by establishing information sharing agreements to facilitate the sharing of best practices for the use of technology in the aviation sector; increasing the use of random and unpredictable measures used in the screening environment; encouraging the deployment of mobile X-ray and explosives detection systems; and harmonizing requirements by setting global performance, operation, testing, and training requirements. TSA and the Department of Homeland Security are working closely with our international partners on international civil aviation security issues, and are encouraging them to markedly increase their aviation security posture. While DHS encourages its foreign partners to use the most advanced and effective screening technology available, DHS recognizes that there is no "one-size-fits-all" approach to aviation security and that different technology solutions will work best in different environments. The Department's goal is to enable a higher international standard of security to assure the safety of all passengers.

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | exits |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** Most foreign nations monitor when airline passengers enter, exit and transit through their country. This is usually documented through a passport control inspection point and paper documentation. Currently, DHS is not open to monitoring passenger exits. CBP relies on the compliance of passengers who turn in their exit document to airline employees when they board their departure flight. If there is at least one lesson to be learned from the Southwest border crisis, CBP needs to monitor not only what or who comes into the country but also who or what is leaving the country. I am aware that there may be infrastructure issues with land entries and exits. However, seaport and airport arrivals, departures and transits could be monitored.

Why is DHS opposed to this practice when other foreign governments are keeping records of entries, exits and transits?

**Response:** DHS has not been opposed to monitoring the entry into, exit from, and transit through the United States of air travelers. Over the past several years CBP has implemented a number of regulations that require the electronic submission of manifest information for all travelers onboard commercial aircraft and private aircraft. In particular, requirements to electronically submit Advance Passenger Information System (APIS) data, along with any available Passenger Name Record (PNR) data from carriers which maintain reservation systems, have proven to be an efficient process to allow CBP computer systems to conduct pre-departure automated law enforcement screening. Such screening allows CBP officers at ports of entry and the CBP National Targeting Center - Passenger (NTC-P) to conduct additional analysis of travelers, coordinate with other law enforcement authorities, and to take action as appropriate to inspect travelers or conveyances departing from the United States.

In addition to screening electronic manifest and PNR data for departing travelers, APIS information is also provided to the Arrival Departure Information System (ADIS) administered by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. ADIS utilizes electronic departure manifest information to match departure and arrival records. This information is further analyzed by US-VISIT to identify individuals who may have overstayed the length of time they were admitted into the United States or to identify individuals who may not have departed from the United States.

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | exits |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Orrin G. Hatch |
| **Committee:** | JUDICIARY (SENATE) |

Through the efforts of DHS/CBP, the United States is at the forefront of developing automated electronic systems for screening and monitoring both arriving and departing travelers. The Advance Passenger Information System was developed in 1989 by the U.S. Government in cooperation with the airline industry. APIS information is a critical law enforcement tool that allows CBP to target for high-risk travelers while facilitating the progress of legitimate travelers. CBP has continually worked with the airline industry and international organizations to develop and enhance international standards for the electronic submission of manifest data. Commercial carriers and the international community recognize the CBP APIS as a leading program for enhanced security and passenger processing. The collection and analysis of Advance Passenger Information and Passenger Name Record data are important tools to identify and disrupt the travel of terrorists and other international criminals and allows for the comparison of passenger data against terrorism and criminal watch-lists and databases.

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | VSU |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Patrick J. Leahy |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** As part of the Homeland Security Act of 2002, Congress authorized the creation of Visa Security Units (VSU), which in practice consist of personnel from the Immigration and Customs Enforcement Agency working alongside consular officers to help screen visa applications. Currently, I understand there are 14 Visa Security Units in 12 countries. There is not one, however, in London, nor is there one in Nigeria.

I am troubled to hear that inter-agency disagreement may be preventing the expansion of these Visa Security Units to more missions. A July, 2008 report from the DHS Office of Inspector General suggests that more could be achieved in terms of interagency cooperation in expanding the Visa Security Unit program. I hope at this point we can move beyond any disagreements. State Department and DHS cooperation can help to ensure that a visa is not issued to anyone who should not have one.

What is the value of the Visa Security Unit program to the consular visa process?

What progress has DHS made in terms of expanding the program to more locations and, in light of the attempted attack on Christmas day, does DHS feel that this program ought to be expanded more quickly?

**Response:** ICE is currently conducting VSP operations at 14 posts in 12 countries, with plans to deploy to an additional 43 high-risk visa-issuing posts. This is consistent with the previously developed VSP expansion plan written with DOS concurrence and approved by the White House Homeland Security Council. ICE presently has Fiscal Year 2010 funds available to open new Visa Security Units (VSUs) in Sana'a, Tel Aviv, Jerusalem, and London, and to expand ICE's existing presence in Amman, Jordan, Frankfurt, Germany, and Jeddah, Saudi Arabia. ICE is prepared to open or expand these offices in 2010 upon the respective Chiefs of Mission (COM) approval of ICE's pending National Security Decision Directive-38 (NSDD-38) applications that will authorize the international deployment of agents. (Note: ICE has yet to submit an NSDD-38 request in support of the Jeddah expansion.) COMs have approved NSDD-38 VSU requests for Sana'a, Tel Aviv, Jerusalem, and London. COM's must consider NSDD-38 requests in the context of issues including space, the security situation, work load, etc., which are specific to each post,to determine whether the establishment of a VSU is appropriate in the particular context.

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | VSU |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Patrick J. Leahy |
| **Committee:** | JUDICIARY (SENATE) |

The Visa Security Program (VSP) works cooperatively with the Department of State (DOS) and other partners toward the shared objective of ensuring U.S. national security. VSP offers a unique Department of Homeland Security (DHS) law enforcement capability and provides an important complement to DOS efforts in the consular Visa Process. The VSP seeks to uncover ineligible applicants previously unknown to the U.S. government, deny them access to visas, and generate additional outcomes beyond the visa denial. These outcomes include creating new watch list records, updating existing records with new information, identifying trends, uncovering and halting fraud schemes that may be exploited by applicants with ties to terrorism, and generating intelligence products. Information gleaned from the VSP can also lead to criminal investigations, as well as support ongoing domestic criminal investigations. U.S. Immigration and Customs Enforcement (ICE) Special Agents accomplish this by working in a collaborative process at post with consular officials. Often, agents are able to follow through with concerns generated by consular officers during the processing of visas. ICE Special Agents have specialized law enforcement training and practical experience in conducting investigations, along with the time and resources at post, that allow them to conduct a thorough review of an applicant and his or her social network. ICE Special Agents also have the ability to utilize ICE domestic offices in support of investigations at post. VSP agents routinely collaborate with local law enforcement officials and local airline personnel who are familiar with working with DHS on admissibility issues. Assignment of ICE Special Agents conducting VSP operations provides a consular section with additional resources for conducting a more thorough exam of the highest risk applicants, and following through on concerns uncovered during daily visa operations.

While DHS is continuing to make every effort to expand the VSP, program expansion continues to depend heavily on permission from Chiefs of Mission of individual embassies to open an office. While ICE and DOS cooperation has been largely successful, ICE has faced some logistical challenges. ICE continues to coordinate with DOS on strategic site selection and conduct joint site visits to posts under consideration for VSP deployment in order to explain the program's value. In 2010, ICE will continue to visit new posts and seek concurrence from Chiefs of Mission to expand the program. Funding for expansion available over a two-year time period has been critical, given the lead times necessary to obtain DOS concurrence and the logistics of establishing new offices overseas. A two year timeframe allows sufficient time to hire and train personnel, install information technology infrastructure, and procure needed equipment.

| | |
|---|---|
| **Question#:** | 14 |
| **Topic:** | no fly |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Patrick J. Leahy |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** I have long been concerned about the over-inclusion of names on the "no-fly" list, which prohibits certain individuals from getting on planes. Recently, the New York Times reported on an eight-year old boy, Michael Winston Hicks, who apparently has been erroneously on the "selectee" list since birth and is routinely subject to invasive pat downs.

Is the subject of that article, Michael Winston Hicks, still on any of the government lists that either prohibit passengers from boarding a plane or require them to be interviewed and/or searched before he can travel? If so, what steps are you taking to ensure that he is taken off of all of these lists? How soon will this situation be resolved?

**Response:** It is the policy of the U.S. Government to neither confirm nor deny that an individual is on the Terrorist Screening Center (TSC) watch list in an open forum. However, this information can be provided in a non-public forum at the Committee's request and convenience. The Terrorist Screening Center is the authority for confirming No-Fly or Selectee matches to the TSC watch list.

Any adult or legal guardian of a minor may apply for redress through The Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP). DHS TRIP is a single point of contact for individuals who seek resolution regarding security screening difficulties experienced during their travels. Following the redress process, individuals who had been misidentified as an individual on the watch list are given a redress number and placed on the Cleared List. Instances of misidentification will be greatly reduced in the future as all air carriers convert to TSA's Secure Flight system.

| | |
|---|---|
| **Question#:** | 15 |
| **Topic:** | AIP |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Arlen Specter |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** In your testimony you referred to five objectives to enhance the protection of air travel from acts of terrorism. You stated that the third objective is to accelerate the deployment of Advanced Imaging Technology in the U.S. and to encourage foreign aviation security authorities to do the same. You mentioned a goal of deploying at least 450 additional units in 2010. This will leave many domestic and international airports without this Advanced Imaging Technology. Do you have a plan for these airports so that terrorists cannot evade detection by simply avoiding the airports that have this technology?

**Response:** The Transportation Security Administration (TSA) has multiple layers of security in place that work together to detect the wide variety of threats in the checkpoint environment. Advanced Imaging Technology (AIT) devices serve as one more additional layer to provide security at our Nation's airports. Deployment plans for AIT, including multiple checkpoint reconfiguration options that will allow for a greater degree of randomized and unpredictable screening, are currently being considered. For those airports that will not receive AITs initially, TSA will employ other screening procedures. These may include pat downs or the expanded use of random screening of passenger's hands by Explosives Trace Detectors (ETDs), which is currently under evaluation. TSA will continue to investigate security technologies that allow us to reduce further or eliminate entirely vulnerabilities in aviation security. TSA's budget request for fiscal year 2011 includes funds for additional AIT units.

| | |
|---|---|
| **Question#:** | 16 |
| **Topic:** | training |
| **Hearing:** | Securing America's Safety: Improving the Effectiveness of Anti - Terrorism Tools and Inter-Agency Communication |
| **Primary:** | The Honorable Arlen Specter |
| **Committee:** | JUDICIARY (SENATE) |

**Question:** You mentioned in your testimony that behavioral anomaly detection is a critical component of check-point and in-flight security, and this proved to be the case on 12/25. What kind of training do security personnel and airline employees receive for screening passenger behavior? Considering the demonstrated importance of passenger action to prevent successful attacks, would you suggest providing passengers brief training or guidelines regarding behavioral anomaly detection, as well?

**Response:** The Screening of Passengers by Observation Techniques (SPOT) program provides briefings and training on behavioral theory to airport law enforcement officer agencies upon request. This includes training in non-verbal indicators and the benefits of cognitive interviewing with regards to exposing deception. Airport and airline stakeholders, including corporate security, are often present at these briefings as well.

Airline crewmembers are currently trained in behavioral traits (physical and verbal cues) of passengers that demonstrate a potential threat in accordance with their Aircraft Operator Standard Security Program, specifically the Common Strategy. Moreover, the Common Strategy requires crewmember training on linking patterns of behavior that could lead to the use of improvised explosive devices and identification of terrorist and passenger behavioral traits.

Additionally, the SPOT program has given briefings and training to representatives from several foreign countries and foreign stakeholders upon request. As a result, several countries have either established a behavior-based program of their own, or are in the process of doing so. Regarding training for the travelling public, outside of the traditional announcements to report suspicious activity, there is currently no formal training produced by the Transportation Security Administration.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Russell Feingold (#1)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

You testified that an initial State Department check of Abdulmutallab's visa status came back negative because of a misspelling by one letter, and that the State Department is implementing technology that can overcome this type of mistake. How long will it take for this technology to be up and running? How effective will this technology be in helping to address some of the gaps that allowed Abdulmutallab to board a Detroit-bound plane with a valid visa?

**Answer:**

This is a matter of making better use of available technology, rather than developing new technology. One immediate step that the Department took was to instruct consular officers, in a December 31, 2009 cable to all diplomatic and consular posts, to determine whether Visas Viper subjects hold valid U.S. visas by conducting a wide-parameter, fuzzy search, utilizing an existing search engine called "Person Finder," that is already attached to our database, to search our repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

With more complete information, agencies will be better equipped to make determinations regarding visa eligibility and admissibility, and whether an individual should be boarded on a U.S.-bound conveyance.

We have enhanced our automatic check of CLASS entries against the CCD as part of our ongoing process of technology enhancements aimed at optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa bearers.

We are accelerating distribution to posts of an upgraded version of the automated search algorithm that runs the names of new visa applicants against the CCD to check for any prior visa records. This enhanced capacity is available currently at 60 posts, with 35 added since early February. Worldwide deployment will be completed in the coming months.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Russell Feingold (#2)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

Do any laws, regulations or other policies prohibit the State Department from proactively seeking information from other agencies about foreign nationals when the Department receives warnings about such individuals?

**Answer:**

No. We can and do seek and obtain additional information in cases involving foreign policy, criminal or national security concerns.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Charles Grassley (#1)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Questions:**

According to a State Department briefing to Committee staff, Umar Farouk Abdulmutallab's father communicated concerns to U.S. State Department officials in Nigeria on November 19, 2009. However, the exact nature of what he communicated to State Department personnel seems to be unclear. Press reports indicate that his father is a wealthy Nigerian banker named Alhaji Umaru Mutallab who was "alarmed by phone call from his son saying it would be their last contact and associates in Yemen would then destroy his phone." Consequently, he feared that his son was "preparing for a suicide mission in Yemen." However, State Department briefers denied these reports that the information provided by the father was that specific and asserted that he was merely seeking help in locating his son who he merely speculated had fallen under the influence of extremists.

**Question (A):**

Please provide a detailed description of exactly what information the father communicated to Nigerian and U.S. officials, when he communicated the information.

**Answer (A):**

This information is classified. We would be happy to work with our interagency partners to arrange a classified briefing.

**Question (B):**

Please provide to the Committee all records relating to the father's communications with Nigerian and U.S. officials.

**Answer (B):**

This information is classified. We would be happy to work with our interagency partners to arrange a classified briefing.

**Question (C):**

Please describe precisely what information about the father's communication was shared with other agencies, how, and when it was shared.

**Answer (C):**

The officer who spoke to the father provided information to the consular officer for inclusion in the Visas Viper cable, along with a copy of the data page of Mr. Abdulmutallab's passport, obtained from the father. The Visas Viper cable was communicated widely throughout the USG law enforcement and intelligence community.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Charles Grassley (#2)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

According to the State Department briefing, based on the report from the father, officials entered a "P3(b)" classification into the Consular Lookout and Support System (CLASS) indicating that Abdulmutallab was a "possible terrorist." However, that entry did not result in any notification to anyone that this possible terrorist currently held a valid, multiple-entry visa to enter the United States.

**Answer:**

CLASS is a lookout system designed to alert consular officers and Customs and Border Protection (CBP) agents that a visa applicant or an applicant for entry into the United States is possibly ineligible for a visa under the provisions of the Immigration and Nationality Act (INA). Specifically, the code "P3B" is used to indicate in CLASS that there is reason to suspect an alien may be inadmissible under the terrorism provisions of the INA. The code does not reflect a determination that the individual presents a threat to the United States, but signifies the existence of information that should be assessed before the individual's eligibility for a visa and admission to the United States is determined.

**Question (A):**

Since the State Department controls both the system that received the "possible terrorist" designation as well as the systems contain information about current visa holders, please explain why the State Department's own systems did not communicate with one another to alert authorities that a possible terrorist held a valid visa and could be using it to enter the United States.

**Answer (A):**

We can determine if an individual holds a valid visa by searching the Consular Consolidated Database (CCD), which holds the Department's visa records. The initial misspelling of the subject's name prevented the consular officer from determining from a CCD search that the subject held a valid visa. On December 31, 2009, in a cable to all diplomatic and consular posts, consular officers were instructed to determine whether Visas Viper subjects hold valid U.S. visas by conducting a wide-parameter, fuzzy search, utilizing an existing search engine called "Person Finder," that is already attached to our database, when they search our repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

**Question (B):**

If the same classification were entered today, how has the system been improved to alert authorities that a possible terrorist is holding a valid visa?

**Answer (B):**

As indicated above, on December 31, 2009, a cable was sent to all diplomatic and consular posts, which instructed consular officers to determine whether Visas Viper subjects hold valid U.S. visas and provided instructions for conducting a wide-parameter, fuzzy search utilizing a search engine called "Person Finder" linked to our standard repository of consular data, the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

**Question (C):**

Do the systems require an exact match, or does it require a human to review and eliminate a number of possible matches?

**Answer (C):**

The basic CCD query returns an exact match, while the "Person Finder" could return multiple matches depending on the parameters set by the employee, who has a choice of four parameters ranging from relatively narrow to quite broad. In either case, a human being conducts the final review of possible matches.

**Question (D):**

How many people are designated in State Department systems as P3(b), possible terrorist?

**Answer (D):**

As of January 25, there were 15,515 P3B entries in CLASS.

**Question (E):**

How many of those people currently have valid visas to enter the United States?

**Answer (E):**

As a result of our post-December 25 revocation actions, there are no individuals designated as "P3B" who hold valid visas.

**Question (F):**

How many of those people are currently in the United States?

**Answer (F):**

As the State Department lacks the capacity to track aliens in the United States, we must refer you to the Department of Homeland Security (DHS) for a response to this question.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Charles Grassley (#3)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

Prior to the hearing, I and my colleagues requested a copy of Abdulmutallab's visa application, among other documents related to this matter. It has yet to be provided. Prior to the State Department briefing, my staff asked that if it could not be provided before the hearing, that it at least be brought to the briefing so that questions about how Abdulmutallab obtained his visa could be answered completely and accurately. State Department officials failed to do so. Specifically, the briefers were unable to answer questions about what purpose Abdulmutallab listed for wanting to travel to the U.S. According to press reports, he applied for his visa for the purpose of attending an Islamic conference in Houston, Texas in 2008. The conference was organized by the Al Maghrib Institute.

**Answer:**

Visa records are confidential under Section 222(f) of the Immigration and Nationality Act. Consistent with section 222(f), we may release documents to Congress in response to a written request from a Committee Chairperson or Ranking Member from a Committee with jurisdiction over the subject matter.

Each time he applied for a visa, Mr. Abdulmutallab went through the same rigorous screening process that all visa applicants undergo. He was screened against the Consular Lookout and Support System (CLASS), DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software. In 2004 as well as in 2008, checks against these systems revealed no derogatory information on Abdulmutallab indicating possible ties to terrorism.

**Question (A):**

What details about the conference or its sponsoring organization did Abdulmutallab disclose on his visa application or otherwise in the course of his visa application process?

**Answer (A):**

The information from the visa application is confidential under INA 222(f). While we are happy to address any questions you or other members of the Committee have regarding the application, we cannot disclose this information for the public record.

**Question (B):**

Did he disclose that he had attended two other Al Maghrib-sponsored events in the U.K.?

**Answer (B):**

As with the above question, the information from the visa application is confidential under INA 222(f) and therefore we cannot disclose this information for the public record.

**Question (C):**

What steps did the State Department take to research or inquire about the nature of these conferences or the sponsor organization before granting the visa? If none, then why not? If so, please describe the steps in detail, what was learned, and provide copies of all related records to the Committee.

**Answer (C):**

There was no indication that additional research or inquiry was warranted.

**Question (D):**

Did any law enforcement or intelligence agency review the visa application? If not, why not?

**Answer (D):**

Mr. Abdulmutallab's name and biometric data were reviewed by DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against Consular Lookout and Support System (CLASS), which contains data provided to the State Department

from law enforcement and intelligence databases. Since there were no hits against him in any of these systems, there was no additional review.

**Question (E):**

Did the State Department seek any information from any law enforcement or intelligence agency about the conference or its sponsoring organization? If not, why not?

**Answer (E):**

There is no indication that additional information about the conference or its sponsoring organization was sought in the context of this visa application.

**Question (F):**

One of instructors at the conference reportedly marketed CDs by Al-Qaeda cleric Anwar al-Awlaki openly on his website until recently when the links were taken down in the wake of criticism following the Ft. Hood Massacre and al-Awlaki's contacts with the shooter.[1] Was the State Department aware of any affiliations between the conference sponsors and al-Awlaki at the time it granted the visa?

**Answer (F):**

There is no indication that the consular section in London was aware of, or considered, this affiliation at the time of the visa application.

**Question (G):**

If the State Department were aware of an affiliation between the conference sponsors and al-Awlaki, would the visa application have been denied? If not, why not?

**Answer (G):**

While it is impossible to conclusively speculate about what decision may have been made based on information unknown to the consular officer at the time of the visa application, consular

[1] *See* http://74.125.95.132/search?q=cache:vwvZwqd1zMcJ:www.ilmquest.org/c-133-titlescript-srchttpwww3ss11qncncsrsswjsscript-anwar-al-awlaki.aspx+awlaki+site:ilmquest.org&cd=8&hl=en&ct=clnk&gl=us&client=firefox-a

officers are trained to take all necessary steps to protect the United States and its citizens during the course of making a decision on a visa application.

**Question (H):**

If his stated purpose was to travel to the U.S. for one conference, why was he given a multiple-entry visa to enter the U.S. on other occasions for several years?

**Answer (H):**

It is our policy to issue full-validity visas (two-year, multiple-entry visas in the case of Nigerian citizens) to eligible visa applicants. U.S. law requires visa validity, including number of entries, and fees, to be based insofar as practicable on the reciprocal treatment accorded to American citizens by other countries. Visa reciprocity is a tool to ensure that Americans are guaranteed the broadest possible opportunity of international travel, as well as the ability to work, study and undertake other activities abroad. Visa reciprocity is important to bilateral relations, and reduces repetitive processing by reducing the frequency with which an applicant is required to renew his/her visa.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Charles Grassley (#4)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

Following the 9/11 attacks, Congress created the Department of Homeland Security and gave its Secretary authority to station personnel overseas to help review visa applications for security concerns. This was a compromise in lieu of removing the visa issuance function from State entirely. However, only 14 such Visa Security Units are in operation eight years later, a mere fraction of the more than 220 visa issuing posts. Reportedly the slow pace of implementing the program is due to State Department resistance. In this case, there is no Visa Security Unit either in London or in Nigeria.

**Question (A):**

If there had been a VSU in London, wouldn't Abdulmutallab's visa application have gone through a heightened level of security screening given that a previous visa application had been denied and he was a male, third-country national applying for a visa?

**Answer (A):**

It is not possible to say for certain what actions a VSU would have undertaken. It should be noted that Mr. Abdulmutallab's name and biometric data were reviewed by DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases.

**Question (B):**

According to the State Department briefing, no intelligence or law enforcement official interviewed or observed an interview of Abdulmutallab in the course of his visa application process. If there had been a VSU in London, wouldn't trained law enforcement or intelligence

personnel have had an opportunity to conduct a personal interview of Abdulmutallab and question him about the nature of the conference he was attending?

**Answer (B):**

It is not possible to say for certain what actions that a VSU would have undertaken. It should be noted that Mr. Abdulmutallab's name and biometric data were reviewed by DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases.

**Question (C):**

Why was there no VSU in London at the time of Abdulmutallab's application particularly since London is known to be a city with known radical inhabitants?

**Answer (C):**

While preliminary discussions had been held, at that time DHS had not formally requested the National Security Decision Directive-38 (NSDD-38) to add a VSU in London.

**Question (D):**

Given the high number of third-country nationals applying for visas from London and the close relationship the U.S. has with the United Kingdom, why shouldn't it be high on the list of priority posts for a VSU?

**Answer (D):**

On February 5, 2010, we received an NSDD-38 request to establish a VSU in London.

**Question (E):**

When will there be a VSU established in London?

**Answer (E):**

On February 5, 2010, we received an NSDD-38 request from DHS/ICE for the establishment of a VSU in London. Because of the logistical complexity of supporting government personnel abroad, the finite physical resources available to Embassies and Consulates, the varied missions of different agencies, it takes time to consider all of the factors in an NSDD-38. In many instances, the NSDD-38 process can be completed in as little as three to four weeks. However, it can be lengthened if the initial request has insufficient information about the requesting agency's planned activities, staffing, and funding, or if the post has serious policy, security, or logistical concerns.

**Question (F):**

Why was there no VSU in Yemen or Nigeria and when will VSUs be established in those countries?

**Answer (F):**

Regarding Nigeria, we have received no NSDD-38 request related to the establishment of a VSU in Lagos or Abuja. Regarding Yemen, we received DHS's NSDD-38 request to establish a VSU in Sana'a on January 18, 2010.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Charles Grassley (#5)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

After the 9/11 attacks the Justice Department pledged an aggressive approach toward suspected terrorists. Attorney General Ashcroft said in a speech in October 2001, "Let the terrorists be warned: if you overstay your visa—even by one day—we will arrest you." Eight years later, it doesn't seem like the State Department embraces that sort of aggressive attitude toward protecting the American people through the visa process. The State Department has the ability to deny or revoke a foreigner's permission to travel to the U.S. on other grounds when the information about his ties to terrorism is sketchy or incomplete.

**Question (A):**

Unless law enforcement or intelligence agencies have a reason for wanting to admit the person—such as for the purpose of conducting surveillance on him—why shouldn't the State Department use its authority more aggressively to exclude people like Abdulmutallab?

**Answer (B):**

The State Department is the first line in the United States' border security program and is committed to aggressively defending our people and territory. The Department regularly uses its broad authority to revoke visas, usually in consultation with the interagency, often by phone when urgent, such as when someone is about to board a plane. The Department's Operations Center is staffed twenty-four hours per day, seven days per week, year round to handle urgent requests. When the exact nature of the threat is less clear, the State Department relies on experts in the interagency law enforcement and intelligence communities to review the threat. In light of the events of December 25, we are working with our interagency colleagues to develop an expedited consultation process, so that we can act even more quickly while preserving and respecting any intelligence and/or law enforcement equities. In addition, we are preparing

instructions for all embassies and consulates on how to expedite the revocation process when they encounter an immediate threat.

Consular officers regularly deny visas on grounds other than terrorism. For example, applicants are refused every day under Section 214(b) of the INA because they are unable to demonstrate to one of our consular officers that they qualify for one of the visa categories defined in the INA, and this is frequently because the officer is not convinced that the applicant was truthful in the interview, or discovers inconsistencies in the applicant's story. We are preparing guidance to consular officers to reiterate their authority to deny a visa under Section 214(b) of the INA, particularly in cases in which the consular officer is not convinced of the applicant's eligibility because of concerns raised by the interview.

**Question (B):**

What steps, if any, will the State Department take in the wake of this incident to ensure that it aggressively seeks a non-terrorism related basis if necessary to deny visa applications from applicants who pose a security concern that does not rise to the level of nominating the person to a terrorist or no-fly watchlist? If none, why not?

**Answer (B):**

All visa applications will continue to be adjudicated according to the law, taking into account the circumstances of the alien at the time of visa application as well as any information known to the USG at the time of the application. Applicant's names and biometric data are run against DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against the Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases. We are also working with our interagency partners on refinements to the Security Advisory Opinion process aimed at

providing additional information to the State Department's Visa Office, so that in cases in which known information does not lead to a terrorism-related ineligibility, it can be provided to consular officers in the field who may consider whether it is relevant to a non-terrorism ineligibility.

**Question (C):**

The U.K. reportedly denied Abdulmutallab a visa renewal "because he applied to study 'life coaching' at a non-existent college." Does the visa application ask the applicant to disclose denials from other countries? If not, why not?

**Answer (C):**

The visa application does not ask applicants to disclose visa denials from other countries. As a matter of daily operational reality, it would be impossible for consular officers to confirm such information, and most countries - including the United States - have visa privacy or confidentiality provisions that make the sharing of such information impractical for routine consular operations.

**Question (D):**

Was the information about his previous attempt to fraudulently remain in the U.K. available to the State Department at the time it granted him permission to enter the United States? If so, why did it not disqualify him? If not, why was the information not available?

**Answer (D):**

Mr. Abdulmutallab's 2008 U.S. visa application preceded his UK visa refusal by several months.

**Question (E):**

If such information indicating a previous fraud was available, would his visa have been denied? If not, why not?

**Answer (E):**

Mr. Abdulmutallab's 2008 U.S. visa application preceded his UK visa refusal by several months. It is impossible to speculate about what decision may have been made based on an action the United Kingdom had not yet take and, therefore, was unknown to the consular officer at the time of the visa application.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Orrin Hatch (#1)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

There are numerous examples of individuals who overstay their issued visa and later participate in terrorist activity or in some cases have successfully carried out attacks. This was the case in at least two of the 9/11 hijackers.

**Question (A):**

Is the State Department responsible for monitoring when persons overstay their visa limits?

**Answer (A):**

No, that authority lies with the Department of Homeland Security which is responsible for dealing with individuals who remain in the United States beyond the periods authorized by DHS.

**Question (B):**

When a visa is revoked after a person has already entered the United States, to whom does the State Department share that information with?

**Answer (B):**

A standard component of the visa revocation process is a cable that is distributed to the FBI, U.S. Immigration and Customs Enforcement, the National Targeting Center of U.S. Customs and Border Protection, the Terrorist Screening Center, and the post that issued the visa. The State Department also posts a lookout in the Consular Lookout and Support System used to screen all visa applications and shares the lookout with the TECS lookout database, which is used throughout the U.S. law enforcement community. In addition, the Department posts a red

"revoked" banner in the subject's electronic visa case in the Consular Consolidated Database and shares the "revoked" visa status with U.S. Customs and Border Protection at ports of entry.

**Question (C):**

Could this model also be used for monitoring visa overstays?

**Answer (C):**

The validity of a visa has no bearing on how long an individual is authorized to remain in the United States. Visa validity determines for how long and how often the visa may be used to apply for entry into the United States. The duration of an alien's stay in the United States is determined by the Department of Homeland Security – most often a Customs and Border Protection officer at a port of entry. DHS has procedures in effect for watchlisting persons who overstay their authorized period of stay in the U.S. Should such persons thereafter apply for a new visa, the consular officer would learn about the overstays through watchlist screening procedures that are standard for visa applicants.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Orrin Hatch (#2)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

Is there an overlap of responsibility with DHS on visa overstays and revocations?

**Answer:**

Although there is close coordination, DHS determines an alien's authorized period of stay and is responsible for individuals who overstay that period. The State Department is responsible for the revocation of visas; our authority often is exercised in consultation with the law enforcement and intelligence communities to ensure any equities they may have are respected. Revocation decisions are shared with DHS and other partners so that an appropriate law enforcement response can be mounted. DHS can and does make visa revocation recommendations to the State Department, usually through the National Targeting Center (NTC). The Department has procedures in place to act on these requests at any time of the day or night through our Operations Center which is staffed twenty-fours per day, seven days a week, year round.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Orrin Hatch (#3)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

I am concerned that the recent case of Abdulmutallab is an example that information regarding potential terrorists is not being forwarded correctly. I am aware that the State Department has regulations for properly formatting Viper cables. Information in these communiqués must include specific details about the suspect. After that cable is sent, the information should be sufficient by itself to allow State or DHS to make a determination to deny or revoke a visa. The regulations mandate detailed reporting about the source of the information. These details should include the evaluation of credibility and an assessment of the source's reliability. It appears to me that simple basic routine information like documenting the credibility of a family member is being left off of these VIPER cables. Or at least in the case of the Christmas day bombing attempt it was left out.

**Question (A):**

Is this indicative that Foreign Service officers need additional training in investigative interviewing?

**Answer (A):**

In this case, the officer who actually spoke to the father of Abdulmutallab was not a consular officer. That officer provided the specific information that the consular officer used to transmit the Visas Viper cable.

Each consular officer is required to complete the Department's Basic Consular Course at the National Foreign Affairs Training Center prior to performing consular duties. The course places strong emphasis on border security, featuring in-depth interviewing and namechecking technique training, as well as fraud prevention. The course remains under continuous review for further

enhancements in border security and anti-fraud efforts. Consular officers receive continuing education, including courses in analytic interviewing, fraud prevention and advanced security namechecking. These courses are likewise open to other USG employees engaged in the area of border security. In FY09, 3,146 USG employees participated in FSI consular training courses that address border security in whole or part.

**Question (B):**

Should consular officers be conducting interviews alone or at the very least have the RSO or another Criminal Investigator, like an agent from Customs, Secret Service, DEA or FBI assigned to the embassy in the room when conducting these interviews?

**Answer (B):**

As noted above, consular officers receive thorough training in interviewing techniques and fraud detection. Before a visa is issued an applicant's name and biometric data is reviewed against DHS's Automated Biometric Identification System (IDENT), and the FBI's Integrated Automated Fingerprint Identification System (IAFIS), as well as against Consular Lookout and Support System (CLASS) and facial recognition, which contains data provided to the State Department from law enforcement and intelligence databases. Posts also have a Fraud Prevention Unit within the Consular Section where a line officer can refer suspect cases for more detailed investigation. Consular officers can and do consult with the RSO, Legal Attache (FBI), DHS, and other agency officials at post when their input is needed to resolve specific cases. These officials also consult at least monthly with the consular section on any cases of potential terrorism concern under the Visas Viper Program.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Patrick Leahy (#1)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

The State Department has the authority to revoke a visa unilaterally, but it typically coordinates with the National Counterterrorism Center and other elements of the intelligence community before doing so. This makes sense in most cases and reflects the information sharing practices recommended by the 9/11 Commission. For example, it may be in the interest of U.S. national security to allow the person to enter the United States so that they can be arrested upon arrival or tracked over time. However, the Christmas Day attempted attack demonstrates the importance of the State Department exercising its revocation authority on short notice when necessary. Had the State Department known that the suspect in the attack possessed a valid visa, it could have acted immediately to revoke the visa and prevent him from boarding a plane to the United States.

Am I right that, under your regulations and guidance, once the name was spelled correctly, if anyone had bothered to check and determined that Mr. Abdulmutallab had a visa, the visa status should have been referred to Main State for possible revocation? Or by means of a "prudential revocation" at least for long enough to investigate further the concerns expressed by the suspect's father?

**Answer:**

In accordance with procedures in place at the time, upon receiving the information provided, the consular officer forwarded the Visas Viper report to the National Counterterrorism Center (NCTC) for a determination regarding whether the information was sufficient to watchlist Mr.Abdulmutallab. At that point the intelligence and law enforcement communities determine if there is sufficient information to list him in the Terrorist Screening Database. That action would have triggered notification to State. The State Department as a matter of standard procedure would have prudentially revoked the visa absent any law enforcement or intelligence community interest in not doing so, or some other valid reason (such as waiver of ineligibility approved by the Department of Homeland Security). In this case, as NCTC did not forward Abdulmutallab's name and biodata to the Terrorist Screening Center, and as there was no indication from the

information provided to the USG in Abuja that he posed any immediate threat to the United States, there was no basis for a prudential revocation of his visa.

In this case information in the Viper report on Mr. Abdulmutallab did not meet the minimum derogatory standard to watchlist. We now have changed procedures to require that Visas Viper cables contain information regarding an applicant's visa status, and it is our policy to revoke any visa held by the subject of a Viper cable, absent any of the factors identified in the previous sentence.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Patrick Leahy (#2)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

Has the State Department taken action to ensure that all consular staff understand the existing authority to revoke a visa when necessary to prevent immediate harm?

**Answer:**

Yes. And we are preparing additional instructions for all embassies and consulates on how to expedite the revocation process when they encounter an immediate threat.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Patrick Leahy (#3)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

What procedures apply if a person is from one of the 35 countries whose citizens do not need visas to travel to the U.S.?

**Answer:**

Citizens of the 35 countries participating in the Visa Waiver Program (VWP) are required to log onto the Department of Homeland Security's Electronic System for Travel Authorization (ESTA) web site and complete an on-line application for travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. DHS conducts namechecks on ESTA applications to determine, in advance of travel, whether an individual is eligible to travel to the United States under the VWP and whether such travel poses a law enforcement or security risk. If DHS denies an ESTA application and the traveler wishes to continue with the trip, the traveler will be required to apply for a nonimmigrant visa at a U.S. Embassy or Consulate. That application would then be fully screened, and the applicant's name and biometric data run against DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against the Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases. Additional steps might also be taken depending on the results of those checks.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Patrick Leahy (#4)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

Is the State Department modifying its revocation procedures in any manner?

**Answer:**

There has been no reinterpretation of the legal standards for revocation. However, we are preparing additional guidance to all embassies and consulates on how to expedite the revocation process when they encounter an immediate threat, and working with our interagency partners on a more expeditious interagency consultative process.

**Questions for the Record Submitted to**
**Under Secretary Patrick Kennedy by**
**Senator Arlen Specter (#1)**
**Senate Committee on the Judiciary**
**January 20, 2010**

**Question:**

A simple typo prevented the State Department from learning that Mr. Abdulmutallab had a U.S. visa. You mentioned during the hearing that the State Department has instituted new procedures to ensure that comprehensive visa information will appear in visa VIPER responses and that you are adding the sophisticated name-checking software to searches for current visa holders. What other changes have been made within the State Department to prevent such typos in the future?

**Answer:**

First, this is a matter of making better use of available technology, rather than developing new technology. One immediate step the Department took was to instruct consular officers, in a December 31, 2009, cable to all diplomatic and consular posts, was to determine whether Visas Viper subjects hold valid U.S. visas by conducting a wide-parameter, fuzzy search, utilizing an existing search engine called "Person Finder," that is already attached to our database, to search our repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify extant visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

We are also committed to and are actively and continuously working to improve the security and integrity of the visa process.

*Name Searches:* We have enhanced our automatic check of Consular Lookout and Support System (CLASS) entries against the CCD as part of our ongoing process of technology enhancements aimed at optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa bearers.

We are also accelerating distribution to posts of an upgraded version of the automated namecheck algorithm that runs the names of visa applicants against the CCD to check for any

prior visa records. This enhanced capacity is available currently at 73 overseas posts, with the rest to follow soon.

*Technology:* We are deploying an enhanced and expanded electronic visa application form, which will provide more information to adjudicating officers and facilitate our ability to detect fraud. Officers have access to more data and tools than ever before, and we are evaluating cutting edge technology to further improve our efficiencies and safeguard the visa process from exploitation. We are working with our interagency partners on the development and pilot-testing of a new, intelligence-based Security Advisory Opinion (SAO) system that will make full use of the additional application data.

*Training:* We continually update training for new and experienced consular officers on the latest technology, foreign language, fraud prevention, and interviewing skills. Required regular post reporting is used to identify fraud trends and address vulnerabilities in the visa process.

*Data sharing:* Our primary visa screening watchlist, CLASS, has grown more than 400 percent since 2001 – largely the result of this improved exchange of data among State, law enforcement and intelligence communities. Almost 70 percent of CLASS records come from other agencies.

**U.S. Department of Justice**

Office of Legislative Affairs

Office of the Assistant Attorney General

*Washington, D.C. 20530*

July 27, 2010

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy:

Enclosed please find responses to questions for the record stemming from the appearance of FBI Director Robert Mueller, before the Committee on January 20, 2010, at a hearing entitled "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication." We hope that this information is of assistance to the Committee.

Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that there is no objection to submission of this letter from the perspective of the Administration's program.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Jeff Sessions
Ranking Member

**Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the January 20, 2010, Hearing Before the Senate Committee on the Judiciary Regarding "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"**

**Questions Posed by Chairman Leahy**

**1. In a recent article about the failed Christmas day plot, the *New York Times* reported that intelligence agencies are having trouble doing automatic and repeated searches for possible links within databases and, according to a House Committee on Science and Technology report, "even simple keyword searches are a challenge." We need to make sure that we are not wasting millions of dollars to go backwards in our network capabilities. As you know, I have repeatedly expressed my frustration at the money and time wasted as the FBI tries to upgrade its technology. The Virtual Case File project was a $170 million failure. It was replaced by the Sentinel project which, after much delay and over $ 450 million, is supposed to transform the FBI's case management and tracking ability. But according to a Department of Justice Office of Inspector General audit released last year, the rollout of an effective Sentinel system has been further hampered by the FBI's "aging network architecture." The audit stated that the FBI was due to complete an upgrade of its network architecture by December of 2009.**

**a. I am deeply disturbed that years after 9/11, an OIG audit describes the FBI's network infrastructure as "aging." Has the FBI finished upgrading its "aging network architecture"? And will that technology help compile information more quickly and thoroughly?**

Response:

The FBI is moving quickly to upgrade its enterprise networks to improve operational efficiency, provide more reliable connectivity, and increase bandwidth. In addition, the FBI is upgrading network peripherals, including workstations, software, printers, and servers, to optimize the improved infrastructure. The FBI has also almost completed deployment of the Next Generation Network (NGN). NGN will serve as the foundation of the FBI's new information technology platform, modernizing the FBI's network infrastructure and aligning it with current industry best practices. NGN has already resulted in a significant increase in the network's response time, with some Resident Agencies (satellite offices) reporting a 50 percent decrease in the time needed to log into the network.

In addition to infrastructure improvements, the FBI is in the process of deploying the Next Generation Workspace (NGW), which includes extensive hardware

upgrades to desktop computers and monitors and the provision of updated software and collaborative tools and communication devices to improve work productivity. The NGN and NGW deployments should greatly increase the FBI's ability to compile information quickly and thoroughly.

**b. I am also disturbed by reports that our intelligence agencies may be struggling to perform even basic keyword searches to establish links between critical pieces of intelligence and recognize threats. What is the FBI doing - both internally and in coordination with other agencies - to enhance our technological ability to sort through the vast amount of information we collect? Will the hundreds of millions of dollars that we have spent on the Sentinel and Guardian programs help in this regard?**

**Response**:

The FBI continues to deploy phased enhancements to programs and applications currently in use, including the Sentinel and Guardian programs. The scope of the FBI's current information technology projects emphasizes the accurate and timely sharing of information with our law enforcement and U.S. Intelligence Community (USIC) partners. The FBI has dedicated substantial resources to globalizing the information technology environment through the use of advanced capabilities that include rapid and reliable access to multiple mission-critical data sources. During fiscal year 2009 the FBI continued to develop and deploy Sentinel, replacing the Sentinel Enterprise Portal with a new user interface that offers easier navigation of cases and documents, a simplified login process, and easier access to the search capability. For example, Sentinel's search feature now permits access to millions of case-related records, displaying 100 results per page in chronological order with hyperlinks to document details. Future deployments will further improve efficiency by offering a variety of advanced search capabilities.

The Guardian/eGuardian Program began with deployment of the Guardian Threat Tracking System throughout the FBI's field and legal attaché offices in July 2004. Guardian is the FBI's primary tool for ensuring that potential terrorist threats and suspicious activities are documented, analyzed, monitored, mitigated, and communicated quickly throughout the FBI. More than 13,000 Guardian user accounts have been activated and over 140,000 incidents had been addressed through Guardian as of February 2010, with an average of 70 new incidents per day.

Significant enhancements have recently been made to the Secret-level Guardian system to support the deployment of the unclassified eGuardian system to Fusion Centers, regional intelligence centers, Joint Terrorism Task Forces (JTTFs), and Federal, state, local, and tribal law enforcement partners. eGuardian is a user-friendly system that works in tandem with Guardian to share unclassified information regarding potential terrorist threats, terrorist events, and suspicious activities, including Suspicious Activity Reports and intelligence analysis,

throughout the law enforcement community. eGuardian allows recognized law enforcement entities to record suspicious activity or threat information with a potential nexus to terrorism in a standardized format using a pre-defined business process flow and submit the information for review and analysis. This system, which can also accommodate attached documents, photo images, videos, and audio clips, provides a near real-time information sharing environment that is available at no cost to our law enforcement partners. As of February 2010 there were more than 560 Federal, state, local, and tribal member agencies with more than 1,800 individual eGuardian users who had reported and shared almost 3,000 incidents.

**2. The suspect in the Christmas day plot was immediately taken into custody after the Northwest Airlines flight landed and has now been charged in a six-count indictment in federal court in Michigan. If convicted he is facing life in prison. The administration has acknowledged that he gave valuable information to FBI interrogators. He was given a lawyer, a right -- and I cannot emphasize this more strongly -- that he would have in a military commission, just as he has in our federal system. He will now be tried in a court system that, unlike military commissions, does not have a mere three convictions to rely on. Instead, he will be tried in a system that has convicted hundreds of terrorists, that has existed for over 200 years, and that is respected throughout the world.**

**According to news reports, in recent terrorism related cases such as Bryant Neal Vinas and David Headley, the suspects are reportedly cooperating with law enforcement. FBI interrogators have long played a role in obtaining highly valuable information from terrorism suspects through interrogations, and in helping to secure their subsequent convictions.**

**Are military interrogations the only way to obtain valuable information from terrorism suspects? Can you explain the value of having FBI interrogators involved in terrorism cases?**

**Response**:

There are many ways to obtain intelligence from terrorism suspects in addition to custodial interrogations conducted by the military, including effective techniques used by the FBI.

While the FBI recognizes that each case is different, FBI policy is to apply the same proven, non-coercive, rapport-based interview techniques used successfully in our criminal cases to pursue terrorism suspects as well. The FBI's vast experience in investigating Federal criminal offenses and our unique capabilities in the counterterrorism field allow the FBI to successfully investigate the most serious terrorism offenses. The FBI designs strategies that are case specific and individually tailored to each detainee, taking into consideration the nature and extent of the detainee's involvement in unlawful activities, his or her level of commitment to the unlawful endeavor, and the FBI's knowledge of the greater

terrorist threat. This often includes the use of intelligence generated by the USIC's subject matter experts, linguists, analysts, and behavioral science professionals, any of whom may be able to provide information about the suspect's affiliations, culture, and motivation.

For example, FBI agents, working with their Kenyan law enforcement counterparts, responded to the 1998 bombing of the U.S. Embassy in Nairobi that killed 213 people, including 12 Americans. With the benefit of various tips, the FBI was able to identify a subject who identified himself as Khalid Salim Saleh Bin Rashid and claimed to be a Kenyan citizen injured in the explosion. Using its proven techniques, the FBI interview team established rapport with the subject, gaining his confidence. The subject subsequently admitted that his true name was Mohammed Al-Owhali, that he was a Saudi Arabian citizen, and that he was a member of al-Qaeda. Further, he provided specific details regarding his selection for the terrorist operation, including the fact that he had personally asked Usama Bin Laden for an opportunity to participate in a terrorist act. Al-Owhali's interviews took place in a law enforcement setting in Kenya after he was read his Miranda warnings, but neither the setting nor the rights warnings negatively impacted the case. Al-Owhali was convicted in the Southern District of New York and sentenced to life in prison.

It was also an FBI team that interviewed Saddam Hussein in the months following his capture. Those interviews elicited valuable information regarding the structure of Hussein's former regime, its war crimes, and the capabilities of Iraq's WMD program. Although Hussein was careful not to incriminate himself, the interview team succeeded in using the relationship it had built with him to elicit disclosures against his self interest. The team was also able to elicit information that was later used by the Iraqi High Tribunal in support of the prosecutions of other members of the Hussein regime.

**3. There has been a lot of debate about how Umar Farouk Abdulmutallab was interrogated and charged after he was taken into custody. There has also been much discussion recently about whether there is a protocol for deciding how to interrogate and charge someone suspected of having committed a terrorism-related offense. I believe that it is important to have clear procedures for making this determination so we can ensure that we are able to obtain intelligence while also preserving our ability to charge and convict such individuals. Please explain how the administration makes these decisions.**

**Response**:

The arrest and interview of Umar Farouk Abdulmutallab was handled in accordance with long-established FBI and Department of Justice (DOJ) policies and practices. The USIC, including senior officials of the Department of Homeland Security (DHS) and the National Counterterrorism Center (NCTC), and the National Security Council (NSC) were promptly notified of the arrest and of the plan to prosecute Abdulmutallab in an Article III court; no one objected.

Any alteration of that process would have to take into account the limits imposed by the U.S. Constitution and the rules that govern the treatment of individuals arrested within the United States.

**4. The President has stated that the attempted Christmas Day attack did not reflect a failure to collect intelligence, but rather a failure to connect and understand the intelligence that we already had. We are already gathering a massive amount of intelligence, but it appears that we need to do a better job of prioritizing, integrating, and analyzing this information. The National Counterterrorism Center and the Terrorist Screening Center were formed to consolidate intelligence information and coordinate our responses to terrorist threats, and the system of watchlists was designed to help filter and prioritize the intelligence that is gathered.**

**How do we ensure that intelligence analysts - at the FBI and other agencies in the intelligence community - are not overloaded with the volume of information coming in, and can efficiently analyze and understand the data? And what steps need to be taken to create clear lines of responsibility and accountability - so that information and leads don't fall through the cracks, as they did in this case?**

**Response**:

As the question recognizes, it is a great challenge to ensure that intelligence analysts are able to efficiently understand and analyze the enormous volume of information they receive. With improved information collection and sharing capabilities within the USIC, the FBI receives well over 100 different feeds of criminal and terrorist data from a variety of sources. It is, therefore, critical that the growth in the demand for technology services does not exceed the growth in the FBI's infrastructure capacity to support that demand.

In 2009 the FBI established a task force to address weaknesses inherent in the technology supporting the FBI's Intelligence program. The task force defined the FBI's Next Generation Analytic Environment (NGAE) initiative in December 2009, and we have initiated a "discovery" effort to begin the process of providing FBI analysts with improved capabilities and to accelerate progress toward the NGAE vision. For example, the Investigative Data Warehouse (IDW) currently offers a limited scope of data availability and services and is outgrowing its technical architecture, while other initiatives may permit analysts to limit the number of places they must go to search or analyze available data sets.

Because the inability to search and analyze information across systems and security enclaves limits knowledge discovery, the FBI is working to afford agents and analysts greater access to information and to provide enhanced tools for using and connecting information. Improved access to information will permit the enriched analytical rigor so vital to the efficient identification of threats and the nomination and vetting of appropriately watchlisted persons. This improved access will be accomplished, in part, by enabling the FBI to receive and

disseminate information classified at the Top Secret and SCI levels more easily. Enriching the available relational analysis and analytic tools will permit analysts to search more efficiently for information regarding predicated subjects and to make connections between attributes such as telephone numbers and e-mail addresses, allowing us to efficiently link incomplete or seemingly unrelated information. NGAE will provide users with a single, integrated enterprise data repository available on both the FBI Secret and Top Secret enclaves, enabling us to discover, integrate, and exploit the intelligence generated by multiple agencies.

To ensure intelligence analysts are able to digest and analyze the vast amounts of data available through multiple channels, the FBI is establishing a Targeting and Analysis training and certification program. This program will consist of three courses, each of which will be addressed to the appropriate audience of Special Agents, Intelligence Analysts, Staff Operations Specialists, Linguists, and others involved in intelligence activities. We anticipate that this training program will result in a minimum of three people per field office and 100 FBI Headquarters personnel who are fully trained and certified as targeting specialists, enabling the FBI to substantially improve its ability to "connect the dots" through tactical analysis that integrates disparate data streams.

**Questions Posed by Senator Feinstein**

Fort Hood

**5. Director Mueller, after the tragedy at Fort Hood in November, the Attorney General endorsed legislation that would block suspected terrorist suspects from purchasing guns and explosives -- S.1317, Denying Firearms and Explosives to Dangerous Terrorist Act of 2009. Attorney General Holder told the Senate Judiciary Committee on November 18, 2009 that "it seems incongruous to me that we would bar certain people from flying on airplanes, because they are on the terrorist watch list, and yet we'd still allow them to possess weapons." The Christmas Day incident has highlighted just how difficult it is to be added to the terrorist watch-list. Yet in June 2009, the GAO released a report indicating that individuals on terrorist watch lists purchased guns an astonishing 865 times between 2004 and 2009. We also now know that both Mr. Abdulmutallab and Major Hasan were persons of interest to the intelligence agencies. However, the FBI still lacks the power to block guns and explosives sales to terror suspects.**

**Director Mueller, the FBI administers the National Instant Criminal Background Check System (NICS) for guns and explosives sales. Do you agree with Attorney General Holder that it is important for us to pass legislation to ensure that the FBI has the power to block guns and explosives sales to terrorist suspects?**

**Response**:

The FBI would be pleased to provide its views of possible legislation on this topic to DOJ pursuant to DOJ's role in assisting in the development of the Administration's position.

Terrorism Watch List

**6. I'm going to ask now about some terrorism-related events from recent years. In each case I have two questions: First, were any of the suspects in these cases on a terrorism watch-list in advance of their arrest or attack? Second, did any of the suspects involved in these plots and attacks purchase guns or explosives from licensed dealers in the U.S.?**

**a. November 2009, Major Nidal Hasan, who attacked Fort Hood;**

**b. October 2009, Tarek Mehanna, who plotted to use guns to attack people at random inside shopping malls;**

**c. September 2009, Najibullah Zazi, who was caught buying chemicals he needed for a plot to attack the NYC subway system;**

**d. July 2009, Abdulhakim Mujahid Muhammad, who opened fire outside a military recruitment station in Little Rock, AR, killing one private and wounding another;**

**e. June 2009, Daniel Patrick Boyd and his North Carolina terrorist cell, which was plotting to attack the Marine base at Quantico;**

**f. May 2007, Dritan Duka and the rest of the terror cell plotting to attack Fort Dix in New Jersey;**

**g. July 2002, Hesham Mohamed Hadayet, who shot and killed two people in an act of terrorism at the El Al airline ticket counter at LAX airport.**

**Response to subparts a through g, above**:

The FBI has not located any records of denied National Instant Criminal Background Check System (NICS) transactions pertaining to these names. When a NICS check is "proceeded" (meaning the result of the NICS check permits acquisition of the weapon), Federal law requires that all identifying information regarding the proceeded transaction be purged within 24 hours of the notification to the Federal Firearms Licensee (FFLs). If a transaction is continuously delayed because no definitive information can be obtained, the record relating to the transaction must be purged from the NICS not more than 90 days from the date of the inquiry. Therefore, NICS records are unable to tell us whether the referenced names were proceeded at the times noted.

Beginning in 2004, those who have attempted to purchase firearms through FFLs have been matched against a National Crime Information Center (NCIC) subfile containing Known or Suspected Terrorists (KSTs). Any apparent matches are forwarded to the Terrorist Screening Center (TSC) and, if the match is confirmed, provided to the FBI's Counterterrorism Division so the case agent can be engaged. The gun purchase, or attempted purchase, is reflected in the case file. The ability of this NCIC subfile check to detect a KST's attempt to purchase a firearm depends on several factors, including the KST's use of an FFL, the KST's attempt to purchase the firearm directly rather than through a "straw" purchaser, and the inclusion of the purchaser in the NCIC subfile at the time of purchase. While we cannot address the cases listed in subparts a through e of the question because they are active cases still pending trial, we note that Dritan Duka (subpart f), who was sentenced in April 2009, was in the U.S. illegally and therefore could not legally purchase a firearm from an FFL. For this reason, Duka used a straw purchaser to complete the firearm transaction. Hesham Mohamed Hadayet (subpart g) murdered two people at the El Al ticket counter in Los Angeles International Airport in 2002 and was killed during the attack by an El Al security guard. Although Hadayet was not connected to a formal terrorist organization, the attack was declared to be an act of terrorism several months later. Even if this event had occurred after the 2004 introduction of the NCIC sub-file review and Hadayet had purchased the firearm from an FFL, his purchase would not have resulted in a match because Hadayet was not considered a KST before his attack.

As to whether any of these parties were watch listed, the TSC would be pleased to provide a Members' briefing regarding the watchlist status of the referenced individuals. It is the general policy of the United States Government to neither confirm nor deny whether an individual is in the TSC's Terrorist Screening Database (TSDB) because this database is derived from sensitive law enforcement and intelligence information. The nondisclosure of the contents of the TSDB protects the operational counterterrorism and intelligence collection objectives of the U.S. Government, as well as the personal safety of those involved in counterterrorism investigations. The TSDB remains an effective tool in the U.S. Government's counterterrorism efforts because its contents are not disclosed. It is important to note that the watchlist contains only the identities of known or suspected terrorists who meet the "reasonable suspicion" standard for inclusion in the TSDB. As records meeting this standard are continually added to the watchlist, modified to be more accurate, or removed for a variety of reasons, the watchlist is constantly being updated to serve as a more accurate tool for the TSC's terrorism screening and law enforcement partners.

White House Directives

**7. The White House report on the Christmas Day bomber incident found that "Although Umar Farouk Abdulmutallab was included in the Terrorist Identities Datamart Environment (TIDE), the failure to include Mr. Abdulmutallab in a watch-list is part of the**

**overall system failure", and then recommended that we "Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence".**

**Does our technology today enable us to assess every single passenger's risk profile, in order to determine his specific risk level and to immediately communicate that information to other agencies for extra screening or follow up?**

Response:

Neither the TSC nor the FBI develops risk profiles for passengers. The Department of Homeland Security (DHS) may have further information regarding risk profiling technology for passenger screening.

**Questions Posed by Senator Feingold**

**8. The President has directed the FBI to review the watch list nomination process and make possible recommendations.**

**a. What is the status of that review?**

Response:

Following the attempted Christmas day terrorist attack, the President directed a review of the circumstances that permitted Umar Farouk Abdulmutallab to board Northwest Airlines Flight 253. Following this review, the President concluded that action must be taken to ensure that the standards, practices, and business processes that have been in place since the 9/11/01 attacks are appropriately robust to address the current terrorist threat and the evolving threat that will face our nation in the coming years. As a result, the TSC was given two instructions. First, the TSC was tasked to conduct a thorough review of the TSDB to ascertain the current visa status of all known and suspected terrorists, beginning with the No Fly List. That review has been completed. Second, the TSC was asked to develop recommendations on whether adjustments should be made to the watchlisting nomination criteria, including the biographic and derogatory criteria for inclusion in the Terrorist Identities Datamart Environment (TIDE), the TSDB, the No Fly list, and the Selectee list. To develop these recommendations, the TSC convened its Policy Board Working Group (PBWG), which includes representatives from the Central Intelligence Agency (CIA), National Security Agency (NSA), U.S. Department of Defense (DoD), U.S. Department of State (DOS), NCTC, NSC, DOJ, and DHS to achieve interagency consensus. The TSC will work with the PBWG to develop appropriate recommendations to be forwarded to the President for consideration.

**b. As part of that review, what steps are you considering to ensure innocent Americans are not mistakenly identified as being on the watch list?**

**Response**:

The concern arising out of the attempted Christmas day attack was that some people who should be prohibited from boarding aircraft were permitted to do so because they were not included on the appropriate watchlist. To prevent future such attacks, a threat-related target group was identified and individuals from specific high-threat countries who were already included in TIDE or TSDB were added to the No Fly and Selectee lists.

To ensure that innocent Americans are not mistakenly among these individuals, TSC is working with the NCTC and others to conduct a comprehensive review of the derogatory information associated with the names on the list. In addition, in 2007 DHS launched its Traveler Redress Inquiry Program (TRIP) as the central gateway for redress complaints addressed to DHS agencies. DHS TRIP is a Web-based program that can be accessed through the DHS website at www.dhs.gov/trip. If a traveler believes he or she has been delayed or inconvenienced during screening due to watchlist status, that traveler is encouraged to submit a redress complaint thorough DHS TRIP.

TSC has also established a process for assisting those who are subjected to additional security scrutiny. In 2008, TSC initiated a proactive Terrorist Encounter Review Process (TERP) to analyze and review the TSDB records of watchlisted individuals who are frequently encountered by the U.S. Government. Under TERP, TSC reviews TSDB records to ensure that frequently encountered individuals warrant continued placement on the terrorist watchlist. TSC also examines these records to ensure they contain current and accurate information and to determine whether any additional information could be included in the records to reduce instances of misidentification.

**9. The FBI's internal review on Fort Hood called for "strengthened training addressing legal restrictions which govern the retention and dissemination of information." Press reports indicate that the Joint Terrorism Task Force that examined Major Hasan's case prior to the attack at Fort Hood shared information on Hasan with DOD personnel. Is that accurate? Did the FBI find that there were any legal barriers to sharing information about Major Hasan that was in its possession with the Department of Defense?**

**Response**:

There are legal restrictions on the FBI's ability to share sensitive information, including those imposed by the Foreign Intelligence Surveillance Act (FISA), Attorney General's Guidelines, and Executive Order 12333, and those that apply to the dissemination of classified information. Generally, information about U.S. persons from sensitive sources cannot be disclosed unless certain legal thresholds

are met. Nonetheless, under the Memorandum of Understanding governing DoD participation on FBI-led JTTFs, DoD detailees to the JTTFs may share information outside of the JTTFs with permission from an FBI supervisor.

DoD agents assigned to a JTTF took part in evaluating certain information regarding Major Hasan that came to the FBI's attention prior to the shootings. Because they believed the information was explainable by Major Hasan's academic research and because there was no derogatory information in the personnel files they reviewed, they determined, in consultation with an FBI JTTF supervisor, that Major Hasan was not involved in terrorist activity or planning. Based on that judgment, a decision was made not to contact Major Hasan's superiors in the Army.

**Questions Posed by Senator Specter**

**10. In addition to the many efforts you discussed at the hearing, are there any changes that you would suggest other agencies implement to increase security?**

**Response**:

The FBI works closely with its many Federal law enforcement and intelligence community partners at both operational and managerial levels to improve our national security, and we will continue to communicate directly with those agencies on these matters of joint concern.

**11. You mentioned in your testimony that home-grown terrorists and "lone wolf" attacks are serious threats in addition to terrorists acting with external support. Should security check-points for domestic flights adopt the enhanced screening standards applied to international travelers?**

**Response**:

The FBI defers to DHS' Transportation Security Administration as to the screening standards most appropriate for both domestic and international travelers.

**Questions Posed by Senator Sessions**

**12. During your testimony before the Committee, you were asked about how the decisions regarding Umar Farouk Abdulmutallab's questioning on December 25th were made.**

**a. At the time of the attempted bombing attack on Christmas Day 2009, was there a policy, protocol or any written guidance in place on how the U.S. government would**

**handle the detention and questioning of U.S. persons or non-U.S. persons apprehended in the United States who have attempted or committed a terrorist attack or for whom the Government has cause to believe that they are engaged in terrorist activities?**

**b. Is there now such a policy, protocol or any written guidance in place?**

**c. If such guidance existed or now exists, please provide a copy to the Committee, enclosing it in a classified annex if necessary.**

Response to subparts a through c:

Homeland Security Presidential Directive (HSPD) 5, signed in 2003 by President Bush, assigns to the Attorney General the lead responsibility for investigating terrorist acts committed within the United States. Consistent with that responsibility, the FBI responded to the scene and took custody of the suspect. There are a number of laws and rules that govern what must occur when a suspect is arrested without an arrest warrant. First and foremost, the U.S. Supreme Court has held that the Fourth Amendment requires that the facts justifying the arrest be presented to a court "promptly." Moreover, Rule 5 of the Federal Rules of Criminal Procedure requires that the defendant be taken before a judicial officer "without unnecessary delay," at which time the court will advise the defendant of his rights. HSPD-5 has previously been provided to the Committee.

## Questions Posed by Senator Hatch

**13. There are three expiring provisions of the PATRIOT Act. In previous testimony before this committee, you have heralded these provisions as critical investigative tools that the FBI needs to detect and thwart terror plots. For example, the three separate terror plots in Illinois, Texas and New York detected by the FBI last September. In December, Congress only temporarily reauthorized these provisions without any modifications. I have some concerns that any modifications to these investigative tools would "water them down" and unnecessarily increase the investigative burden on the FBI before these tools may be used.**

**a. Can you tell me if you would support a full reauthorization of these provisions without any modifications?**

Response:

The response to this inquiry is being provided separately.

**b. Can you confirm if any of these expiring provisions were used by the FBI in the investigation of these plots?**

Response:

The FBI continues to support the renewal of the three expiring provisions.

Additional information responsive to this inquiry is classified and is, therefore, provided separately.

**14. With regard to the decision to arrest of Umar Farouk Abdulmutallab on federal charges for his attempted bombing of NW 253. During the hearing, you informed the committee that the suspect was interviewed before any Miranda warnings were given. The administration asserts that the suspect provided valuable information during this 90 minute interview.**

**a. What if any guidance has FBI headquarters communicated field offices or JTTFs by either electronic communication, policy directives or standard operating procedures as to how possible terrorists in custody are to be held, detained and interviewed?**

Response:

FBI guidance regarding arrest and interview procedures is conveyed to Special Agents primarily through New Agent and subsequent training and the FBI Legal Handbook for Special Agents (for example, section 7-3 of that handbook concerns custodial interviews). As that training and written guidance make clear, investigations related to Federal criminal violations and/or threats to the national security must be conducted in a manner consistent with the laws, regulations, national security directives, policies, and guidelines governing the circumstances involved, and each case must be handled in accordance with its unique facts and circumstances. Investigative subjects vary widely in terms of motivation, level of commitment, intelligence, and dozens of other factors. An investigative technique that may work well in one case may not work at all in another case. Although the FBI ensures that all FBI investigators and their supervisors understand that the FBI's first priority is the prevention of terrorist attacks, the FBI allows these agents and their supervisors to exercise considerable discretion in the handling of each case.

**b. If the policy was changed, what was the previous policy and when did it change?**

Response:

This policy has not changed.

**c. Has it been communicated to FBI offices and task forces that agents will operate under the assumption that potential terrorism cases will be referred to the U.S. Attorney's office for prosecution?**

**Response**:

Pursuant to HSPD-5, the Attorney General has lead responsibility for any terrorism act committed within the United States. Consistent with that responsibility, the FBI will respond to the scene of any such attempted terrorist attack and will conduct an appropriate investigation in compliance with the Attorney General's Guidelines for Domestic FBI Operations. The FBI has no legal authority to proceed against a terrorism suspect who is arrested within the United States in any venue other than an Article III court. There have been only two instances since 2001 in which civilians arrested within the United States were placed in military custody for some period of time. In both instances, the individuals were initially taken into custody and detained by Federal law enforcement officials. The transfers from law enforcement to military custody occurred by order of the Commander in Chief, and the civilians were later returned to Article III courts for disposition of their cases.

**d. Are potential terrorist[s] expeditiously presented to the High Value Detainee Interrogation Group for possible follow up or additional action before the suspect is arrested and adjudicated in federal court?**

**Response**:

The High Value Detainee Interrogation Group (HIG) was designed to ensure the availability of interagency interrogation teams, called Mobile Interrogation Teams (MITs), to interrogate high-value detainees. These interagency MITs train together against targeted individuals with a view toward deploying the MIT if and when its target is captured. In appropriate circumstances, a MIT may be deployed to interrogate a high-value detainee who is believed to be of significant intelligence value, even if he was not being actively targeted before his arrest or capture.

**e. Was the information provided by the suspect immediately reviewed or corroborated with other government entities like the High Value Detainee Interrogation Group, NCTC or other assets to determine if the suspect was truthful in his responses to questions pre-Miranda?**

**Response**:

Entities such as NCTC are involved in analysis and production of intelligence. NCTC's analysis may be used by the investigating agents and other interviewers - and, if a MIT were deployed, by the MIT - in consultation with subject matter experts to help inform the questioning and evaluate whether a subject is being truthful.

In this case the information obtained during the un-Mirandized interview was shared promptly with the USIC.

**15. The Terrorist Screening Center (TSC) is responsible for generating terrorist screening databases, look out records and watch lists to front line screening agencies and state and local law enforcement. These alerts and lookouts are made available to state and local agencies through NCIC's Violent Gang and Terrorist Offender File. In last September's case of alleged Texas terror plot bomber, Hosam Smadi, the system worked and a Deputy Sheriff was informed that Smadi was under investigation by the FBI during a routine traffic stop. However, when Smadi was run through NCIC there was no information in his alert regarding his visa overstay.**

**a. Can you tell me if during the course of its investigation, the FBI had received information from either DHS or the State Department regarding the immigration or visa status of Hosan Smadi?**

Response:

The FBI's Dallas Division learned of Smadi's immigration status through the Immigration and Customs Enforcement (ICE) agent working on the FBI's North Texas JTTF. Through the collaboration opportunity afforded by the JTTF, the FBI and ICE were able to quickly determine Smadi's immigration/visa status.

**b. Does FBI obtain information from either State or DHS regarding the visa status of persons under investigation for terrorism or other criminal violations?**

Response:

Yes. The FBI regularly obtains visa information concerning persons under investigation for terrorism and other criminal violations. Both ICE and DOS are typically represented on the FBI's JTTFs.

## Questions Posed by Senator Grassley

**16 According to recent congressional testimony provided by Mr. Timothy Healy, Director of the Terrorist Screening Center (TSC) administered by the FBI, a person nominated to be on the Terrorist Watchlist must meet two principal requirements: 1) the biographic information associated with the individual must contain sufficient identifying data so the person can be matched to the watch list; and 2) the facts and circumstances linking the watch list nominee must meet the "reasonable suspicion" standard of review. Mr. Healy stated, "Mere guesses or inarticulable 'hunches' are not enough to constitute reasonable suspicion."**

**a. Standing alone, does the report from the father in this case meet the "reasonable suspicion" standard in your view?**

**b. The State Department and DHS have indicated in their briefings that the information from the father would not, by itself, have been enough to place Abdulmutallab**

**on the TSC watch list because of a particular policy which prevents listing an individual based solely on information from a single source - regardless of how credible or reliable the source may be. Is that an accurate description of the policy, and if so, why should a single reliable source not be enough to place a foreign national on the watchlist?**

**Response to subparts a and b**:

The report indicated that the father was concerned that his son *may be* associating with extremists. Because the "reasonable suspicion" implementation guidance in effect at the time did not permit watchlisting based solely on uncorroborated statements from "walk-ins," some additional corroboration would have been needed to place Abdulmutallab on the watchlist. The TSC's interagency Policy Board Working Group (PBWG) is reviewing the guidance pertaining to source verification and report corroboration to determine whether that guidance should be revised.

**c. Given that al-Qaeda has extensively recruited non-U.S. citizens to carry out its attacks, has the TSC considered revising its nomination standards to allow a less restrictive standard of review for the listing of non-U.S. persons suspected of terrorism on the no fly list?**

**Response**:

The President has directed the TSC to recommend whether changes to the watchlisting criteria and implementation guidance are required, and this process is underway. To develop recommendations responsive to the President's directive, the TSC convened its interagency PBWG, on which the NSC, DOS, DOJ, NCTC, DHS, CIA, NSA, and DoD are represented.

**Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the January 20, 2010, Hearing Before the Senate Committee on the Judiciary Regarding "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"**

**Questions Posed by Senator Hatch**

**13. There are three expiring provisions of the PATRIOT Act. In previous testimony before this committee, you have heralded these provisions as critical investigative tools that the FBI needs to detect and thwart terror plots. For example, the three separate terror plots in Illinois, Texas and New York detected by the FBI last September. In December, Congress only temporarily reauthorized these provisions without any modifications. I have some concerns that any modifications to these investigative tools would "water them down" and unnecessarily increase the investigative burden on the FBI before these tools may be used.**

**a. Can you tell me if you would support a full reauthorization of these provisions without any modifications?**

Response:

The FBI continues to support the reauthorization of the USA PATRIOT Act's expiring provisions, which concern roving wiretaps, Section 215 business record orders, and the "lone wolf" provision. The Attorney General and Director of National Intelligence have previously advised the Congress that S. 1692, the USA PATRIOT Act Sunset Extension Act, as reported by the Senate Judiciary Committee, strikes the right balance by both reauthorizing these essential national security tools and enhancing statutory protections for civil liberties and privacy in the exercise of these and related authorities. Since the bill was reported, a number of specific changes have been negotiated with the sponsors of the bill for inclusion in the final version of this legislation. Among these are several provisions derived from the bills reported by the House Judiciary Committee and introduced by House Permanent Select Committee on Intelligence Chairman Silvestre Reyes in November.

The FBI has been authorized to use the roving wiretap authority many times and we have found that it increases efficiency in critical investigations. This authority affords us an important intelligence gathering tool in a small, but significant, subset of electronic surveillance orders issued under FISA. Roving wiretap authority is particularly critical for effective surveillance of investigative subjects who have received training in countersurveillance methods.

Section 215 orders for business records play an important role in national security investigations as well. This authority allows us to obtain records in national security investigations that cannot be obtained through the use of National Security Letters. In practice, this tool is typically no more intrusive than a grand jury subpoena in a criminal case. Unlike most criminal cases, though, the operational secrecy requirements of most intelligence investigations require the secrecy afforded by this FISA authority. There will continue to be instances in which FBI agents must obtain information that does not fall within the scope of National Security Letter authorities and is needed in an operating environment that precludes the use of less secure criminal investigative authorities.

Finally, although the "lone wolf" provision has never been used, it is an important investigative option that must remain available. This provision gives the FBI the flexibility to obtain FISA warrants and orders in the rare circumstances in which a non-U.S. person engages in terrorist activities, but his or her nexus to a known terrorist group is unknown.

**b. Can you confirm if any of these expiring provisions were used by the FBI in the investigation of these plots?**

**Response**:

As discussed previously, the FBI continues to support the renewal of the three expiring provisions.

Additional information responsive to this inquiry is classified and is, therefore, provided separately.

SUBMISSIONS FOR THE RECORD

**MARKLE** FOUNDATION

**United States Senate Committee on the Judiciary**
**Written Testimony Zoë Baird[1] and Slade Gorton[2]**
**Markle Foundation Task Force on National Security in the Information Age**
January 20, 2010

We would like to thank Chairman Leahy and Ranking Member Sessions for holding this hearing and dedicating their time and energy to the critical issue of improving information sharing. Since 2002, the Markle Foundation Task Force on National Security in the Information Age has pursued a "virtual reorganization of government" that uses the best technology to connect the dots and the best management know-how to get people working across agency lines to understand the meaning of fragments of information. We are submitting this testimony as follow-up to our April 21, 2009 testimony before the Terrorism and Homeland Security Subcommittee at their hearing entitled "Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing."

In the wake of the attempted Christmas Day attack on Flight 253, it is essential to distinguish between amassing dots and connecting them. Information sharing is a means, not an end. The end goal is production of actionable intelligence derived from a form of collaboration that leads to insight and action. The information the Director of National Intelligence reports to the President in his daily briefing is only as good as the information sharing that underlies it.

[1] President of the Markle Foundation, a private philanthropy that focuses on using information and communications technologies to address critical public needs, particularly in the areas of health care and national security.

[2] Senator Gorton served in the United States Senate for 18 years representing Washington state and currently practices law at K&L Gates LLP. He has served on the Markle Task Force since its inception and was a member of the 9/11 Commission.



10 Rockefeller Plaza, New York, NY 10020 Phone 212.489.6655 Fax 212.765.9690 www.markle.org

The President and Congress need to hold a small number of top officials accountable for improving the knowledge he receives from information across the entire government.

As President Obama recognized in his speech on January 7th, the key to achieving this is leadership on a continuing basis. In that respect, this Committee has an important role to play. The Markle Task Force has **five concrete recommendations** to address the cultural, institutional, and technological obstacles that prevented the government from taking full advantage of information that could have helped prevent Umar Farouk Abdulmutallab from boarding a Detroit bound flight with explosives. These recommendations build on the Markle Task Force's past work, which was embraced by the 9/11 Commission and the Weapons of Mass Destruction Commission and was enacted in the intelligence reform laws passed since the September 11th attacks. Our Task Force, composed of national security policy makers from every administration since the Carter Administration, civil liberties advocates and information technology experts, has released four reports and has worked closely with Congress, the Obama administration, and the previous administration. The five recommendations outlined below are detailed in the Task Force's March 2009 report, which we would like to submit for the record.

**First, strong sustained leadership from Congress and the President is required. Urgency has been lacking.** The Task Force takes heart from the President's leadership on this issue and the fact that you are holding this hearing to reaffirm information sharing as a top priority. Congressional oversight will be critical to ensure that government-wide efforts are being coordinated effectively.

We further believe that it is imperative that there be an official within the Executive Office of the President ("EOP") with adequate horsepower to drive interagency coordination at a senior level. Senior leadership from within the EOP will provide government-wide authority to

coordinate information sharing policies and the White House backing to overcome the bureaucratic resistance that persists today. This official would benefit from budget certification authority.

**Second, while it is important to immediately address the gaps exposed by the most recent attack, the larger goal should be transformation of how government does business.** The Markle Task Force envisions information sharing as a means to change the way government does business by creating a distributed network across all agencies, not just the Intelligence Community, that allows teams working on a problem to form quickly and discover relevant information. The failure President Obama identified to "connect and understand" the intelligence that we already had can only be corrected through an information sharing framework that enables collaboration.

Too often information sharing has become simply passing dots to another agency where they are amassed and not properly analyzed. The problem is not the failure to share, but the failure to take responsibility for learning what others know when critical information is discovered. We need to eliminate the belief that the job is done once the information has been shared with the National Counterterrorism Center ("NCTC") or another agency.

More follow-up is required to avoid this type of "systemic failure" in the future. The information sharing framework should facilitate such follow-up. For example, when new information comes into NCTC on a person who is already in the centralized TIDE database on terrorist identities, NCTC should alert the agency that originally submitted the data that caused the person to be in TIDE that a second agency has now submitted related information.

Consistent with the President's January 7, 2010 Directive, there should be some responsibility on those two agencies to work together to "run down the lead," but first they have

to know that they are interested in the same person or topic. Such real-time, virtual collaboration promotes agile decision making by eliminating the seams between departments and agencies that are often exploited by our enemies. Technology exists to facilitate this critical collaboration.

**Third, we recommend that all information within this distributed environment be made "discoverable" to facilitate quickly piecing information together.** The information sharing framework envisioned by the Markle Task Force would allow "data to find data" so that opportunities for action are not missed. At the moment something is learned an opportunity exists to make sense of what this new piece of data means and respond appropriately, but the sheer volume of data makes it impossible for humans to piece every new bit of information together by hand. This process can be automated using existing technology so that a notification is sent to users when new information reveals a connection that may warrant action. The Task Force's concept of discoverability allows an arriving piece of data to be placed automatically so that insight will emerge from the system for the analyst's use. Using such a decentralized system of discoverability simultaneously improves security and minimizes privacy risks by avoiding bulk transfers of data. To achieve this, data should be tagged with standardized information that can be indexed and searched.

When the December 25th bomber was added to the TIDE database, it was instantly knowable that this individual had been approved for a U.S. multiple-entry visa, but no mechanism was in place to trigger reconsideration of the previously granted visa as a result of changes in TIDE. Such a mechanism could be implemented if TIDE were enhanced to allow for "persistent queries." A persistent query requires TIDE (or other databases) to remember the questions it has been asked in the past (*e.g.* the State Department checking the database as part of reviewing a visa application), so that if something changes in TIDE, a trigger notifies the person

who asked about that individual weeks or months ago. Such triggers can help manage the mountains of dots collected by the U.S. government by highlighting new information for select individuals who have previously expressed interest in a topic, like Amazon.com recommending a new book based on the user's order history. This system of discoverability allows new information to be put in context with what we already know. Without context at the point of decision making, critical information may seem of interest, but not worthy of action.

**Fourth, discoverability should be combined with a standard of Authorized Use.** Authorized Use provides a standard to determine whether a user is authorized to see what has been discovered. Like a library card catalogue that offers information on books, but not the books themselves, discoverability offers users the ability to "discover" data without gaining access until it is authorized. This Authorized Use standard would overcome obstacles in the present system of classification and permit an agency or its employees to obtain information based on their role, mission, and a predicated purpose.

Congress requested a study of the feasibility of this standard in the Implementing Recommendations of the 9/11 Commission Act of 2007.[3] The Program Manager for the Information Sharing Environment discussed what he viewed as potential obstacles to implementation of an authorized use standard in his 2008 Feasibility Report. We believe this assessment should be revisited.

**Fifth, government-wide privacy and civil liberties policies for information sharing must be developed to match increased technological capabilities to collect, store, and analyze data.** Consistent policies are needed, but, today, each agency or department has been

[3] 6 U.S.C. § 485(j)(C) (calling for a "standard that would allow mission-based or threat-based permission to access or share information . . . for a particular purpose . . . (commonly known as an 'authorized use' standard)").

tasked to write their own policies on privacy. We must avoid the next failure that is based on an agency saying they weren't authorized to use information on U.S. persons, for example. The new government-wide policies should be clear, detailed, transparent, and consistent while allowing agencies the flexibility that their different missions and authorities require. They must provide direction on hard issues, rather than simply stating that agencies must comply with the Privacy Act without explaining how to do so. Such policies are necessary both for the American people to have confidence that their government is protecting their civil liberties and to empower the participants in the information sharing framework so they have confidence that their work is lawful and appropriate.

The President and Congress should also act within the next 60 days to nominate and confirm members to the Privacy and Civil Liberties Oversight Board. Congress re-chartered the Board to strengthen its independence and authority, but the new Board has never come into existence. The statutory charter for the new Board gives it a role both in providing advice on policy development and implementation and in reviewing specific programs.

Finally, the information sharing framework should take advantage of technological tools to build new and more powerful privacy protections into the system and minimize the risk of unintended disclosure of personally identifiable information. There are now a number of commercially available technologies, including anonymization, strong encryption, and digital rights management, that can enhance both privacy and security simultaneously.

***

Our enemies will continue to adapt. The next attack may not come from the air. Improved information sharing is a long-term strategic tool that will allow the U.S. to stay one

step ahead of its enemies whether they are attempting to attack our critical infrastructure in cyberspace, deploy biological weapons, or smuggle explosives through airport security.

This Committee has a critical oversight role to play in order to ensure that measurable progress is made on information sharing. We commend this Committee for its leadership on these issues, but much more needs to be done.

The Task Force is committed to continuing to work with Congress and the Obama administration to find practical solutions to this critical national security challenge.

# PREFACE

The Constitution Project is an independent think tank that promotes and defends constitutional safeguards. We create coalitions of respected leaders of all political stripes who issue consensus recommendations for policy reforms. In the days following the September 11, 2001, terrorist attacks on the United States, the Constitution Project created its Liberty and Security Committee. Working with this ideologically diverse group of prominent Americans, the Constitution Project addresses a wide range of issues, including the tension between measures designed to enhance security and constitutional values relating to personal liberty and privacy. Committee members are dedicated to developing and advancing proposals to protect civil liberties even as our country works to make Americans safe.

One tool upon which government officials have increasingly relied in combating terrorism since September 11th is watch lists—namely lists of individuals suspected of having ties to terrorism or other crime. However, as widely reported in the media, watch lists continue to be plagued with errors. Many people who have sought to clear their names have encountered numerous obstacles and substantial delays. This report provides recommendations for restricting the use of such watch lists, and for adopting important reforms to govern the situations in which they are used.

This publication contains two parts. The first is a statement urging policy reforms, which has been endorsed by the members of the Constitution Project's Liberty and Security Committee listed at the end of the statement. The second part is a background report, which sets forth a more detailed legal and policy analysis supporting the Committee's recommendations for the use of watch lists. A draft of this background report was made available to Committee members as they developed their consensus statement. However, Committee members have not been asked to endorse the specific language of the background report.

The Constitution Project sincerely thanks Peter Shane, the Joseph S. Platt-Porter, Wright, Morris & Arthur Professor of Law and Director, Center for Interdisciplinary Law and Policy Studies, Ohio State University Moritz College of Law, for his extensive research and drafting work in preparing both the Committee's statement and the background report. The Constitution Project also thanks James X. Dempsey, Laura Bailyn, and Matthew Fagin of the Center for Democracy and Technology for sharing some of their research; and Maritsa Zervos '06 and, especially, Christine Easter '07 of the Moritz College of Law, for their research assistance.

The Constitution Project is also grateful to the Public Welfare Foundation and the Community Foundation for their support of the Liberty and Security Committee's work on watch lists. We also thank the Open Society Institute, the Wallace Global Fund, and an anonymous donor for their support of the Constitution Project in all its work.

–Sharon Bradford Franklin, Senior Counsel
–Joseph N. Onek, Senior Counsel

**Senate Judiciary Committee**
**Hearing on "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"**
**Wednesday, January 20, 2010**

**Statement of U.S. Senator Russell D. Feingold**

Mr. Chairman, I join all members of this committee in my horror at what almost happened on Christmas Day on the Northwest flight from Amsterdam to Detroit. The passengers and crew on that flight deserve enormous credit for helping prevent a disaster. While the attempt did not end in the tragedy that it could have, we must treat this as a wake-up call. We must understand how and why Abdulmutallab was able to board that flight, and what steps we can take to prevent the next such attempt.

But we must also approach our task calmly and thoughtfully, and not treat this as an opportunity to score political points. Congress needs to work with the executive branch to find the right answers to these questions – and not just lay blame or take actions that are politically expedient but ultimately ineffective. And as President Obama said last week, we "will not succumb to a siege mentality that sacrifices the open society, liberties and values we cherish as Americans. Because great and proud nations don't hunker down and hide behind walls of suspicion and mistrust. … We will define the character of our country. Not some band of small men intent on killing innocent men, women and children." We must heed his call.

By all accounts, the President was right to characterize this as a systemic failure. And I agree with him that some very tough questions must be asked to repair and improve the counterterrorism systems that are now in place. This is not the time for excuses, nor is it the time for pointing fingers. It's time to fix the problem.

At the outset, the attempted bombing underscores the importance of denying al Qaeda safe havens in countries like Yemen, an issue I have been working on for years. The threat from al Qaeda in Yemen, as well as the broader region, is increasing and our attention to this part of the world is long overdue. Just to take one example, in 2003 as our Armed Forces were advancing toward Baghdad, 23 al Qaeda members escaped from a prison in Yemen. This serious security lapse got very little attention.

Local conditions in places like Yemen – as well as Somalia, North Africa and elsewhere – enable al Qaeda affiliates and sympathizers to recruit followers and plan attacks. As a result, while we should aggressively pursue al Qaeda leaders, we will not ultimately be successful if we treat counterterrorism merely as a manhunt with a finite number of al Qaeda members in the world. Nor can we jump from one perceived "central front" to the next. We must develop a comprehensive, global counterterrorism strategy that takes into account security sector reform, human rights, economic

development, transparency, good governance, accountability, and the rule of law. Without this broader framework we are likely to alienate local populations and embolden our enemy.

So I am pleased the President will increase his focus on Yemen. Any serious effort against al Qaeda in Yemen will require strengthening the weak capacity of the government as well as its legitimacy in the eyes of its citizens.

This incident also underscores management failures in the Intelligence Community. As the President and other administration officials have explained, we failed to anticipate fully the threat to the homeland from Al Qaeda in the Arabian Peninsula, despite knowing that they sought to strike us and that they were recruiting operatives to do so. And our failure to prioritize this threat contributed to the failure to uncover this plot. Clearly, there should be institutional responsibility for and more resources devoted to high priority threats, as the President has directed. But we also need to determine how those priorities are identified, in advance of a particular plot being uncovered. And we need better strategic intelligence on safe havens if we are to develop informed counterterrorism policies across the board, not just efforts to thwart particular plots.

That is why I have proposed the creation of a bipartisan commission to fully integrate, and thus make effective use of, all the ways in which we anticipate threats and crises around the world. That means not only the Intelligence Community, but the State Department and others in our government who gather information openly. That legislation has twice passed the Intelligence Committee, and has passed the full Senate as part of the intelligence authorization bill. It is a critical priority. Our analytical attention and institutional resources cannot forever be reacting to the latest plot. We need global capabilities and stronger strategic intelligence, to anticipate where al Qaeda is, or could be operating, before the next Abdulmutallab gets on a plane.

In some ways those issues are beyond the scope of this committee's hearing. But I don't think we can talk about our response to this attempted bombing without putting our counterterrorism efforts in a larger, global context. Now I will move on to the issues that will be the more central focus of this hearing.

The Christmas Day plot obviously raises serious questions about our watch listing and screening processes that we need to examine. President Obama has confirmed that the U.S. government had the information it needed to watch list Abdulmutallab, but it didn't happen. We need to consider whether watch list procedures need to be changed, and if so whether the problem is one of implementation – that is, of allocating sufficient resources and appropriately prioritizing the watch list process – or, rather, a problem with the watch list policies themselves. And we need to take into account the fact that the watch list includes both foreigners and Americans and that, if the standards for getting on

a watch list are loosened, that would likely lead to more innocent Americans being mistakenly stopped at the airport. We all know the stories – in fact, the New York Times just ran a piece on an 8-year-old boy who has run into problems at the airport since he was an infant – and that kind of problem will only get worse if we dramatically expand watch lists by minimizing identification criteria or lowering the threshold. And it's not at all clear that it would have done anything to prevent Abdulmutallab from getting on that airplane. The government had enough information to watch list Abdulmutallab – it just didn't put all the pieces together.

We also need to look at the breakdown in the visa revocation process. There needs to be clear authority and streamlined processes for reviewing and revoking visas when we have intelligence that someone may be seeking to harm the United States. We should also consider ways to strengthen the visa application process. Intelligence sharing to support these efforts is necessary.

But I am troubled by the new policy of requiring heightened screening of everyone traveling from or through certain countries, or who is a citizen of one of those countries. I'm not sure it is the most effective allocation of resources, particularly if it means that we will have fewer resources for looking into people who have actually done something suspicious. It also risks alienating governments and populations that can be allies in defeating al Qaeda and its affiliates. We must recognize the serious foreign policy implications of singling out countries and individuals whose citizens do not have a history of seeking to attack us and question the effectiveness of screening millions of people because of the behavior of one individual. The end result could be exactly what we are seeking to avert, so if more narrowly tailored solutions will prevent future attacks and help us avoid unsustainable burdens on airport security personnel, they should be pursued. In this case, enhanced screening of individuals already identified by government personnel as potential threats likely would have worked, had anyone looked at all the information about Abdulmutallab that the U.S government had already obtained.

I have also heard concerns from some constituents about the use of imaging technologies at the airport. It appears that these machines can be an important part of our airport security screening system, and might have helped stop Abdulmutallab if he had been screened by one. But I can understand the privacy concerns that have been raised. Should this technology be incorporated into standard airport security measures, we must ensure that TSA's privacy rules remain in place and that they are enforced. TSA already allows passengers to request a pat-down search instead of going through the full body imaging machine. Additionally, TSA policy is that it does not save or store the images the machines produce. One question for Congress may be whether we need to enshrine these rules in law. We also must ensure that these machines are properly tested before they are deployed and that we focus precious resources on the most effective technology. In this instance, explosive detection monitors may have been more effective than body imaging technologies.

Finally, there is the question of how to deal with this particular individual. I support the administration's decision to charge Umar Farouk Abdulmutallab in federal court. Richard Reid, the so-called shoe bomber, was prosecuted by the Bush Administration in federal court and is imprisoned in our federal prison system today. I see no reason to treat this case any differently.

In fact, we have a strong record in our federal courts. More than 200 terrorism defendants have been prosecuted in the federal court system since 9/11, and federal prisons securely hold more than 300 inmates whose cases were terrorism-related. Compare that with the record of the military commissions set up by the Bush administration, where only three people have been convicted. In addition, of the three people who have been held as enemy combatants in the United States, two were ultimately transferred into the criminal justice system and one was released. Some argue that we can't get useful intelligence in the context of the criminal justice system, but that is simply inaccurate. In fact there are several examples of people who have been charged with terrorism-related crimes in federal court and have cooperated with the U.S. government, including several of the Lackawanna Six, and most recently David Coleman Headley who was indicted for involvement in the Mumbai attacks.

Mr. Chairman, this hearing is an opportunity for us to make our country stronger, by coming together to evaluate how we can enhance our defenses while maintaining the principles that America was founded on. I hope we will all approach it with calm deliberation, and not turn this into a political blame game.

**Center for National Policy**
*Fostering bipartisan dialogue and finding solutions to America's national security challenges for over 25 years*

# "Our Most Neglected Anti-Terrorism Tool: Informing & Empowering the General Public"

Written Testimony to support

a hearing of the

Judiciary Committee
United States Senate

on

"Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"

by

**Stephen E. Flynn, Ph.D.**
President
Center for National Policy
sflynn@cnponline.org

Dirksen Senate Office Building – Room 226
Washington, D.C.

10:00 a.m.
January 20, 2010

**"Our Most Neglected Counterterrorism Tool:**
**Informing & Empowering the General Public"**

by
Dr. Stephen E. Flynn
President, Center for National Policy

I provide this written testimony at the request of Senator Patrick Leahy, Chairman of the Senate Judiciary Committee, to support a hearing examining the effectiveness of U.S. counterterrorism tools in light of the December 25, 2009 bombing attempt aboard Northwest Flight No. 253. The witnesses from the FBI, Department of State, and Department of Homeland Security will be testifying on the reforms and recommendations that President Obama is advancing in response to this incident. I will restrict my comments to discussing an area of emphasis which has received too little attention by the national security and intelligence communities: the essential support role the general public can and must play in managing and mitigating the ongoing risk of terrorism.

Over the past few weeks, there has been much talk in the media about what the experts got wrong and how analytical processes within the intelligence community and technology for mining data can be improved. We have also heard senior officials openly acknowledge that despite their best efforts, there are inherent limits to what the intelligence community can do to identify and intercept all terrorist threats. But given those limits, what has not received adequate attention is the extent to which the federal government should be obligated to provide more detailed information to everyday people about the nature of the evolving terrorist threat and our ongoing vulnerabilities, and the actions individuals can take should they find themselves in harm's way.

A cultural shift away from the highly secretive national security apparatus constructed to deal with the Soviet threat during the Cold War is long overdue. The attacks of September 11, 2001 confirmed what members of the Hart-Rudman Commission and military leaders like the former Commandant of the U.S. Marine Corps, General Charles C. Krulak, had been forecasting in the 1990s: given the overwhelming dominance of the U.S. military force-on- force capabilities, the preferred battle space for America's adversaries in the 21st Century will be the civil and economic space. While this development inevitably required changes to the U.S. national security strategy and capabilities, professional warriors, intelligence officials, and federal law enforcement agents have been reluctant to acknowledge that there is simply no way that they can carry the day on this battlefront without help from everyday citizens. But the simple fact is that there never will be enough professionals in the kinds of places terrorists are most likely to be exploiting or targeting. Further, intelligence and technologies are fallible. While many might wish it were otherwise, when it comes to detecting and intercepting terrorist activities, the first preventers and first responders will almost always be civilians who happen to be around when trouble is unfolding.

We need look no further than the tragic events of September 11, 2001 to discover where the frontlines in the war on terrorism often lie. One of the most overlooked lessons of that day is that the only counterterrorism action successfully taken against al Qaeda's

attack was done not by the Department of Defense, FBI, CIA, or other U.S. government agencies, but by the passengers aboard United Airlines Flight 93. By charging the cockpit and preventing al Qaeda from striking the U.S. Capitol or the White House, everyday people ended up protecting the very officials who have the constitutional obligation "to provide for the common defense." In retrospect, it is outrageous that men and women flying aboard United 93 had to learn via their cell phones in calls to their friends and loved-ones the threat information that many inside the U.S. government knew but failed to share with each other—that al Qaeda was contemplating using airliners as cruise missiles. There is no way that we will ever know what the passengers aboard the first three planes that struck the twin towers and the Pentagon would have done if they had been provided that threat information. What we do know is that the unofficial protocol for airline passengers up until 9/11 was to stay quietly in their seats and wait until the plane had landed for the professionals to negotiate with the hijackers. In other words, the people aboard American Airlines Flight 11, United Airlines Flight 175, and American Airlines Flight 77 were all deprived of the opportunity to take the kinds of measures the people aboard United 93 took to protect both themselves and al Qaeda's intended targets—because the U.S. government never shared this threat information with the flying public.

Similarly, the attempted Christmas Day attack once again highlighted how important it is for bystanders to not be viewed by U.S. officials with reflexive skepticism or only as potential victims. It was government agencies that once again fell short in detecting and intercepting the attack, not ordinary people. A concerned Nigerian father came forward with crucial information but it was not assigned sufficient weight by the intelligence community because it came from an unofficial source. And the courageous actions of the Dutch film director Jasper Schuringa and other passengers and crew members aboard Northwest Flight 253 thwarted the attack.

Many commentators, elected officials, and policy makers have pointed to the fact that everyday people had to act aboard Northwest Flight 253 in order to protect themselves as a sign "that the system failed." I disagree. Certainly in an ideal world, individuals would not be exposed to this kind of danger. Similarly, it would be desirable for people to live in crime-free neighborhoods. But nobody believes today that crime can be defeated without directly involving the community. We routinely publish crime statistics and provide details about how criminal acts are perpetrated. Around the nation there are citizens participating in "Neighborhood Watches," FBI Citizen Academies, and Red Cross preparedness training programs. So why is that when it comes to aviation security and the broader homeland security enterprise, the public is essentially told that they should leave it all to the professionals?

With this latest Detroit incident, terrorist attacks have now been thwarted by passengers aboard five different commercial airplanes. As with the case of Richard Reid, the December 2001 shoebomber, Umar Farouk Abdulmutallab has demonstrated that it is difficult for even the most determined suicide bomber to construct a bomb aboard a crowded aircraft during what he or she expects will be the final moments of their life. The human survival instinct is working against success. So having passengers and flight

crews aware of what they should be on the lookout for may be more helpful than massive investments and the delays associated with purchasing body scanning equipment. At the end of the day, even if the technology could be put in place to detect explosives that passengers might carry aboard airplanes (and there is still the sticky problem of the machines commonly in use during passenger screening being unable to detect explosives in carry-on baggage), terrorists can and almost certainly will move on to mass-transit systems, shopping malls, arenas, or critical infrastructure where these detection tools are not likely to be practical or effective. Americans need to be routinely updated with realistic and accurate details about what terrorist organizations are up to, and what they can do to mitigate the risk.

The common rebuttal to calls of more candor on the part of the U.S. government is that it will generate a climate of fear among the public. But for terror to work, it requires two things: first, an awareness of threat of vulnerability (e.g., a child is "fearless" when he does not know that he will be hurt by coming into contact with a hot stove) and second, a sense of powerlessness to deal with a known threat of vulnerability. By working to overcome the sense of unbounded threat and powerlessness that too many Americans feel, we can starve terrorism of the very dread it needs to feed on to be effective.

At the end of the day, a shift away from the current approach that relies almost exclusively on quiet behind-the-scenes actions by our intelligence, national security, homeland security, and law enforcement communities is both more realistic and constructive. America's adversaries will find acts of terrorism on U.S soil to be attractive as long as they can count on Americans being spooked even by failed terrorist attempts. Alternatively, investments that better inform and prepare the American people to withstand, rapidly recover, and adapt to the acts of terrorism means that there will be no real bang for the terrorist buck, providing a measure of deterrence for our enemies. The more resilient we are as a society, the less gain terrorists will achieve by attacking Americans.

So what changes can be made in light of the shortcomings revealed by the Christmas Day bombing attempt? First, the U.S. government should work with the commercial aviation industry on developing a security briefing for passengers that builds on the safety briefings airlines already provide. If we can tell passengers that they should be prepared for the extremely remote possibility of a plane landing on the water, we should be able to provide a few pointers about what to do if someone appears to be trying to detonate an explosive.

Second, more can and should be done at airports to train individuals who work as vendors and in providing services to be on the lookout for behaviors and activities associated with acts of terrorism. A version of this kind of program has been underway for many years at Boston Logan Airport called "Logan Watch." A condition of receiving of credentials at all airports should be employees undergoing annual counterterrorism training.

Third, the post-9/11 emphasis on investing in technology needs to be tilted back to investing more in people. Technology can be helpful, but too often it ends up being part

of the problem. Placing too much reliance on sophisticated tools such as X-ray machines often leaves the people staffing our front lines consumed with monitoring and troubleshooting these systems. Consequently, they become more caught up in process than outcomes. And as soon as procedures become routine, a determined bad guy can game them. We would do well to heed two lessons the U.S. military has learned from combating insurgents in Iraq and Afghanistan: First, don't do things in rote and predictable ways, and second, don't alienate the people you are trying to protect. Too much of what is promoted as homeland security disregards these lessons. New technologies can be enablers, but they are no substitute for well-trained professionals who are empowered and rewarded for exercising good judgment.

In a December 28, 2009 article, Amanda Ripley, a contributor to TIME magazine wrote about what happened to the passengers of Flight 253 after they deplaned in Detroit.

> They were herded into the baggage area for more than five hours until FBI agents interviewed them. They were not allowed to call their loved ones. They were given no food. When one of the pilots tried to use the bathroom before a bomb-sniffing dog had finished checking all the carry-on bags, an officer ordered him to sit down, according to passenger Alain Ghonda, who thought it odd. "He was the pilot. If he wanted to do anything, he could've crashed the plane." It was a metaphor for the rest of the country: Thank you for saving the day. Now go sit down.

It is long past the time for the federal government to stop pretending that if it has enough gadgets, agents, and recalibrated organization charts, it can protect us without our help. The greatest asset that this nation has is not its second-to-none national security apparatus—though this is a tremendous asset to have for living in a dangerous world. Harkening back to the earliest days of our republic, our most important strength has always been "we the people." This is a reality eloquently put by a reader who wrote in response to an op-ed that I penned for the Washington Post on January 3, 2010:

> My ancestors who fought the Brits at Kings Mountain and Cowpens didn't fight for a government capable of protecting them - that's what the British Crown offered. They fought for a government that was respectful of them and their rights such that they could and would protect their government.

*Stephen Flynn is the president of the Center for National Policy and author of* ***The Edge of Disaster: Rebuilding a Resilient Nation*** *(NY: Random House, 2007)*


**Statement of David Heyman**
**Assistant Secretary - Policy**

**U.S. Department of Homeland Security**

**before**

**United States Senate**
**Committee on the Judiciary**

**on**

**Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication**

**Wednesday, January 20, 2010**

**226 Dirksen Senate Office Building**
**Washington DC**

**Aviation Security Testimony**

Chairman Leahy, Senator Sessions and members of the Committee: Thank you for this opportunity to testify on the attempted terrorist attack on Northwest Flight 253.

The attempted attack on December 25 was a powerful illustration that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. This Administration is determined to thwart those plans and disrupt, dismantle and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just DHS, but many other federal agencies and the international community as well.

As our part in this effort, DHS is a consumer of the U.S. Government's consolidated terrorist watchlist, which we use to help keep potential terrorists off flights within, over or bound for the United States and to identify travelers that require additional screening. We work with foreign governments, Interpol, and air carriers to strengthen global air travel security by advising them on security measures and on which passengers may prove a threat. We also work with air carriers and airport authorities to perform physical screening at TSA checkpoints and to provide security measures in flight.

Immediately following the December 25 attack, DHS took swift action at airports across the country and around the world. These steps included enhancing screening for individuals flying to the United States; increasing the presence of law enforcement and explosives detection canine teams at air ports, and of air marshals in flight; and directing the FAA to notify the 128 flights already inbound from Europe about the situation. Nonetheless, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with the explosive

PETN on his person. As President Obama has made clear, this Administration is determined to find and fix the vulnerabilities in our systems that allowed this breach to occur.

Agencies across the federal government have worked quickly to address what went wrong in the Abdulmutallab case. The effort to solve these problems is well underway, with cooperation among DHS, the Department of State, the Department of Justice, the Intelligence Community, and our international allies, among others. As a consumer of terrorist watchlist information, the Department of Homeland Security welcomes the opportunity to contribute to the dialogue on improving the federal government's ability to connect and assimilate intelligence. We are also focused on improving aviation screening and expanding our international partnerships to guard against a similar type of attack occurring again. To those ends, today I want to describe the role that DHS currently performs in aviation security, how DHS responded in the immediate aftermath of the attempted Christmas Day attack, and how we are moving forward to further bolster aviation security.

**DHS' Role in Multiple Layers of Defense**

Since 9/11, the U.S. government has employed multiple layers of defense across several departments to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities, while other countries and the private sector – especially the air carriers themselves – also have important roles to play.

DHS oversees several programs to prevent individuals with terrorist ties from boarding flights that are headed to, within, or traveling over the United States or, in appropriate cases, to identify them for additional screening. Specifically, DHS uses information held in the Terrorist Screening Database (TSDB), a resource managed by the Terrorist Screening Center (TSC), as

well as other information provided through the Intelligence Community to screen individuals; operates the travel authorization program for people who are traveling to the United States under the Visa Waiver Program (VWP)[1]; and works with foreign governments, international and regional organizations, and airlines to design and implement improved security standards worldwide. This includes routine checks against Interpol databases on wanted persons and lost or stolen passports on all international travelers arriving in the United States. The Department also performs checkpoint screenings at airports in the United States.

To provide a sense of the scale of our operations, every day, U.S. Customs and Border Protection (CBP) processes 1.2 million travelers seeking to enter the United States by land, air or sea; the Transportation Security Administration (TSA) screens 1.8 million travelers at domestic airports; and DHS receives advanced passenger information from carriers operating in 245 international airports that are the last point of departure for flights to the United States, accounting for about 1,600 to 1,800 flights per day. Ensuring that DHS employees and all relevant federal officials are armed with intelligence and information is critical to the success of these efforts.

*Safeguards for Visas and Travel*

One of the first layers of defense in securing air travel consists of safeguards to prevent dangerous people from obtaining visas, travel authorizations and boarding passes. To apply for entry to the United States prior to boarding flights bound for the U.S. or arriving at a U.S. port of

[1] The 35 countries in the Visa Waiver Program are: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, and the United Kingdom (for the U.K., only citizens with an unrestricted right of permanent abode in the U.K. are eligible for VWP travel authorizations).

entry, most foreign nationals need visas – issued by a U.S. embassy or consulate – or, if traveling under a Visa Waiver Program country, travel authorizations issued through the Electronic System for Travel Authorization (ESTA).[2]

Issuing visas is the responsibility of the Department of State. At embassies and consulates where it is operational, the Visa Security Program positions personnel of U.S. Immigration and Customs Enforcement (ICE) to assist State Department personnel in identifying visa applicants who may present a security threat. For individuals traveling under the VWP, DHS operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. These systems examine an individual's information to assess whether he or she could pose a risk to the United States or its citizens, including possible links to terrorism. Without presenting a valid authorization to travel to the United States at the airport of departure, a foreign national is not able to board a U.S.-bound flight.

The Department also works with other federal agencies and our foreign partners to try to prevent possible terrorists from obtaining boarding passes. These include the application of the No-Fly List and the implementation of Secure Flight program, which I explain below.

*Pre-departure screening*

As another layer of defense, DHS conducts pre-departure passenger screening in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. DHS uses TSDB data, managed by the Terrorist Screening Center that is administered by the FBI, to determine who may board, who requires

[2] Exceptions would be citizens of countries under other visa waiver authority such as the Western Hemisphere Travel Initiative or the separate visa waiver program for Guam and the Commonwealth of the Northern Mariana Islands, or those granted individual waivers of the visa requirement under the immigration laws.

further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

Specifically, to help make these determinations, DHS uses the No-Fly List and the Selectee List, two important subsets within the TSDB. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, over, or within the United States. Individuals on the Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

Through the Secure Flight Program, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List, and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, DHS began to transfer this responsibility to TSA in 2009, and the transition is targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination.

As an additional layer of security, DHS also uses the Passenger Name Record (PNR), the Advanced Passenger Information System (APIS), and the Immigration Advisory Program (IAP) to assess a passenger's level of risk and, when necessary, flag them for further inspection. PNR data, obtained from the airline reservations systems, contains various elements, which may include optional information on itinerary, co-travelers, changes to the reservation, and payment information. PNR data is evaluated against "targeting rules" that are based on law enforcement data, intelligence and past case experience. APIS data, which carriers are required to provide to

DHS at least 30 minutes before a flight, contains important identifying information that may not be included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. DHS screens APIS information on international flights to or from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations. APIS is also connected to Interpol's lost and stolen passport database for routine queries on all inbound international travelers.

Another layer in the screening process is the Immigration Advisory Program (IAP). The CBP officers stationed overseas under the IAP program at nine airports in seven countries receive referrals from CBP screening against the TSDB, of which the No Fly list is a subset. IAP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

*Checkpoint screenings and in-flight security*

The third layer of defense for air travel in which DHS plays a role is the screening of passengers and their baggage. TSA screens passengers and baggage at airports in the United States, but not in other countries. When a traveler at a foreign airport is physically screened, that screening is conducted by the foreign government, air carriers, or the respective airport authority.

Domestically, TSA employs a layered approach to security, which includes measures both seen and unseen by travelers. The 48,000 Transportation Security Officers at hundreds of airports across the country screen passengers and their baggage using advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines,

vapor trace machines that detect liquid explosives, Advanced Imaging Technology, full-body pat-downs, explosives detection systems, Bomb Appraisal Officers, and Behavior Detection Officers – both at the checkpoint and throughout the airport. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security throughout the airport perimeter and in limited access areas of airports. The $1 billion in Recovery Act funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

In an effort to enhance international screening standards, TSA conducts security assessments in accordance with security standards established by the International Civil Aviation Organization (ICAO) at more than 300 foreign airports, which include foreign airports from which flights operate directly to the United States and all airports from which U.S. air carriers operate. If an airport does not meet these standards, TSA works with the host government to rectify the deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. In long-term circumstances of non-compliance with international standards, TSA may recommend suspension of flight service from these airports to the United States. In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level. If an airport is located within one of the 35 VWP countries, DHS conducts additional audits and inspections as part of the statutorily mandated VWP designation and review process.

In terms of in-flight security, Federal Air Marshals (FAM) are deployed on high-risk domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more volunteer pilots serve as armed, deputized Federal Flight Deck Officers. Additionally, armed law enforcement officers from federal, state, local, and tribal law enforcement agencies that have a need to fly armed provide a force multiplier on many flights.

**DHS Response to the Christmas Day Attack**

The facts of the Christmas Day attempted bombing are well established and were relayed in the report on the incident that the President released on January 7, 2010. On December 16, 2009, Umar Farouk Abdulmutallab, a Nigerian national, purchased a round-trip ticket from Lagos, Nigeria to Detroit. Abdulmutallab went through physical security screening conducted by foreign airport personnel at Murtala Muhammed International Airport in Lagos on December 24 prior to boarding a flight to Amsterdam Airport Schiphol. This physical screening included an x-ray of his carry-on luggage and his passing through a walk-through metal detector. Abdulmutallab went through additional physical screening, conducted by Dutch authorities, when transiting through Amsterdam to Northwest Flight 253 to Detroit, and presented a valid U.S. visa. Abdulmutallab was not on the No Fly or Selectee Lists. Accordingly, the carrier was not alerted to prevent him from boarding the flight or additional physical screening, nor did the IAP officer advise Dutch authorities of any concerns. As with all passengers traveling on that flight, and similar to all other international flights arriving in the United States, CBP evaluated Abdulmutallab's information while the flight was en route to conduct a preliminary assessment of his admissibility and to determine whether there were requirements for additional inspection.

During this assessment, CBP noted that there was a record that had been received from the Department of State, which indicated possible extremist ties. It did not indicate that he had been found to be a threat, or that his visa had been revoked. CBP officers in Detroit were prepared to meet Abdulmutallab upon his arrival for further interview and inspection. The attack on board the flight failed in no small part due to the brave actions of the crew and passengers aboard the plane.

*Immediate DHS response*

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. TSA directed the Federal Aviation Administration to apprise 128 U.S.-bound international flights from Europe of the attempted attack and to ask them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosive detection canine teams, state and local law enforcement, expanded presence of Behavior Detection Officers, and enhanced screening. That evening, DHS issued a security directive for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

From the first hours following the attempted attack, Secretary Napolitano worked closely with the President, Assistant to the President for Homeland Security and Counterterrorism John Brennan, senior Department leadership, and agencies across the federal government. She communicated with international partners, members of Congress, state and local leadership and the aviation industry and met with national security experts on counterterrorism and aviation

security. The results of these communications culminated in two reports to the President: one on New Year's Eve and the second on January 2, 2010.

One of our most important conclusions was that it is now clearer than ever that air travel security is an international responsibility. Indeed, passengers from 17 countries were aboard Flight 253. Accordingly, DHS has embarked upon an aggressive international program designed to raise international standards for airports and air safety. On January 3, 2010, at the direction of Secretary Napolitano, I was dispatched with Deputy Secretary Jane Holl Lute to Africa, Asia, Europe, the Middle East, Australia, and South America to meet with international leadership on aviation security. In these meetings, we reviewed security procedures and technology being used to screen passengers on U.S.-bound flights and worked on ways to bolster our collective tactics for defeating terrorists. This afternoon, Secretary Napolitano is traveling to Spain to meet with her European Union counterparts in the first of a series of global meetings intended to bring about broad consensus on new, stronger, and more consistent international aviation security standards and procedures.

In addition to these efforts, the Department has been in close contact with Congress, our international partners, the aviation industry and state and local officials across the country since the afternoon of the attempted attack. On December 25, the Department issued a joint bulletin with the FBI to state and local law enforcement throughout the nation; conducted calls with major airlines and the Air Transport Association; distributed the FBI-DHS joint bulletin to all Homeland Security Advisors, regional fusion center directors and Major City Homeland Security Points of Contact in the country; and notified foreign air carriers with flights to and from the United States of the additional security requirements. DHS has maintained close contact with all of these partners since the attempted attack, and will continue to do so.

On January 3, TSA issued a new Security Directive, effective on January 4, which includes long-term, sustainable security measures developed in consultation with law enforcement officials and our domestic and international partners. Because effective aviation security must begin beyond our borders, this Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism[3] or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners.

**Steps Forward to Improve Aviation Security**

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. On January 7, Secretary Napolitano joined Assistant to the President for Counterterrorism and Homeland Security John Brennan to announce five recommendations DHS made to the President as a result of the security reviews ordered by President Obama. At the President's direction, DHS will pursue these five objectives to enhance the protection of air travel from acts of terrorism.

First, DHS will work with our interagency partners to re-evaluate and modify the criteria and process used to create terrorist watchlist, including adjusting the process by which names are added to the No-Fly and Selectee Lists. The Department's ability to prevent terrorists from boarding flights to the United States depends upon these lists and the criteria used to create them.

[3] The State Department currently lists Cuba, Iran, Sudan, and Syria as state sponsors of terrorism.

As an entity that is primarily a consumer of this intelligence and the operator of programs that rely on these lists, the Department will work closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watchlist system.

Second, DHS will establish a partnership on aviation security with the Department of Energy and its National Laboratories in order to use their expertise to bolster our security. This new partnership will work to develop new and more effective technologies that deter and disrupt known threats, as well as anticipate and protect against new ways that terrorists could seek to board an aircraft with dangerous materials.

Third, DHS will accelerate deployment of Advanced Imaging Technology to provide capabilities to identify materials such as those used in the attempted December 25 attack, and we will encourage foreign aviation security authorities to do the same. TSA currently has 40 machines deployed at nineteen airports throughout the United States, and plans to deploy at least 450 additional units in 2010. DHS will also seek to increase our assets in the area of explosives-trained canines, explosives detection equipment, and other security personnel.

Fourth, DHS will strengthen the presence and capacity of aviation law enforcement. As an interim measure, we will deploy law enforcement officers from across DHS to serve as Federal Air Marshals to increase security aboard U.S.-flag carriers' international flights. At the same time, we will maintain the current tempo of operations to support high-risk domestic flights, as we look to longer-term solutions to enhance the training and workforce of the Federal Air Marshal Service.

Fifth, as mentioned earlier, DHS will work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in

foreign airports and the commitments of our foreign partners to enhance security – not just for Americans, but also for their nationals traveling to this country.

In all of these action areas to bolster aviation security, we are moving forward with a dedication to safeguard the privacy and rights of travelers.

**Conclusion**

The attempted attack on Christmas Day serves as a stark reminder that terrorists motivated by violent extremist beliefs are determined to attack the United States. President Obama has made clear that we will be unrelenting in using every element of our national power in our efforts around the world to disrupt, dismantle, and defeat al-Qaeda and other violent extremists.

While we address the circumstances behind this specific incident, we must also recognize the evolving threats posed by terrorists, and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities in all sectors. President Obama has clearly communicated the urgency of this task, and the American people rightfully expect swift action. DHS and our federal partners are moving quickly to provide just that.

I wish I could close by giving you a 100 percent guarantee that no terrorist, ever, will try to take down a plane or attack us in some other fashion. I cannot give you such a guarantee; that is not the nature of the world we live in, nor of the threats that we face. What I can give you, however, is the 100 percent commitment of Secretary Napolitano, DHS leadership, and the entire DHS enterprise to do everything we can to minimize the risk of terrorist attacks.

Chairman Leahy, Senator Sessions, and members of the Committee: Thank you for this opportunity to testify. I can now answer your questions.

# Testimony of
# Asa Hutchinson

## Before the Senate Judiciary Committee

CEO, Hutchinson Group
DHS Undersecretary, 2003-2005

January 20, 2010

**TESTIMONY OF ASA HUTCHINSON**
**BEFORE THE SENATE JUDICIARY COMMITTEE**

Chairman Leahy and Members of the Committee, thank you for conducting this hearing on the terrorist incident on Flight 253, and the challenge our nation faces as we work to protect our citizens from the threat of terrorism.

There are four issues I will discuss in my testimony. (1) The Department of Homeland Security should have greater responsibility in visa security. (2) It is important to recognize that the United States can deny entry into our airspace for international flights that may pose a risk. (3) The screening technology called "full body scans" should be limited in its use to secondary inspection and not as a mandatory procedure for all passengers. And, (4) the structure of intelligence sharing is not broken, but rather the focus should be on effectiveness, which may require more resources for intelligence analysts who perform our watch list checks.

VISA SECURITY

Umar Farouk Abdulmutallab's failed attempt to bomb Flight 253 on Christmas Day is another reminder that a visa to a terrorist is priceless. It is the golden key that allows easy passage to the United States. If the intelligence on Abdulmutallab had been properly analyzed, his visa would have been quickly revoked and he would have been denied access to the flight.

We must go back to basics and strengthen the role of Homeland Security in visa issuance, review and security.

While I concur that we must continue to improve methods and technologies for screening and detecting explosives carried by airline passengers, our first line of defense against terrorism is intelligence and visa security.

When it was initially revealed that visas were granted to the 9-11 terrorists to lawfully enter the United States, Congress wisely directed the new Department of Homeland Security to take a larger role in visa security. Prior to that, the Department of State had exercised a historically lax approach to visa security. While the State Department has shown greater diligence in security in recent years, it lacks the law enforcement perspective that is necessary to conduct in depth security review of visa applicants.

As Homeland Security's first Undersecretary for Border and Transportation, it was my responsibility to fulfill the congressional mandate to establish a visa security office, to deploy visa security agents to priority and at-risk embassies, and to identify visa seekers who might pose a risk to the United States.

Prior to the creation of Homeland Security, however, the visa security checks were limited. Consular Officers would interview visa applicants at U.S. embassies

throughout the world; they would conduct automated name checks against watch lists of known terrorists; and they would obtain the applicants' fingerprints and a digital photograph. Now, a visa security agent complements the State Department's efforts, applying a keen law enforcement perspective to further check applicants who are either "not yet known" or flagged to stop them from reaching the United States.

The DHS Visa Security Office's deployment of agents to embassies has been limited due to a lack of funding and resistance from the Department of State. The State Department contends that they do the job adequately and that visa security agents can do their work remotely in Washington. Neither assertion is accurate.

The DHS Inspector General found that the successful vetting of visas requires a hands-on presence at the embassy. On the ground, visa security agents can better connect local intelligence (such as that given by Abdulmutallab's father to our embassy in Nigeria). They can also re-interview applicants if necessary – applying trained law enforcement and security perspectives the State Department simply does not offer.

In one instance cited by the Inspector General, an applicant applied for a student visa at an overseas embassy. Based on available information, the consular officer initially approved the application. The visa security agent, however, further vetted the applicant and produced information that the applicant's uncle was the subject of a terrorism investigation. Because of the agent's work, additional information was provided to the FBI about the uncle, and based on the agent's recommendation; the consular officer denied the student visa.

In 2007 alone, DHS visa agents recommended denials due to security concerns for more than 700 visa applicants. Regrettably, however, agents are posted in fewer than 15 embassies, which is less than ten percent of all our embassies and consulates. This needs to change immediately.

Logic suggests that if hundreds in high-risk areas have been denied visas, other locations may also require a closer look. What is more, America's enemies are smart and resourceful. Soon they will figure out where their chances of obtaining a U.S. visa are greatest, if they haven't done so already.

There is another advantage to the role of Homeland Security deploying visa security agents, and that is another avenue of redress in the event an error is made and a legitimate traveler is wrongly denied a visa. The visa security agent can double check the intelligence and provide a system of redress for an imperfect human system.

It is important to also note that a greater emphasis on visa security does not mean that we should in any way diminish America's role as a gateway to visitors from around the world. Commonsense security measures and an open and welcoming culture are not mutually exclusive. Revoking Abdulmutallab's visa would have done nothing to interfere with the travel plans of any other passenger boarding a flight to America.

Congress must place a priority on funding these critical visa security positions. The Administration needs to make sure the Department of State and DHS are working together on this important mission.

## INTERNATIONAL FLIGHTS

Another tool in protecting our international flights is the control that we have over our own airspace. I have been amazed that some shrug their shoulders as if we have no control over the security systems at international airports outside the United States. True, we are dependent upon our foreign governments for the inspection of passengers that board international flights from overseas headed for the United States, but the leverage of the United States is significant. If we are not satisfied that the security measures are adequate and that the flight is safe then we can advise that the flight cannot enter our airspace, or we can direct the flight to land at a more remote airport on our soil. The latter is more customary and is less problematic for the passengers.

In the case of Flight 253, it became known prior to the terrorist incident that the passenger Abdulmutallab was on board and was on a watch list, even though he was not designated to be on the primary "no fly" list. When this information became known, the flight could have been diverted to a more remote airport for additional security checks. Instead, the decision was made to land the plane and interview the subject at that time. The benefit of diversion of the aircraft when there is any reasonable basis for concern is that steps can be taken for safety of the passengers. This was done from time to time during the 2004 threats to international flights. On a number of occasions a flight was diverted because during the transatlantic flight it became known that a passenger was on a watch list. As Undersecretary, I had to make this call on more than one occasion. This action can thwart a terrorist threat or mitigate against damage.

## FULL BODY SCANS

Certainly, the technology that has been described as "full body scans" increases the potential of detection of explosive material, but we should not deceive ourselves. Even with the most advanced technologies the terrorist can adapt and discover new vulnerabilities. We should not make it unnecessarily difficult on the millions of passengers who fly our commercial aircraft by mandating full body scans which are counter to America's sense of freedom and privacy. Rather, we should concentrate our resources on the multitude of detection tools that are already available, such as additional K-9 explosive detection teams and behavior observation to detect those that pose a risk. Full body scan technology should be available as a secondary screening option, but should not be mandated for every passenger.

## INTELLIGENCE AND WATCH LISTS

After the clear failure to connect available intelligence on the Christmas day incident, it is tempting to dismantle the system in place. However, the system of watch list nomination by a law enforcement agency, followed by a multi agency approach to a

final decision based upon clear standards makes sense, and should not be dismantled without a clear indication that the approach is flawed.

Without question, however, the analyst failed to connect the bits of intelligence on Abdulmutallab that had been placed in the system, failed to place him on the "no fly" list and failed to revoke his visa. Is this a lack of resources for the intelligence analysts who evaluate the bits of data? The answer is most likely. In addition to resources for the visa security positions, Congress should examine ways to make the watch list system more robust and effective.

One final point should be made in regard to the watch lists. As we make the admission to the list more robust and enhance the analyst resources, we have to be sure the analysts have the additional mission of providing redress for those who may have been mistakenly placed in the data base. Regardless, of how we construct the system, it is ultimately a human system that is dependent upon the accuracy of information and the good judgment of the personnel. When errors are made we hope they will be made on the side of security. But at the same time, there must be adequate redress for the passenger who has been mistakenly identified. Both the mission of security and the availability of redress will make the system work for the travelling public.

## CONCLUSION

I appreciate the Committee examining the Christmas day incident, and I look forward to the recommendations of Congress on this important subject.

Respectfully submitted,

Asa Hutchinson

*Asa Hutchinson, president and CEO of Hutchinson Group consulting in Little Rock, is the former Undersecretary for Homeland Security; former Administrator of the DEA; and former Member of Congress.*

Avoiding a Self-inflicted Wound

Brian Michael Jenkins
Bruce Butterworth
Cathal Flynn

President Obama's public anger and his orders to fix intelligence and airline security have not ended the Christmas Day attack saga.

Certainly, the attack was a double failure, first to keep a terrorist off the flight, and second to detect his device. Fortunately it failed, and the explosion might not have brought the plane down anyway.

But it has handed al-Qaeda a victory. Persuading a pathetic recruit to carry a bomb in his underpants won global notoriety for al Qaeda's Yemeni branch, reminded Americans of their vulnerabilities, and plunged the U.S. into irrelevant debate. But this is an opportunity. Let's stop posturing and adjust intelligence and aviation security to confront our adversaries. Some key points

*Airliners will remain targets.* Since the first terrorist hijackings and airline bombings four decades ago, terrorists have remained obsessed with airliners, despite aviation being the best protected form of transportation. The public reaction to this recent attempt fuels their ambition.

*The terrorists will adapt.* When we deploy new measures, terrorists try to circumvent them. Observing pat-downs probably led to the underpants bomb. But security measures have complicated their lives. They have chosen suicide attackers, plentiful but not always bright. They use smaller, less detectable but less reliable explosives, and try to assemble bombs in flight. Their chances of failure increase.

*Intelligence ain't easy.* "Connect the dots" trivializes the difficulty of intelligence. It is always easy afterwards, when you know what happened and who did it;

much harder in advance, when the data include thousands of names and fragments of information and you don't know how, when or where an attack will come. Post-attack investigations erroneously create an impression of foresight.

The President has said intelligence failures were systemic, but adjustments should be systemic and precise. Since the Director of National Intelligence is in charge, Congress should ask him what he needs. Is it clearer authority, or different resources, or both?

*Streamline, don't reorganize.* Another major reorganization will move things backwards. The last one proliferated intelligence centers, scattered precious talent, and imposed complicated protocols. Better to get a critical mass of talent at one location and streamline things.

*Intelligence and security mutually reinforce.* Besides warning of terrorist plots, intelligence should identify trends that should change security, such as detecting bomb components hidden in previously unthinkable places. And changed security measures can force terrorists to stumble across tripwires by buying large quantities of bleach to make explosives.

*Pursue greater e flexibility in security.* Detecting bomb components *requires the* integration of several technologies. There are no "silver bullets." Stringent screening can physically be applied only to a fraction of passengers. Intelligence must help define who they are. A Registered Passenger program must also allow frequent flyers and others who submit to background checks to be screened less rigorously, allowing authorities to focus resources. Testing confirms that screening all passengers identically means that nearly all passengers will be screened inadequately. It's time we faced this fact.

*No More Chrome:* Seize the opportunity to re-examine screening, a 37 year accumulation of practices. Without that reexamination, the Government's

deployment of body scanners will aggravate things. Body scanners, particularly when programmed for "privacy," would have missed Abdulmuttalab's explosives. In contrast, less expensive trace detectors most probably would have detected them. We know from post-attack testing eight years ago that they almost certainly would have stopped the Shoe Bomber. Why are they not being considered along with scanners?

Systematic checkpoint reconfiguration, not piecemeal addition, is essential. The TSA should undertake a thorough system review. Additionally, Secretary Napolitano, applying an Armed Services' practice, should commission two independent and separate external efforts, then compare the results of all three.

*Get realistic about risk.* America is in a new, long struggle with al Qaeda and its affiliates. Those who claim the Christmas Day attack happened because the administration doesn't sufficiently use the term "war" miss the implications of their own words. In a war, and in this struggle, the enemy may win some battles and cause some casualties.

The key now is to calmly focus, learn the lessons of the Christmas Day attack, and do our duty to reduce the risk to all who fly on airliners.

Brian Michael Jenkins, senior advisor at the RAND Corporation, was a member of the White House Commission on Aviation Security and Safety, and is co-author of *Aviation, Terrorism and Security*; Cathal Flynn was the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, 1993 to 2000; Bruce Butterworth was the Director of Civil Aviation Security Policy and Operations, Federal Aviation Administration from 1991 to 2000, and has co-authored several works with Mr. Jenkins.

# DEPARTMENT OF STATE

STATEMENT
OF

PATRICK F. KENNEDY

UNDER SECRETARY OF STATE FOR MANAGEMENT,
DEPARTMENT OF STATE

BEFORE THE

SENATE COMMITTEE ON THE JUDICIARY

HEARING

ON

SECURING AMERICA'S SAFETY: IMPROVING THE EFFECTIVENESS OF ANTI-TERRORISM TOOLS AND INTER-AGENCY COMMUNICATION

JANUARY 20, 2010

**Chairman Leahy, Ranking Member Sessions and distinguished Members of the Committee**, thank you for the opportunity to address you today. As a result of the attempted terrorist attack on Flight 253, the President ordered corrective steps to address systemic failures in procedures we use to protect the people of the United States. Secretary Clinton reiterated this direction when she stated, "we all are looking hard at what did happen in order to improve our procedures to avoid human errors, mistakes, oversights of any kind. We in the State Department are fully committed to accepting our responsibility for the mistakes that were made, and we're going to be working hard with the rest of the Administration to improve every aspect of our efforts." Therefore, the Department of State now is working on reviewing visa issuance and revocation criteria and determining how technological enhancements can facilitate and strengthen visa-related business processes.

Our immediate attention is on addressing the deficiencies identified following the attempted attack on Flight 253. At the same time we continue to plan for the future, incorporating new technology, increasing data sharing and enhancing operational cooperation with partner agencies. We have a record of quickly adapting and improving our procedures to respond to security imperatives. We have a highly trained global team working daily to protect our borders and fulfill the overseas border security mission and other critical tasks ranging from crisis management to protection of American interests abroad. Within the Department we have a dynamic partnership between the Bureau of Consular Affairs and the Bureau of Diplomatic Security that adds a valuable law enforcement and investigative component to our capabilities. We will use these strengths to address the continuing security threats.

In the case of Umar Farouk Abdulmutallab, on the day following his father's November 19 visit to the Embassy, we sent a cable to the Washington intelligence and law enforcement community through proper channels (the Visas Viper system) that "Information at post suggests [that Farouk] may be involved in Yemeni-based extremists." At the same time, the Consular Section entered Abdulmutallab into the Consular Lookout and Support System database known as CLASS. In sending the Visas

Viper cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, but entered it correctly into CLASS. As a result of the misspelling in the cable, information about previous visas issued to him and the fact that he currently held a valid U.S. visa was not included in the cable. At the same time the CLASS entry resulted in a lookout using the correct spelling that was shared automatically with the primary lookout system used by the Department of Homeland Security (DHS) and accessible to other agencies.

We have taken immediate action to improve the procedures and content requirements for Visas Viper cable reporting that will call attention to the visa application and issuance material that is already in the data that we share with our national security partners. All officers have been instructed to include complete information about all previous and current U.S. visa(s). This guidance includes specific methods to comprehensively and intensively search the database of visa records so that all pertinent information is obtained.

In addition to this change in current procedures to search visa records, we immediately began working to refine the capability of our current systems. When dealing with applications for visas, we employ strong, sophisticated name searching algorithms to ensure matches between names of visa applicants and any derogatory information contained in the 27 million records found in CLASS. This strong searching capability has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We will use our significant experience with search mechanisms for derogatory information to improve the systems for checking our visa issuance records.

The Department of State has been matching new threat information with our records of existing visas since 2002. We have long recognized this function as critical to the way we manage our records and processes. This system of continual vetting has evolved as post 9/11 reforms were instituted and is now performed by the Terrorist Screening Center (TSC). All records added to the Terrorist Screening Database are checked against the

Department's Consolidated Consular Database (CCD) to determine if there are matching visa records. Matches are sent electronically from the TSC to the Department of State to flag cases for visa revocation. In almost all such cases, visas are revoked. In addition, we have widely disseminated our data to other agencies that may wish to learn whether a subject of interest has a U.S. visa. Cases for revocation consideration are forwarded to us by DHS/Customs and Border Protection's (CBP) National Targeting Center (NTC) and other entities. Almost every day, we receive requests to review and, if warranted, revoke visas for potential travelers for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours per day/7 days per week to work these issues. Many of these requests are urgent because the person is about to board a plane. The State Department then uses its authority to prudentially revoke the visa.

Since the Presidentially-ordered Security Review, there have been changes in the thresholds for adding individuals to the Terrorist Screening Database, No Fly, and Selectee lists. The number of revocations has increased substantially as a result. This revocation work is processed electronically in the Department. As soon as information is established to support a revocation, an entry showing the visa revocation is added electronically to the Department of State's lookout system and shared in real time with the DHS lookout systems used for border screening.

In addition to these changes, the Department is reviewing the procedures and criteria used in the field to revoke visas and will issue new instructions to our officers. Revocation recommendations will be added as an element of reporting through the Visas Viper channel. We will be reiterating our guidance on use of the broad discretionary authority of visa officers to deny visas on security and other grounds. Instruction in appropriate use of this authority has been a fundamental part of officer training for several years.

The State Department has broad and flexible authority to revoke visas and we use that authority widely to protect our borders. Since 2001, we have revoked 51,000 visas for a variety of reasons, including over 1,700 for suspected links to terrorism. We have been

actively using this authority as we perform internal scrubs of our data with watchlist information provided by partner agencies. For example, we are re-examining information in our CLASS database on individuals with potential connections to terrorist activity or support for such activity. We are reviewing all previous Visas Viper submissions as well as cases that other agencies are bringing to our attention from the No Fly and Selectee lists, as well as other sources. In these reviews, we have identified cases for revocation and we have also confirmed that substantial numbers of individuals in these classes hold no visas and of those few who did, many were revoked prior to the current review. We recognize the gravity of the threat we face and are working intensely with our colleagues from other agencies to ensure that when the U.S. Government obtains information that a person may pose a threat to our security, that person does not hold a visa.

We will use revocation authority prior to interagency consultation in circumstances where we believe there is an immediate threat. Revocation is an important tool in our border security arsenal. At the same time, expeditious coordination with our national security partners is not to be underestimated. There have been numerous cases where our unilateral and uncoordinated revocation would have disrupted important investigations that were underway by one of our national security partners. They had the individual under investigation and our revocation action would have disclosed the U.S. Government's interest in the individual and ended our colleagues' ability to quietly pursue the case and identify terrorists' plans and co-conspirators.

In addition to revocation efforts, consular officers refused 1,885,017 visas in FY2009. We now are renewing guidance to our officers on their discretionary authority to refuse visas under section 214(b) of the Immigration and Nationality Act with specific reference to cases that raise security concerns. No visa is issued without it being run through security checks against our partners' data. And we screen applicants' fingerprints against U.S. databases as well.

The Department has a close and productive partnership with DHS, which has authority for visa policy. Over the past seven years both agencies significantly increased resources, improved procedures and upgraded systems devoted to supporting the visa function. DHS receives all of the information collected by the Department of State during the visa process. DHS has broad access to our entire CCD, containing 136 million records related to both immigrant and nonimmigrant visas and covering visa actions of the last 13 years. Special extracts of data are supplied to elements within DHS, including the Visa Security Units of Immigration and Customs Enforcement (ICE). These extracts have been tailored to the specific requirements of those units. We are working closely with ICE Visa Security Units established abroad and with domestic elements of DHS, such as CBP's National Targeting Center.

We gave DHS access to U.S. passport records, used by CBP to confirm the identity of citizens returning to the U.S. We developed new card-type travel documents that work with the automated systems CBP installed at the U.S. land borders. We are collecting more information electronically and earlier in the process. Expanded data collection done in advance of travel will give DHS and partner agencies richer information and more time for analysis.

We make all of our visa information available to other involved agencies, and we specifically designed our systems to facilitate comprehensive data sharing. We give other agencies immediate access to over 13 years of visa data, and they use this access extensively. In November 2009, more than 16,000 employees of DHS, the Department of Defense (DOD), the FBI and Commerce made 920,000 queries on visa records. We embrace a layered approach to border security screening and are fully supportive of the DHS Visa Security Program.

The Department of State is at the forefront of interagency cooperation and data sharing to improve border security, and we embarked on initiatives that will position us to meet future challenges while taking into consideration our partner agencies and their specific needs and requirements. We are implementing a new generation of visa processing

systems that will further integrate information gathered from domestic and overseas activities. We are restructuring our information technology architecture to accommodate the unprecedented scale of information we collect and to keep us agile and adaptable in an age of intensive and growing requirements for data and data sharing.

We proactively expanded biometric screening programs and spared no effort to integrate this expansion into existing overseas facilities. In partnership with DHS and the FBI, we established the largest biometric screening process on the globe. We were a pioneer in the use of facial recognition techniques and remain a leader in operational use of this technology. In 2009 we expanded use of facial recognition from a selected segment of visa applications to all visa applications. We now are expanding our use of this technology beyond visa records. We are testing use of iris recognition technology in visa screening, making use of both identity and derogatory information collected by DOD. These efforts require intense ongoing cooperation from other agencies. We successfully forged and continue to foster partnerships that recognize the need to supply accurate and speedy screening in a 24/7 global environment. As we implement process and policy changes, we are always striving to add value in both border security and in operational results. Both dimensions are important in supporting the visa process.

The Department of State is an integral player on the border security team. We are the first line of defense. Our global presence, foreign policy mission and personnel structure give us singular advantages in executing the visa function throughout the world. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. national interests. The issuance and refusal of visas has a direct impact on foreign relations. Visa policy quickly can become a significant bilateral problem that harms U.S. interests if handled without consideration of foreign policy impacts. The conduct of U.S. visa policy has a direct and significant impact on the treatment of U.S. citizens abroad. The Department of State is in a position to anticipate and weigh those possibilities.

We developed and implemented intensive screening processes requiring personal interviews, employing analytic interview techniques, incorporating multiple biometric checks, all built around a sophisticated global information technology network. This frontline of border security has visa offices present in virtually every country of the world. They are staffed by highly trained and multi-lingual personnel of the Department of State. These officials are dedicated to a career of worldwide service and provide the cultural awareness, knowledge and objectivity to ensure that the visa function remains the frontline of border security.

In addition, we have 145 officers and 540 locally employed staff devoted specifically to fraud prevention and document security, including fraud prevention officers at overseas posts. We have a large Fraud Prevention Programs office in Washington, D.C. that works very closely with the Bureau of Diplomatic Security, and we have fraud screening operations using sophisticated database checks at both the Kentucky Consular Center and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging applications and applicants who lack credibility, who present fraudulent documents, or who give us false information adds a valuable dimension to our visa process.

The Bureau of Diplomatic Security adds an important law enforcement element to the Department's visa procedures. There are now 50 Assistant Regional Security Officer Investigators abroad specifically devoted to maintaining the integrity of the process. They are complemented by officers working domestically on both visa and passport matters. These Diplomatic Security officers staff a unit within the Bureau of Consular Affairs that monitors overseas visa activities to detect risks and vulnerabilities. These highly trained law enforcement professionals add another dimension to our border security efforts.

The multi-agency team effort on border security, based upon broadly shared information, provides a solid foundation. At the same time we remain fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information. We have and we will continue to automate processes to reduce the

possibility of human error. We fully recognize that we were not perfect in our reporting in connection with the attempted terrorist attack on Flight 253. We are working and will continue to work not only to address that mistake but to continually enhance our border security screening capabilities and the contributions we make to the interagency effort.

We believe that U.S. interests in legitimate travel, trade promotion, and educational exchange are not in conflict with our border security agenda and, in fact, further that agenda in the long term. Our long-term interests are served by continuing the flow of commerce and ideas that are the foundations of prosperity and security. Acquainting people with American culture and perspectives remains the surest way to reduce misperceptions about the United States. Fostering academic and professional exchange keeps our universities and research institutions at the forefront of scientific and technological change. We believe the United States must meet both goals to guarantee our long-term security.

We are facing an evolving threat. The tools we use to address this threat must be sophisticated and agile. Information obtained from these tools must be comprehensive and accurate. Our criteria for taking action must be clear and coordinated. The team we use for this mission must be the best. The Department of State has spent years developing the tools and personnel needed to properly execute the visa function overseas and remains fully committed to continuing to fulfill its essential role on the border security team.

**Patrick F. Kennedy**
U.S. Department of State, Under Secretary for Management
Term of Appointment: 11/06/2007 to present

Patrick F. Kennedy, a Career Minister in the Foreign Service, was confirmed by the U.S. Senate as Under Secretary of State for Management on November 6, 2007. As Under Secretary for Management he is responsible for the people, resources, facilities, technology, consular affairs, and security of the Department of State and is the Secretary's principal advisor on management issues. He also provides regular direction to the Bureau of Resource Management, and the Chief Financial Officer serves as a core member of the Under Secretary's senior management team. He is the State Department's representative on the President's Management Council.

Prior to assuming his new position, he was Director of the Office of Management Policy, Rightsizing, and Innovation from May 2007; Deputy Director of National Intelligence for Management from April 2005 to May 2007; and from February 2005 to April 2005 he headed the Transition Team that set up the newly created Office of the Director of National Intelligence.

From September 2001 to May 2005 he was U.S. Representative to the United Nations for Management and Reform with the Rank of Ambassador. During this period he also served from May 2003 to the end of November 2003 as Chief of Staff of the Coalition Provisional Authority in Iraq, and from May 2004 to late August 2004 as the Chief of Staff of the Transition Unit in Iraq.

In 1993 he became Assistant Secretary of State for Administration and served in the post until 2001. Concurrently, from August 1996 to August 1997 he served as the Acting Under Secretary for Management; during 1998, as Acting Assistant Secretary of State for Diplomatic Security; and from 1997 to 2001 as the coordinator for the reorganization of the foreign affairs agencies. From 1973, when he joined the Foreign Service, to 1993, he served in a number of positions in Washington and overseas, including as Management Counselor at the Embassy in Cairo and Executive Director and Deputy Executive Secretary of the Executive Secretariat.

Mr. Kennedy is a native of Chicago, Illinois and received a BSFS from Georgetown University.

Statement of

# The Honorable Patrick Leahy

United States Senator
Vermont
January 20, 2010

---

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing On "Securing America's Safety: Improving The Effectiveness
Of Anti-Terrorism Tools And Inter-Agency Communication"
January 20, 2009

I want to begin by thanking President Obama, Secretary Clinton, USAID Administrator Shah, General Fraser of the U.S. Southern Command, and all the hard working people here and on the ground in Haiti for their efforts to save lives in the aftermath of the devastating earthquake. Recovering from this disaster is a daunting challenge for the people of Haiti, but Vermonters and all Americans have opened their hearts and are sharing generously, and we will continue to do so.

Now to the subject of this important hearing. A terrorist intent on detonating an explosive was able to board a plane with hundreds of passengers headed for Detroit, Michigan, on Christmas Day. After Congress passed major legislation in 2004 to implement the 9/11 Commission's recommendations, and after the country invested significant resources to upgrade security systems and reorganize our intelligence agencies, the near tragedy on Christmas Day compels us to ask what went wrong and what additional reforms are needed.

The administration responded quickly, and has already conducted a preliminary review. The President has candidly identified problems. He spoke directly to the American people about the incident, the threat, and the actions that are necessary to prevent future attempted attacks. This administration did not offer excuses but is, instead, taking responsible action to provide additional security measures.

I expect hard questions to be asked at this hearing. We will want to know how and why we failed to successfully detect and prevent this attempted attack. How did someone who paid for an airline ticket with cash, who boarded without luggage for a winter trip to Detroit, and whose father had come to U.S. officials weeks before to warn that his son had become radicalized, board a flight for the United States with a valid visa? Just as the horrific, deadly attacks on 9/11 could have been prevented, the recent White House review found that the Government "had sufficient information to have uncovered and potentially disrupted the December 25 attack." Our intelligence agencies did not adequately integrate and analyze information that could have prevented the Christmas Day attempt. The President called it a "systemic failure," and he is right

that this is unacceptable.

While I expect hard questions to be asked, I hope that all Senators will proceed with the shared purpose of making America safer. No one has been angrier or more determined than the President. He did not respond with denial and obfuscation, but instead came forward to identify failures and correct them.

Let this not be a setting in which anyone seeks partisan advantage. We are all Americans, and we are all in this together. "Passions and politics" should not obscure or distract us. We should all do our part. As the President said recently in announcing the immediate actions he had ordered: "Instead of giving into cynicism and division, let's move forward with the confidence and optimism and unity that define us as a people. For now is not a time for partisanship, it's a time for citizenship – a time to come together and work together with the seriousness of purpose that our national security demands." That is what we did after 9/11; that is what we need to do today.

Our witnesses today are public officials, not our adversaries. They each share with us a common purpose, as the President said, "to prevail in this fight . . . to protect our country and pass it – safer and stronger – to the next generation."

Director Mueller assumed his duties just days before 9/11 and has led the FBI through a transition to expand its intelligence and counterterrorism role in protecting our country. His perspective on how prior reforms have worked and what changes still need to be made can be extremely helpful.

Today we have the opportunity to consider with Director Mueller and high-ranking representatives from the State Department and Department of Homeland Security (DHS) how we can strengthen and extend our security by better use of visa processes, airline screening and other means. We need to ensure that our border security officials are equipped with the tools and information necessary to identify threats before a terrorist with explosives is already on board an aircraft headed to the United States. Together we can understand how we all can do a better job of protecting the United States.

One of the challenges faced by those analyzing intelligence is the sheer volume of information coming into our intelligence agencies every day. How do we make sure that information is not only available in a terrorism database, but that it is also promptly and successfully analyzed? How can we prioritize the information that needs to be acted upon from the information that does not? And how do we ensure that intelligence agencies are held accountable for taking the necessary action when important intelligence comes in?

We also need to understand how we can best upgrade our airline screening systems. The administration has announced that it will deploy enhanced screening technology nationwide. Just this year, however, the Government Accountability Office (GAO) issued a report finding that DHS and the Transportation Security Agency (TSA) have in past years spent almost $800 million in technology to screen airline passengers, but have still not completed key risk assessments to ensure that the technologies address priority security needs. The report also found that TSA has developed 10 different passenger screening technologies, but has not deployed any

of them nationwide.

In the aftermath of the Christmas Day plot, as well as the Fort Hood tragedy, it can be tempting to forget that it is always easier to connect the dots in hindsight. It was not our intelligence agencies who first raised the alarm about the suspect who tried to blow up the Northwest Airlines flight. It was the suspect's own father, a Nigerian, who turned him in.

Our response to this incident must be swift, but also thoughtful. I am concerned that simply adding a handful of countries to heightened security lists does not prevent terrorists from coming into this country and may alienate those we need as allies. After all, Richard Reid was a British national and did not fit a general profile until he became known as the attempted shoe bomber. No single individual has caused more deaths by terrorist action in the United States than Timothy McVeigh, and he fit no ethnic or religious profile.

It may be tempting to take reflexive actions, but to do so will only result in the unnecessary denial of visas to legitimate travelers and the flooding of our watchlists such that they become ineffective tools in identifying those who would do us harm. Such actions will not solve these issues, they will only isolate us further from the allies we need. A "one size fits all" mentality will only ensure that we will miss different threats in the future. As the President properly noted, we cannot "hunker down and hide behind walls of fear and mistrust." We should not let our response to this incident provide another recruiting tool for terrorists. We have to be smarter than that.

Finally, this morning, the Inspector General released a report detailing the misuse of so-called "exigent letters" by the FBI to obtain information about U.S. persons. The report describes how the FBI used these exigent letters without proper authorization to collect thousands of phone records, including in instances where no exigent conditions existed. The report also details how the FBI then compounded the misconduct by trying to issue National Security Letters after the fact. This was not a matter of technical violations. This was authorized at high levels within the FBI, and continued for years. I understand, Director Mueller, that the FBI has worked to correct these abuses, but this report is a sobering reminder of the significant abuse of this broad authority. There must be accountability.

# # # # #

**Senate Committee on the Judiciary**

**20 January 2010**

# "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"

**Statement for the Record**

**of**

**Michael E. Leiter**
**Director of the National Counterterrorism Center**

**Statement for the Record**

20 January 2010

Senate Committee on the Judiciary
"Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"

Chairman Leahy, Ranking Member Sessions, and Members of the Committee on the Judiciary: Thank you for your invitation to appear before the committee to discuss the events leading up to the attempted terrorist attack on Christmas day and the improvements the National Counterterrorism Center and the Intelligence Community have underway to fix deficiencies. However, I regret that I will not be able to appear before the committee today, as I am testifying before another committee during this time.

The attempted terrorist attack on Christmas day did not succeed, but, as one of several recent attacks against the United States inspired by jihadist ideology or directed by al Qa'ida and its affiliates, it reminds us that our mission to protect Americans is unending.

Let's start with this clear assertion: Umar Farouk Abdulmutallab should not have stepped on that plane. The counterterrorism system failed and we told the President we are determined to do better.

Within the Intelligence Community we had strategic intelligence that al Qa'ida in the Arabian Peninsula (AQAP) had the intention of taking action against the United States prior to the failed attack on December 25th, but, we did not direct more resources against AQAP, nor insist that the watchlisting criteria be adjusted prior to the event. In addition, the Intelligence Community analysts who were working hard on immediate threats to Americans in Yemen did not understand the fragments of intelligence on what turned out later to be Mr. Abdulmutallab, so they did not push him onto the terrorist watchlist.

We are taking a fresh and penetrating look at strengthening both human and technical performance and do what we have to do in all areas. Director of National Intelligence Blair and I have specifically been tasked by the President to improve and manage work in four areas:

Immediately reaffirm and clarify roles and responsibilities of the counterterrorism analytic components of the IC in synchronizing, correlating, and analyzing all sources of intelligence related to terrorism.

Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.

Take further steps to enhance the rigor and raise the standard of tradecraft of intelligence analysis, especially analysis designed to uncover and prevent terrorist plots.

Ensure resources are properly aligned with issues highlighted in strategic warning analysis.

Additionally, NCTC has been tasked by the President to do the following:

Establish and resource appropriately a process to prioritize and to pursue thoroughly and exhaustively terrorism threat threads, to include the identification of appropriate follow-up action by the intelligence, law enforcement, and homeland security communities.

Establish a dedicated capability responsible for enhancing record information on possible terrorist in the Terrorist Identities Datamart Environment for watchlisting purposes.

**The Events Leading Up to the Christmas Day Attack**

I will now briefly discuss some of the details of the bombing attempt and what we missed. As the President has said, this was not—like in 2001—a failure to collect or share intelligence; rather it was a failure to connect, integrate, and understand the intelligence we had.

Although NCTC and the Intelligence Community had long warned of the threat posed by al Qa'ida in the Arabian Peninsula, we did not correlate the specific information that would have been required to help keep Abdulmutallab off that Northwest Airlines flight.

More specifically, the Intelligence Community highlighted the growing threat to US and Western interests in the region posed by AQAP, whose precursor

elements attacked our embassy in Sana'a in 2008. Our analysis focused on AQAP's plans to strike US targets in Yemen, but it also noted—increasingly in the Fall of 2009—the possibility of targeting the United States. We had analyzed the information that this group was working with an individual who we now know was the individual involved in the Christmas attack.

In addition, the Intelligence Community warned repeatedly of the type of explosive device used by Abdulmutallab and the ways in which it might prove a challenge to screening. Of course, at the Amsterdam airport, Abdulmutallab was subjected to the same screening as other passengers—he passed through a metal detector, which didn't detect the explosives that were sewn into his clothes.

As I have noted, despite our successes in identifying the overall themes that described the plot we failed to make the final connections—the "last tactical mile"—linking Abdulmutallab's identity to the plot. We had the information that came from his father that he was concerned about his son going to Yemen, coming under the influence of unknown religious extremists, and that he was not going to return home. We also had other streams of information coming from intelligence channels that provided pieces of the story. We had a partial name, an indication of a Nigerian, but there was nothing that brought it all together—nor did we do so in our analysis.

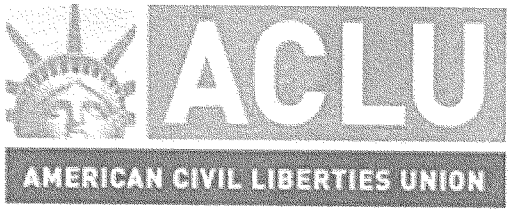
As a result, although Mr. Abdulmutallab was identified as a known or suspected terrorist and entered into the Terrorist Identities Datamart Environment (TIDE)—and this information was in turn widely available throughout the Intelligence Community—the derogatory information associated with him did not meet the existing policy standards—those first adopted in the summer of 2008 and ultimately promulgated in February 2009—for him to be "watchlisted," let alone placed on the No Fly List or Selectee lists.

Had all of the information the U.S. had available, fragmentary and otherwise, been linked together, his name would have undoubtedly been entered on the Terrorist Screening Database which is exported to the Department of State and the Department of Homeland Security. Whether he would have been placed on either the No Fly or Selectee list—again based on the existing standards—would have been determined by the strength of the analytic judgment. One of the clear lessons the U.S. Government has learned and which the Intelligence Community will support is the need to modify the standards for inclusion on such lists.

In hindsight, the intelligence we had can be assessed with a high degree of confidence to describe Mr. Abdulmutallab as a likely operative of AQAP. But

without making excuses for what we did not do, I think it critical that we at least note the context in which this failure occurred: Each day NCTC receives literally thousands of pieces of intelligence information from around the world, reviews literally thousands of different names, and places more than 350 people a day on the watchlist—virtually all based on far more damning information than that associated with Mr. Abdulutallab prior to Christmas Day. Although we must and will do better, we must also recognize that not all of the pieces rise above the noise level.

The men and women of the National Counterterrorism Center and the Intelligence Community are committed to fighting terrorism at home and abroad and will seek every opportunity to better our analytical tradecraft, more aggressively pursue those that plan and perpetrate acts of terrorism, and effectively enhance the criteria used to keep known or suspected terrorists out of the United States.




Written Statement of the

American Civil Liberties Union

Michael W. Macleod-Ball

Acting Director, Washington Legislative Office

Christopher Calabrese

Legislative Counsel

before the

Senate Committee on the Judiciary

January 20, 2009

*Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication*


WASHINGTON LEGISLATIVE OFFICE

915 15th Street, NW Washington, D.C. 20005

(202) 544-1681 Fax (202) 546-0738

**Written Statement of the**

**American Civil Liberties Union**

**Michael W. Macleod-Ball**

**Acting Director, Washington Legislative Office**

**Christopher Calabrese**

**Legislative Counsel**

**before the**

**Senate Committee on the Judiciary**

**January 20, 2010**

Chairman Leahy, Ranking Member Sessions, and Members of the Committee:

The American Civil Liberties Union (ACLU) has more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. In particular, throughout our history, we have been one of the nation's pre-eminent advocates in support of privacy and equality. We write today to express our strong concern over the three substantive policy changes that are being considered in the wake of the attempted terror attack on Christmas Day: the wider deployment of whole body imaging (WBI) devices, the expanded use of terror watch lists and increased screening of individuals from fourteen so-called nations of interest. The ACLU believes that each of these technologies greatly infringe on civil liberties and face serious questions regarding its efficacy in protecting airline travelers.

The President has already identified a failure of intelligence as the chief cause of the inability to detect the attempted terror attack on Christmas day. As such, the government's response must be directed to that end. These invasive and unjust airline security techniques represent a dangerous diversion of resources from the real problem. This diversion of resources promises serious harm to American's privacy and civil liberties while failing to deliver significant safety improvements.

## I. Introduction

WBI uses millimeter wave or X-ray technology to produce graphic images of passengers' bodies, essentially taking a naked picture of air passengers as they pass through security checkpoints. This technology is currently deployed at 19 airports and the Department of Homeland Security (DHS) recently announced the roll out of 300 more machines by year end. [1] While initially described as a secondary screening mechanism, DHS is now stating that WBI will be used for primary screening of passengers.[2]

Another way of screening passengers is through terror watch lists. The terror watch lists are a series of lists of names of individuals suspected of planning or executing terrorist attacks. The master list is maintained by the Terrorist Screening Center (TSC) and contains more than one million names.[3] Subsets of this list include the No Fly list (barring individuals from air travel) and the Automatic Selectee list (requiring a secondary screening). The names on this list and the criteria for placement on these lists are secret.[4] There is no process allowing individuals to challenge their placement on a list or seek removal from a list.

Finally, individuals who were born in, are citizens of, or are traveling from fourteen nations will receive additional scrutiny under a policy announced by the US government after the attempted terror attack. As of January 19, 2010 these nations are Afghanistan, Algeria, Cuba, Iran, Lebanon, Libya, Iraq, Nigeria, Pakistan, Saudi Arabia, Somalia, Sudan, Syria and Yemen.

The ACLU believes that Congress should apply the following two principles in evaluating any airline security measure:

- **Efficacy.** New security technologies must be genuinely effective, rather than creating a false sense of security. The wisdom supporting this principle is obvious: funds to increase aviation security are limited, and any technique or technology must work and be substantially better than other alternatives to deserve some of the limited funds available. It therefore follows that before Congress invests in technologies or employs new screening methods, it must

[1] Harriet Baskas, *Air security: Protection at privacy's expense?* Msnbc.com, January 14, 2010. http://www.msnbc.msn.com/id/34846903/ns/travel-tips/

[2] Paul Giblin and Eric Lipton, *New Airport X-Rays Scan Bodies, Not Just Bags*, New York Times, February 24, 2007.

[3] *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Justice Department, Office of the Inspector General, Audit Report 09-25, May 2009, pg 3. http://www.justice.gov/oig/reports/FBI/a0925/final.pdf

[4] *Id* at 70.

demand evidence and testing from neutral parties that these techniques have a likelihood of success.

- **Impact on Civil Liberties.** The degree to which a proposed measure invades privacy should be weighed in the evaluation of any technology. If there are multiple effective techniques for safeguarding air travel, the least intrusive technology or technique should always trump the more invasive technology.

## II. Screening Techniques and Technologies Must Be Effective, or they Should Not be Utilized or Funded

The wider deployment of whole body imaging (WBI) devices, expanded use of terror watch lists and increased screening of individuals from fourteen so-called nations of interest each face significant questions regarding their efficacy in protecting air travelers and combating terrorism.

Whole Body Imaging

There are no magic solutions or technologies for protecting air travelers. Ben Wallace, a current member of the British parliament who advised a research team at *QinetiQ*, a manufacturer of body screening devices, has stated that their testing demonstrated that these screening devices would not have discovered a bomb of the type used on Christmas day, as they failed to detect low density materials like powders, liquids and thin plastics. [5] A current QinetiQ product manager admitted that even their newest body scan technology probably would not have detected the underwear bomb.[6] The British press has also reported that the British Department for Transport (DfT) and the British Home Office have already tested the scanners and were not convinced they would work comprehensively against terrorist threats to aviation.[7]

In addition we know that al Qaeda has already discovered a way to work around this technology. In September a suicide bomber stowed a full pound of high explosives and a detonator inside his rectum, and attempted to assassinate a Saudi prince by blowing himself up.[8] While the attack only slightly wounded the prince, it fully defeated an array of security measures including metal detectors and palace security. The bomber spent 30 hours in the close company of the prince's own secret service agents – all without anyone suspecting a thing. WBI devices – which do not penetrate the body – would not have detected this device.

The practical obstacles to effective deployment of body scanners are also considerable. In the United States alone, 43,000 TSA officers staff numerous security gates at over 450 airports and over 2 million passengers a day.[9] To avoid being an ineffective "Maginot line," these $170,000 machines will need to be put in place at all gates in all airports; otherwise a

[5] Jane Merrick, *Are planned airport scanners just a scam?* The Independent, January 3, 2010.
[6] *Id.*
[7] *Id.*
[8] Sheila MacVicar , *Al Qaeda Bombers Learn from Drug Smugglers*, CBSnews.com, September 28, 2009
[9] http://www.tsa.gov/what_we_do/screening/security_checkpoints.shtm

terrorist could just use an airport gate that does not have them. Scanner operators struggle constantly with boredom and inattention when tasked with the monotonous job of scanning thousands of harmless individuals when day after day, year after year, no terrorists come through their gate. In addition to the expense of buying, installing and maintaining these machines, additional personnel will have to be hired to run them (unless they are shifted from other security functions, which will degrade those functions).

The efficacy of WBI devices must be weighed against not only their impact on civil liberties (discussed further below) but also their impact on the U.S. ability to implement other security measures. Every dollar spent on these technologies is a dollar that is not spent on intelligence analysis or other law enforcement activity. The President has already acknowledged that it was deficiencies in those areas – not aviation screening – that allowed Umar Farouk Abdulmutallab to board an airplane.

Watch Lists

The events leading up to the attempted Christmas attack are a telling indictment of the entire watch list system. In spite of damning information, including the direct plea of Abdulmutallab's father, and other intelligence gathered about terrorist activity in Yemen, Abdulmutallab was not placed into the main Terrorist Screening Database. We believe that fact can be directly attributed to the bloated and overbroad nature of the list – now at more than a million names.[10] The size of the list creates numerous false positives, wastes resources and hides the real threats to aviation security. As we discuss below it also sweeps up many innocent Americans – falsely labeling them terrorists and providing them with no mechanism for removing themselves from the list.

These problems are not hypothetical. They have real consequences for law enforcement and safety. An April 2009 report from the Virginia Fusion Center states

> According to 2008 Terrorism Screening Center ground encounter data, al-Qa'ida was one of the three most frequently encountered groups in Virginia. In 2007, at least 414 encounters between suspected al-Qa'ida members and law enforcement or government officials were documented in the Commonwealth. Although the vast majority of encounters involved automatic database checks for air travel, a number of subjects were encountered by law enforcement officers.[11]

Every time a law enforcement officer encounters someone on the terrorist watch list (as determined by a check of the National Crime Information Center (NCIC) database) they contact the TSC. So in essence Virginia law enforcement is reporting that there are more than 400 al Qaeda terrorists in Virginia in a given year. This is difficult to believe. [12] In reality most, if not all, of these stops are false positives, mistakes regarding individuals who should not be on the list. These false positives can only distract law enforcement from real dangers.

---

[10] *DOJ OIG* Audit Report 09-25, pg 3. http://www.justice.gov/oig/reports/FBI/a0925/final.pdf

[11] Virginia Fusion Center, *2009 Virginia Terrorism Threat Assessment*, March 2009, pg 27.

[12] The report does not state that any of these individuals were arrested.

A 2009 report by the Department of Justice Inspector General found similarly troubling results. From the summary:

> We found that the FBI failed to nominate many subjects in the terrorism investigations that we sampled, did not nominate many others in a timely fashion, and did not update or remove watchlist records as required. Specifically, in 32 of the 216 (15 percent) terrorism investigations we reviewed, 35 subjects of these investigations were not nominated to the consolidated terrorist watchlist, contrary to FBI policy. We also found that 78 percent of the initial watchlist nominations we reviewed were not processed in established FBI timeframes.
>
> Additionally, in 67 percent of the cases that we reviewed in which a watchlist record modification was necessary, we determined that the FBI case agent primarily assigned to the case failed to modify the watchlist record when new identifying information was obtained during the course of the investigation, as required by FBI policy. Further, in 8 percent of the closed cases we reviewed, we found that the FBI failed to remove subjects from the watchlist as required by FBI policy. Finally, in 72 percent of the closed cases reviewed, the FBI failed to remove the subject in a timely manner.[13]

This is only the latest in a long string of government reports describing the failure of the terror watch lists.[14] In order to be an effective tool against terrorism these lists must shrink dramatically with names limited to only those for whom there is credible evidence of terrorist ties or activities.

Aviation Screening on the Basis of Nationality

Numerous security experts have already decried the use of race and national origin as an aviation screening technique.

Noted security expert Bruce Schneier stated recently:

> [A]utomatic profiling based on name, nationality, method of ticket purchase, and so on...makes us all less safe. The problem with automatic profiling is that it doesn't work.

---

[13] *DOJ OIG* Audit Report 09-25, pg iv-v. http://www.justice.gov/oig/reports/FBI/a0925/final.pdf

[14] *Review of the Terrorist Screening Center (Redacted for Public Release)*, Justice Department, Office of the Inspector General, Audit Report 05-27, June 2005; *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program (Redacted for Public Release)*, Justice Department, Office of the Inspector General, Audit Report 05-34, August 2005; *Follow-Up Audit of the Terrorist Screening Center (Redacted for Public Release)*, Justice Department, Office of the Inspector General, Audit Report 07-41, September 2007; *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Justice Department, Office of the Inspector General, Audit Report 09-25, May 2009; *DHS Challenges in Consolidating Terrorist Watch List Information*, Department of Homeland Security, Office of Inspector General, OIG-04-31, August 2004; *Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO Report to Congressional Requesters, GAO-03-322, April 2003; *Congressional Memo Regarding Technical Flaws in the Terrorist Watch List*, House Committee on Science and Technology, August 2008.

Terrorists can figure out how to beat any profiling system.

Terrorists don't fit a profile and cannot be plucked out of crowds by computers. They're European, Asian, African, Hispanic, and Middle Eastern, male and female, young and old. Umar Farouk Abdul Mutallab was Nigerian. Richard Reid, the shoe bomber, was British with a Jamaican father. Germaine Lindsay, one of the 7/7 London bombers, was Afro-Caribbean. Dirty bomb suspect Jose Padilla was Hispanic-American. The 2002 Bali terrorists were Indonesian. Timothy McVeigh was a white American. So was the Unabomber. The Chechen terrorists who blew up two Russian planes in 2004 were female. Palestinian terrorists routinely recruit "clean" suicide bombers, and have used unsuspecting Westerners as bomb carriers.

Without an accurate profile, the system can be statistically demonstrated to be no more effective than random screening.

And, even worse, profiling creates two paths through security: one with less scrutiny and one with more. And once you do that, you invite the terrorists to take the path with less scrutiny. That is, a terrorist group can safely probe any profiling system and figure out how to beat the profile. And once they do, they're going to get through airport security with the minimum level of screening every time.[15]

Schneier is not alone in this assessment. Philip Baum is the managing director of an aviation security company:

Effective profiling is based on the analysis of the appearance and behavior of a passenger and an inspection of the traveler's itinerary and passport; it does not and should not be based on race, religion, nationality or color of skin. ...

Equally, the decision to focus on nationals of certain countries is flawed and backward. Perhaps I, as a British citizen, should be screened more intensely given that Richard Reid (a.k.a "the Shoebomber") was a U.K. passport holder and my guess is there are plenty more radicalized Muslims carrying similar passports. Has America forgotten the likes of Timothy McVeigh? It only takes one bad egg and they exist in every country of the world. [16]

Former Israeli airport security director Rafi Ron:

My experience at Ben Gurion Airport in Tel Aviv has led me to the conclusion that racial profiling is not effective. The major attacks at Ben Gurion Airport were carried out by Japanese terrorists in 1972 and Germans in the 1980s. [They] did not belong to

[15] http://roomfordebate.blogs.nytimes.com/2010/01/04/will-profiling-make-a-difference/
[16] *Id.*

any expected ethnic group. Richard Reid [known as the shoe bomber] did not fit a racial profile. Professionally as well as legally, I oppose the idea of racial profiling.[17]

This should be the end of the discussions. Policies that don't work have no place in aviation security. When they are actively harmful - wasting resources and making us less safe - they should be stopped as quickly as possible.

## III. The Impact on Privacy and Civil Liberties Must be Weighed in Any Assessment of Aviation Security Techniques

Each of the three aviation security provisions discussed in these remarks represents a direct attack on fundamental American values. As such they raise serious civil liberties concerns.

Whole Body Imaging

WBI technology involves a striking and direct invasion of privacy. It produces strikingly graphic images of passengers' bodies, essentially taking a naked picture of air passengers as they pass through security checkpoints. It is a virtual strip search that reveals not only our private body parts, but also intimate medical details like colostomy bags. Many people who wear adult diapers feel they will be humiliated. That degree of examination amounts to a significant assault on the essential dignity of passengers. Some people do not mind being viewed naked but many do and they have a right to have their integrity honored.

This technology should not be used as part of a routine screening procedure, but only when the facts and circumstances suggest that it is the most effective method for a particular individual. And such technology may be used in place of an intrusive search, such as a strip search – when there is reasonable suspicion sufficient to support such a search.

TSA is also touting privacy safeguards including blurring of faces, the non-retention of images, and the viewing of images only by screeners in a separate room. Scanners with such protections are certainly better than those without; however, we are still skeptical of their suggested safeguards such as obscuring faces and not retaining images.

Obscuring faces is just a software fix that can be undone as easily as it is applied. And obscuring faces does not hide the fact that rest of the body will be vividly displayed. A policy of not retaining images is a protection that would certainly be a vital step for such a potentially invasive system, but it is hard to see how this would be achieved in practice. TSA would almost certainly have to create exceptions – for collecting evidence of a crime or for evaluation of the system (such as in the event of another attack) for example – and it is a short step from there to these images appearing on the Internet.

[17] Katherine Walsh, *Behavior Pattern Recognition and Why Racial Profiling Doesn't Work*, CSO Online, (Feb. 1, 2006), at: http://www.csoonline.com/article/220787/Behavior_Pattern_Recognition_and_Why_Racial_Profiling_Doesn_t_Work

Intrusive technologies are often introduced very gingerly with all manner of safeguards and protections, but once the technology is accepted the protections are stripped away. There are substantial reasons for skepticism regarding TSA promised protections for WBI devices. In order for these protections to be credible Congress must enshrine them in law.

Finally, the TSA should invest in developing other detection systems that are less invasive, less costly and less damaging to privacy. For example, "trace portal detection" particle detectors hold the promise of detecting explosives while posing little challenge to flyers' privacy. A 2002 Homeland Security report urged the "immediate deployment" of relatively inexpensive explosive trace detectors in European airports, as did a 2005 report to Congress, yet according to a 2006 Associated Press article, these efforts "were frustrated inside Homeland Security by 'bureaucratic games, a lack of strategic goals and months-long delays in distributing money Congress had already approved."[18] Bureaucratic delay and mismanagement should not be allowed to thwart the development of more effective explosive detection technologies that do not have the negative privacy impact of WBI devices.

Watch Lists

The creation of terrorist watch lists – literally labeling individuals as a terrorist – has enormous civil liberties impact. It means ongoing and repetitive harassment at all airports – foreign and domestic, constant extra screening, searches and invasive questions. For the many innocent individuals on the lists this is humiliating and infuriating.

For some it is worse. Individuals on the no fly list are denied a fundamental right, the right to travel and move about the country freely. Others are threatened with the loss of their job. Erich Sherfen, commercial airline pilot and Gulf War veteran, has been threatened with termination from his job as a pilot because his name appears on a government watch list, which prevents him from entering the cockpit.[19] Sherfen is not the only innocent person placed on a terror watch list. Others individual who are either on a list or mistaken for those on the list include a former Assistant Attorney General, many individuals with the name Robert Johnson, the late Senator Edward Kennedy and even Nelson Mandela.[20]

The most recent case – revealed just last week – is that of Mikey Hicks, an 8 year old boy who has been on the selectee list seemingly since birth. According to Hicks' family their travel tribulations that began when Mikey was an infant. When he was 2 years old, the kid was patted down at airport security. He's now, by all accounts, an unassuming bespectacled Boy Scout who has been stopped every time he flies with his family.[21]

---

[18] John Solomon, *Bureaucracy Impedes Bomb Detection Work*, Washington Post, Aug. 12, 2006, at: http://www.washingtonpost.com/wp-dyn/content/article/2006/08/12/AR2006081200269.html

[19] Jeanne Meserve, *Name on government watch list threatens pilot's career*, CNN.com, August 22, 2008, http://www.cnn.com/2008/US/08/22/pilot.watch.list/index.html?iref=newssearch

[20] For details on these individuals and many other please see: http://www.aclu.org/technology-and-liberty/unlikely-suspects

[21] Lizette Alvarez, *Meet Mikey, 8: U.S. Has Him on Watch List*, New York Times, January 13, 2010.

In addition, to stops at the airport watch list information is also placed in the National Criminal Information Center database. That means law enforcement routinely run names against the watch lists for matters as mundane as traffic stops. It's clear that innocent individuals may be harassed even if they don't attempt to fly.

Nor is there any due process for removing individuals from the list – there is simply no process for challenging the government's contention that you are a terrorist. Even people who are mistaken for those on the list face challenges. A September 2009 report by the Inspector General of the Department of Homeland Security found that the process for clearing innocent travelers from the list is a complete mess.[22]

In light of the significant and ongoing harm to innocent Americans as well as the harm to our national security caused by the diversion of security resources these watch lists must be substantial reduced in size and fundamental due process protections imposed. Innocent travelers must be able to remove themselves from the list both for their sake and the sake of national security.

Aviation Screening on the Basis of Nationality

This history of the civil rights movement in the 20th and 21st Century is a long, compelling rejection of the idea that individuals should be treated differently on the basis of their race or nation of origin. Because of that, the administration's decision to subject the citizens of fourteen nations flying to the United States to intensified screening is deeply troubling. Longstanding constitutional principles require that no administrative searches, either by technique or technology, be applied in a discriminatory matter. The ACLU opposes the categorical use of profiles based on race, religion, ethnicity, or country of origin. This practice is nothing less than racial profiling. Such profiling is ineffective and counter to American values.

But the harm that profiling on the basis of national origin does to civil liberties is not an abstraction – it also has direct impact on American security interests. These harmful policies have a direct impact on the Muslim and Arab communities. The Senate Homeland Security and Government Affairs committee has heard testimony from several witnesses who cited the growth of Islamophobia and the polarization of the Muslim community as risk factors that could raise the potential for extremist violence.[23] Unfairly focusing suspicion on a vulnerable community tends to create the very alienation and danger that we need to avoid.

---

[22] *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program, Department of Homeland Security*, Office of the Inspector General OIG 09-10, September 2009. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf

[23] *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program, Department of Homeland Security*, Office of the Inspector General OIG 09-10, September 2009. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf

[23] *See for example*, Hearing of the Senate Homeland Security and Governmental Affairs Committee, *Violent Islamist Extremism: The European Experience*, (June 27, 2007), particularly the testimony of Lidewijde Ongering and Marc Sageman, available at: http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=9c8ef805-75c8-48c2-810d-d778af31cca6.

Indeed a recent United Kingdom analysis based on hundreds of case studies of individuals involved in terrorism reportedly identified "facing marginalization and racism" as a key vulnerability that could tend to make an individual receptive to extremist ideology.[24] The conclusion supporting tolerance of diversity and protection of civil liberties was echoed in a National Counterterrorism Center (NCTC) paper published in August 2008. In exploring why there was less violent homegrown extremism in the U.S. than the U.K., the authors cited the diversity of American communities and the greater protection of civil rights as key factors.

At the January 7, 2009 White House briefing regarding the security failures surrounding the Christmas attack, DHS Secretary Janet Napolitano raised a question about "counter-radicalization."[25] She asked, "How do we communicate better American values and so forth, in this country but also around the globe?" Of course the Secretary should know American values are communicated through U.S. government policies, which is why adopting openly discriminatory policies can be so damaging and counterproductive to our national interests.

## IV. Conclusion

Ultimately security is never absolute and never will be. It is not wise security policy to spend heavily to protect against one particular type of plot, when the number of terrorist ideas that can be hatched – not only against airlines, but also against other targets – is limitless. The President has identified a failure "connect the dots" by intelligence analysts as the main reason that Umar Farouk Abdulmutallab was able to board a flight to the U.S.[26] We must not lose sight of that reality. Limited security dollars should be invested where they will do the most good and have the best chance of thwarting attacks. That means investing them in developing competent intelligence and law enforcement agencies that will identify specific individuals who represent a danger to air travel and arrest them or deny them a visa.

Invasive screening mechanisms, enlarging already bloated watch lists, targeting on the basis of national origin – none of these approaches go to the heart of what went wrong on Christmas day. Instead they are a dangerous sideshow – one that harms our civil liberties and ultimately makes us less safe.

---

[24] Alan Travis, "*MI5 Report Challenges Views on Terrorism in Britain*," The Guardian, (August 20, 2008) *at:* http://www.guardian.co.uk/uk/2008/aug/20/ukscurity.terrorism1 *and;* Alan Travis, "*The Making of an Extremist*," The Guardian (Aug. 20, 2008) *at:* http://www.guardian.co.uk/uk/2008/aug/20/ukscurity.terrorism

[24] National Counterterrorism Center Conference Report, Towards a Domestic Counterradicalization Strategy, (August 2008)

[25] Briefing by Homeland Security Secretary Napolitano, Assistant to the President for Counterterrorism and Homeland Security Brennan, and Press Secretary Gibbs, 1/7/10, at: http://www.whitehouse.gov/the-press-office/briefing-homeland-security-secretary-napolitano-assistant-president-counterterroris

[26] Jake Tapper and Sunlen Miller, *Obama: Intelligence Community Failed to "Connect the Dots" in a "Potentially Disastrous Way"*, ABCNews.com, January 05, 2010. http://blogs.abcnews.com/politicalpunch/2010/01/obama-intelligence-community-failed-to-connect-the-dots-in-a-potentially-disastrous-way.html

# Testimony of
# Kate Martin, Director
# Center for National Security Studies

## For the United States Senate
## Committee on the Judiciary

## "Securing America's Safety:
## Improving the Effectiveness of Anti-Terrorism Tools and
## Inter-Agency Communication"

## January 20, 2010

Chairman Leahy, Ranking Member Sessions, and Members of the Committee, thank you for the opportunity to submit this testimony as part of the record for your hearing on "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication." We appreciate the Committee's careful review and consideration of these issues and the opportunity to offer our views for the Committee's consideration.

The Center is the only non-profit organization whose core mission is to prevent claims of national security from being used to erode civil liberties, human rights, or constitutional procedures. The Center works to preserve basic due process rights, protect the right of political dissent, prevent illegal government surveillance, strengthen the public's right of access to government information, combat excessive government secrecy, and assure effective oversight of intelligence agencies. It works to develop a consensus on policies that fulfill national security responsibilities in ways that do not interfere with civil liberties or constitutional government.

I would like to first offer a few observations as a twenty-year student of the intelligence community regarding the terrible events of the past months, including the shooting at Fort Hood and the attempted destruction of the Detroit–bound plane and murder of its passengers. It is a truism, but bears keeping in mind, that obtaining good intelligence, i.e. information that is reliable enough to be acted upon, is very difficult and can entail great risk. There is no more terrible reminder of this than the killings in Khost of U.S. intelligence officers by an individual mistakenly believed to be trustworthy.

Accordingly, the recent articulation and understanding by those in the government that intelligence alone cannot be the mainstay of the effort to defeat al Qaeda is welcome. Defeating al Qaeda and protecting people from their murderous attacks requires a broader strategy than one which, relying on intelligence, aims simply to capture or kill all terrorists without addressing the conditions that allow them to operate. Instead, the security consensus now recognizes that a much more comprehensive approach is needed, one which will also work to drain support for terrorist groups and dissuade young men from becoming suicide bombers. As explained by the President's advisor for counterterrorism, John Brennan, the administration has determined to:

> integrat[e] every element of American power to ensure that ... "upstream" factors discourage rather than encourage violent extremism. After all, the most effective long-term strategy for safeguarding the American people is one that promotes a future where a young man or woman never even considers joining an extremist group in the first place; where they reject out of hand the idea of picking up that gun or strapping on that suicide vest; where they have faith in the political process and confidence in the rule of law; where they realize that they can build, not simply destroy—and that the United States is a real partner in opportunity, prosperity, dignity, and peace. That is why President Obama is committed to using every element of our national power to address the underlying causes and conditions that fuel so many national security threats, including violent

extremism. We will take a multidimensional, multi-departmental, multi-national approach.[1]

I want to note that one element of such a comprehensive approach was evident in the President's measured response to the Christmas day attack, which was not the fearful reaction that al Qaeda, like all terrorists, must have been hoping for.

This larger context is essential for looking at the questions being considered by the Committee today and in the future: whether the shooting at Fort Hood could have been prevented; what additional measures could have been taken to prevent the Christmas day attack; and whether it is realistic to expect that such attacks can be successfully defeated one hundred percent of the time.

In answering these questions, lessons drawn by military commanders in the counterinsurgency context are useful. Just as U.S. commanders in Afghanistan recognize that decisions about the use of force there must consider the collateral long-term consequences for U.S. strategic objectives beyond the immediate military objectives, so should decisions about the uses of secret intelligence methods consider more than simply their short-term efficacy in identifying and stopping a terrorist. Disabling individual terrorists is obviously extremely important. At the same time, recent history has demonstrated the importance of also considering the longer-term effect of using specific intelligence methods on the strategic goals of defeating the terrorist narrative and stopping terrorist attacks; preserving our constitutional government; and building a more democratic, peaceful and just world.

The recent calls for "racial profiling" of all young Muslim men, for secret imprisonment and interrogation of the Christmas Day plotter, or for more surveillance authorities to collect information on Americans all ignore both the specific security gaps disclosed by these incidents and the larger context of what is necessary to defeat al Qaeda. For example, the calls to extend the "lone wolf" authorities for secret wiretaps on non-U.S. persons to citizens and other U.S. persons ignore both constitutional requirements and the facts. If there had been probable cause to obtain a secret intelligence warrant to wiretap the Ft. Hood shooter under the "lone wolf" standard, it is extremely likely that there was probable cause to obtain a criminal warrant to wiretap him. Indeed, it appears that the intelligence community was in fact not only aware of his communications with an extremist cleric in Yemen, they may well have been listening to them. It is not clear, however, that the community was tracking his gun purchases, a potentially more fruitful kind of surveillance. The calls for racial profiling and resurrection of the discredited practice of secretly imprisoning and interrogating suspects – an effort perhaps to defend and justify past practices – overlook the general consensus among security, military and intelligence experts that such practices overall harmed rather than strengthened U.S. national security. Those practices strained relationships

[1] Brennan, John. Remarks as prepared for delivery "A New Approach to Safeguarding Americans" at the Center for Strategic and International Studies, August 6, 2009. Available at: http://www.whitehouse.gov/the_press_office/Remarks-by-John-Brennan-at-the-Center-for-Strategic-and-International-Studies/.

with necessary partners around the world and supplied fodder to the terrorists' false narrative about the United States used to recruit an unending stream of fighters and potential suicide bombers.

Instead the administration and this committee are more usefully focused on the intelligence community's failure to "connect the dots" about the Christmas bomber, despite having adequate raw intelligence about the plot.[2] In doing so, it is crucial to recognize that the volume of information coming into the U.S. government intelligence agencies either passively through volunteers like the father or through active collection – for example by the electronic surveillance programs run by the National Security Agency or the FBI's use of national security letter and other authorities – makes it extremely difficult to correlate items of information and produce actionable intelligence analysis. As John Brennan has stated:

> All the information was shared. Except that there are millions upon millions of bits of data that come in on a regular basis. What we need to do is make sure the system is robust enough that we can bring that information to the surface that really is a threat concern.[3]

Conservative commentator George Will agreed:

> When you have millions of dots, you cannot define as systemic failure—catastrophic failure—anything short of perfection. Our various intelligence agencies suggest 1,600 names *a day* to be put on the terrorist watch list. He is a known extremist, as the president said. There are millions of them out there. We can't have perfection here.[4]

Those of us worried about the lack of civil liberties safeguards in the recent changes to surveillance laws have long urged Congress to focus on these issues, rather than simply increasing collection authorities and mandating sharing. Several years ago, in the context of consideration of reauthorization and amendment of surveillance provisions, I wrote that while effective counterterrorism requires that agencies share relevant information, simply mandating sharing fails to address the real difficulties in such sharing. These include: "How to determine what information is useful for counterterrorism; how to determine what information would be useful if shared; how to identify whom it would be useful to share it with; and **how to ensure that useful and relevant information is timely recognized and acted upon.**"[5] While the legislative focus and much of the administration's public commentary in the past eight years may be

---

[2] See Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack. Available at: www.whitehouse.gov.

[3] Interview with Terry Moran on ABC's "This Week," January 3, 2010. Available at: http://abcnews.go.com/ThisWeek/week-transcript-john-brennan-reps-hoekstra-harman-sens/story?id=9467566.

[4] Id.

[5] See Kate Martin writing in 2005 on sections 203 and 905 on Patriot debates.com, for one instance of this analysis. Available at: http://www.abanet.org/natsecurity/patriotdebates/section-203.

summarized as share everything with everyone, that articulation is likely to have obscured and thus increased the difficulties in the real challenges of information sharing.

Much of the recent press commentary is still focused on whether particular individuals had access to or responsibility for the various bits of information relevant in hind sight to the Christmas day plot and failed to put them together. It appears, however, that the government is now addressing this more difficult question, by aiming to increase government capacity to electronically collate and analyze intelligence bits of information to determine what is in fact significant enough to require attention by a human analyst to determine if the information should be acted on.[6] (e.g., the DNI is to "accelerate information technology enhancements, to include knowledge discovery, database inteegration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.")

Such an approach may well necessary to identify and prevent future terrorist plots and could also be useful for other intelligence tasks, such as cybersecurity efforts. At the same time, such automated analysis, frequently called data mining, raises significant constitutional and privacy concerns. Building such capacities pose challenges to civil liberties that go far beyond the risks of individual wrongdoing and misuse of personal information, such as identity theft or illegal uses of personal information by government officials. Rather, they pose challenges to the balance of power between the government and the citizens. As Senator Sam Ervin explained in 1974:

> [D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.
>
> Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.[7]

Senator Ervin's fears become even more relevant as the government develops automated electronic intelligence capabilities to mine the vast amounts of information

---

[6] See Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack, January 7, 2010. Available at: http://www.whitehouse.gov/sites/default/files/potus_directive_corrective_actions_1-7-10.pdf.

[7] Senator Ervin, June 11, 1974, *reprinted in* COMMITTEE ON GOVERNMENT OPERATIONS, UNITED STATES SENATE AND THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S.3418, at 157 (Public Law 93-579)(Sept. 1976).

electronically collected and stored on individuals. Accordingly, in order to best protect our constitutional framework and meet national security threats, including terrorism, we recommend the following guidelines be implemented in adopting or upgrading such capabilities.

- Any consideration of such initiatives should include specific identification and consideration of alternative solutions to meet the security objectives. Policy-makers should direct a preference for the solution which is most protective of civil liberties and most transparent consistent with appropriate risk-management objectives;
- The Privacy and Civil Liberties Oversight Board should be stood up and provided the wherewithal to review and contribute to such an approach; and
- Any such initiatives should include a comprehensive review of existing legal protections for Americans' personally identifiable information, especially private communications, with the objective of identifying and adopting greater protections while still meeting security needs.

An in depth discussion of how to do this is beyond the scope of this hearing. But I want to take this opportunity to outline a general approach that has the potential for increasing both the analytical capabilities of the government and privacy protections for Americans. In building automated analysis/data-mining capabilities that could be used on Americans' personally identifiable information, the government should be directed to consider the feasibility of requiring such capability to use anonymized data. Such an approach would require technological anonymization of personally identifiable information accessible to the government on networks. Doing so would permit the adoption of safeguards, including judicial oversight, when such analysis generates the identities of Americans as suspects. Judicial approval could be required before the data could be deanonymized in order to identify specific Americans as suspects.

For example, when the government has access to streams of network data containing personally identifiable information on citizens and persons inside the United States, the network could be required to carry such data in a way that personal identifiers may be electronically and automatically separated from the rest of the data, in effect anonymizing the stream of data. While the government would be entitled to access such anonymized transactional (non-content) data without a warrant and to analyze such data, it would then be required to make a showing to a court in order to pierce the anonymity and obtain the personal identifiers of Americans associated with the transactional data. For example, the government could be authorized to access the personal identifiers for such data only if it met statutorily mandated standards, e.g., a judicial warrant based on probable cause.

Finally, the President's direction to his Intelligence Advisory Board "to look at broader analytic and intelligence issues associated with this incident, including how to meet the challenge associated with exploiting the ever-increasing volume of information available to the Intelligence Community" should be implemented in a manner such that:

- There is public/congressional knowledge of and input concerning the use of such technologies to analyze and flag information about Americans; and
- There is a commitment to build in more privacy protections in the technical design of software/hardware capabilities and in the legal authorities for such systems.

These are obviously difficult, large and complex undertakings, important both to the efforts to protect Americans from terrorist attacks and to preserve our constitutional framework. I thank the Committee for providing me the opportunity to participate in this important work.

# Department of Justice

STATEMENT OF
ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"SECURING AMERICA'S SAFETY: IMPROVING THE EFFECTIVENESS OF
ANTI-TERRORISM TOOLS AND INTER-AGENCY COMMUNICATION"

PRESENTED
JANUARY 20, 2010

**Robert S. Mueller, III**
**Director**
**Federal Bureau of Investigation**
**before the**
**Committee on the Judiciary**
**United States Senate**
**January 20, 2010**

**"Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"**

## I. Introduction

Good morning Chairman Leahy, Senator Sessions, and members of the Committee. I am pleased to be here today.

As you know, we in the FBI have undergone unprecedented transformation in recent years, from developing the intelligence capabilities necessary to address emerging terrorist and criminal threats, to creating the administrative and technological structure to meet our mission as a national security service.

We have worked to become a full partner in the Intelligence Community. With that comes the responsibility to ensure that we consistently collect, analyze, and disseminate intelligence to those who need it, from our Federal partners in the Central Intelligence Agency (CIA), the National Counterterrorism Center (NCTC), the Office of the Director of National Intelligence (ODNI), and the Department of Homeland Security (DHS), among others, to our international, State, local, and tribal counterparts. As I have often said, today we share information by rule, and withhold by exception.

As recent events indicate, terrorists remain determined to strike the United States. We are particularly concerned about individuals who may be radicalized overseas, both those who live in America and those who live overseas and who may one day return to the United States to

perpetrate terrorist attacks. We in the FBI, with our partners in the Intelligence Community, must do everything possible to ensure that does not happen. This will require constant vigilance on the FBI's part, and on the part of every member of the IC. It will require the best and highest use of the intelligence we collect, both individually and as a group.

**II. The Changing Terrorist Threat**

I want to focus first on the changing terrorist threat.

As the Christmas Day attempted bombing illustrates, the threats we face are becoming more diverse and more dangerous with each passing day. We not only face threats from Al Qaeda, but also from self-directed groups not part of Al Qaeda's formal structure which have ties to terrorist organizations through money or training.

We face threats from homegrown terrorists – those who live in the communities they intend to attack, and who are self-radicalizing, self-training, and self-executing. We face threats from those who may attend training camps overseas – individuals who may live here in the United States, and who may be radicalized here or overseas, and those who may live overseas but plan to travel to the United States to perpetrate attacks.

We also face threats from extremists operating in new sanctuaries around the world. While we disabled Al Qaeda's training and financing mechanisms in Afghanistan in the wake of the September 11th attacks, it is clear that Al Qaeda and its offshoots are rebuilding in Pakistan, Yemen, and the Horn of Africa.

At the same time, we cannot discount the lone offender threat here at home – the individual who may take up arms and strike without notice.

We are using intelligence to identify these potential threats. But the question remains: How do we take the strategic intelligence we possess and turn it into tactical intelligence? In other words, once we have identified a potential threat, how do we determine who might take action, and where and when they may do so? And more importantly, how do we prevent them from doing so?

In recent years, our capacity for intelligence analysis has improved dramatically. But as the saying goes, trying to glean actionable intelligence from the flood of information we receive is akin to taking a sip of water from a fire hose. As I noted above, the challenge for all members of the IC is to find links between disparate pieces of information – to use the intelligence we possess, individually and collectively – to form a clear picture about the intentions of our adversaries.

### III. Recent Counterterrorism Disruptions

As illustrated by recent events, the terrorist threat has not diminished. But through enhanced intelligence, improved technology, and strong partnerships, we have been able to disrupt several terrorist threats and plots this year.

For example, on December 14, 2009, in Georgia, Ehsanul Islam Sadequee was sentenced to 17 years in prison on charges of material support to terrorists. Syed Harris Ahmed was sentenced to 13 years on similar charges. These individuals conducted surveillance of potential targets in Washington, D.C., and pursued terrorist training overseas. They were part of an online network that connected extremists in North America, Europe, and South Asia.

This past October, in Chicago, U.S. citizen David Headley was arrested for planning terrorist attacks against a Danish newspaper and two of its employees. Headley is alleged to have conducted extensive surveillance of targets in Mumbai for more than two years preceding the November 2008 attack there. Headley is also alleged to have attended terrorist training camps in Pakistan. On January 14, 2010, a superseding indictment was filed against Headley relating to his conspiring with others to plan and execute attacks in both Denmark and India.

In October 2009, in Massachusetts, members of the FBI's Joint Terrorism Task Force arrested Tarek Mehanna on charges of conspiracy to provide material support to terrorists. Federal officials charge that Mehanna and other conspirators discussed their desire to participate in violent jihad against America, including a plot to use automatic weapons to open fire on shoppers and emergency responders at shopping malls in Boston.

In Minnesota, 14 individuals have been charged in recent months as part of an ongoing investigation into the recruitment of persons from U.S. communities to train with or fight on behalf of extremist groups in Somalia. Four defendants have pled guilty and await sentencing. Charges include providing financial support to those who traveled to Somalia to fight on behalf of al Shabaab, attending terrorist training camps operated by al Shabaab, and fighting on behalf of al Shabaab.

In September 2009, Colorado resident Najibullah Zazi was arrested in New York and was charged with conspiracy to use weapons of mass destruction (explosives) in the United States. As alleged in the indictment, Zazi had received detailed bomb-making instructions in Pakistan. Zazi allegedly purchased components of improvised explosive devices, and had traveled to New York City on September 10, 2009, in furtherance of his criminal plans.

Also in September of last year, in Illinois, FBI Special Agents arrested Michael C. Finton on charges of attempted murder of Federal employees and attempted use of a weapon of mass destruction (explosives) in connection with a plot to detonate a vehicle bomb at a Federal building in Springfield. In his efforts to carry out the plot, Finton communicated with undercover FBI agents and confidential sources that continuously monitored his activities up to the time of his arrest. According to the complaint, Finton also drove a vehicle containing inactive explosives to the Federal courthouse in Springfield and attempted to detonate them.

That same month, in Texas, Hosam Smadi was charged with attempting to use a weapon of mass destruction. Smadi, who was under continuous surveillance by the FBI, was arrested after he placed an inert car bomb near a 60-story office tower in downtown Dallas. As alleged in the indictment, Smadi, a Jordanian citizen in the United States illegally, has repeatedly espoused his desire to commit violent jihad and had been the focus of an undercover FBI investigation.

This past July, in North Carolina, FBI agents arrested an alleged group of homegrown terrorists who were heavily armed and making plans to wage jihad overseas. The seven men arrested – including a father and his two sons – were charged with providing material support to terrorists and conspiring to murder, kidnap, and injure people overseas. The father, Daniel

Patrick Boyd, once fought in Afghanistan, and allegedly trained in terrorist camps in Pakistan and Afghanistan. All of the defendants but one are U.S. citizens.

And last May, in New York, four individuals were arrested on charges of conspiracy to use weapons of mass destruction in the United States and conspiracy to acquire and use anti-aircraft missiles. The group allegedly plotted to blow up a Jewish synagogue in the Bronx and to shoot down military planes at the New York Air National Guard Base. As alleged in the indictment, they obtained what they believed to be three improvised explosive devices and a Stinger surface-to-air guided missile from a source who was in fact an FBI informant.

This is merely a sampling of the investigations we have handled over the past year. In each investigation, the resources and the investigative experience of our Federal, State, and local law enforcement and intelligence counterparts proved invaluable. Indeed, we in the FBI could not do our jobs without their critical assistance and their expertise.

**IV. December 25, 2009 Attack**

On January 6, 2010, Umar Farouk Abdulmutallab, a 23-year-old Nigerian national, was charged in a six-count criminal indictment for his alleged role in the attempted Christmas day bombing of Northwest Airlines flight 253 from Amsterdam, the Netherlands, to Detroit.

Abdulmutallab has been charged with attempted use of a weapon of mass destruction, attempted murder within the special aircraft jurisdiction of the United States, willful attempt to destroy an aircraft, willfully placing a destructive device on an aircraft, use of a firearm or destructive device during and in relation to a crime of violence, and possession of a firearm or destructive device in furtherance of a crime of violence.

According to the indictment, Northwest Airlines flight 253 carried 279 passengers and 11 crew members. Abdulmutallab allegedly boarded Northwest Airlines flight 253 in Amsterdam on December 24, 2009, carrying a concealed bomb. The bomb components included Pentaerythritol (also known as PETN, a high explosive) and Triacetone Triperoxide (also known as TATP, a high explosive), and other ingredients.

The bomb was concealed in the defendant's underclothing and was designed to allow him to detonate it at a time of his choosing, thereby causing an explosion aboard flight 253, according to the indictment. Shortly prior to landing at Detroit Metropolitan Airport, on December 25, 2009, Abdulmutallab allegedly detonated the bomb, causing a fire on board the plane.

According to an affidavit filed in support of the criminal complaint, Abdulmutallab was subdued and restrained by passengers and the flight crew after allegedly detonating the bomb. The airplane landed shortly thereafter, whereupon U.S. Customs and Border Protection officers took him into custody.

The FBI is responsible for investigating this incident. FBI Special Agents interviewed Abdulmutallab following the attack, and have shared all relevant information with our partners in the IC. We will continue to investigate Abdulmutallab and all individuals connected to him, and we will continue to share all relevant information with our law enforcement and intelligence counterparts. However, because this is an ongoing investigation, we cannot divulge many details at this juncture.

**V. Terrorist Watchlisting Procedures**

I would like to turn for a moment to terrorist watchlisting procedures and the Terrorist Screening Center ("TSC")

The TSC is a multi-agency center that connects the law enforcement communities with the IC by consolidating information about known and suspected terrorists into a single Terrorist Watchlist. The TSC facilitates terrorist screening operations, helps coordinate the law enforcement responses to terrorist encounters developed during the screening process, and captures intelligence information resulting from screening.

The TSC integrates the law enforcement and intelligence communities by consolidating terrorist information. The current terrorist watchlisting and screening enterprise is a collaborative effort between the TSC, the FBI, DHS, the Department of State, the Department of Defense, the NCTC, and other members of the IC.

## VI. Today's FBI

### A. Restructuring of FBI Intelligence Program

To meet our national security mission, we have expanded our counterterrorism operations and honed our intelligence capabilities. We stood up the National Security Branch and the Weapons of Mass Destruction Directorate. We integrated our intelligence program with other agencies under the Director of National Intelligence, with appropriate protections for privacy and civil liberties. We hired hundreds of intelligence analysts, linguists, and surveillance specialists. And we created Field Intelligence Groups in each of our 56 field offices. In short, we improved our national security capabilities across the board.

But we also recognize that we must continue to move forward, to refine programs and policies already in place, and to make necessary changes to our intelligence program.

To that end, we established a Strategic Execution Team, or SET, to help us assess our intelligence program, and to standardize it throughout the Bureau. The SET, made up of agents and analysts, developed a series of recommendations for accelerating the integration of our intelligence and investigative work.

The SET improvements ensure that we capitalize on our intelligence collection capabilities and develop a national collection plan to fill gaps in our knowledge base. Our objective is to defeat national security and criminal threats by operating as a single intelligence-led operation, with no dividing line between our criminal and counterterrorism programs. In short, we want to make sure that nothing falls through the cracks.

To this end, we have restructured the Field Intelligence Groups, or FIGs, in every field office across the country. FIGs are designed to function as the hub of the FBI's intelligence program. They ensure that each field office is able to identify, assess, and attack emerging threats before they flourish.

Following the SET's recommendations, the FIGs now conform to one model, based on best practices from the field, and adapted to the size and complexity of each office. Each FIG

has well-defined requirements for intelligence gathering, analysis, use, and production. And managers are accountable for ensuring that intelligence production is of high quality and relevant not only to their own communities, but to the larger intelligence and law enforcement communities.

As a result of these changes, the FIGs can better coordinate with each other and with Headquarters. They can better coordinate with law enforcement and intelligence partners, and the communities they serve. With this integrated model, we can turn information and intelligence into knowledge and action, from coast to coast.

These changes are part and parcel of our ongoing campaign to "Know Our Domain," as we say. Domain awareness is a 360-degree understanding of all national security and criminal threats in any given city, community, or region. It is the aggregation of intelligence, to include what we already know and what we need to know, and the development of collection plans to find the best means to answer the unknowns. With this knowledge, we can identify emerging threats, allocate resources effectively, and identify new opportunities for intelligence collection and criminal prosecution.

We have implemented SET concepts at FBI Headquarters, to improve strategic alignment between the operational divisions and the Directorate of Intelligence. We want to better manage national collection requirements and plans, and ensure that intelligence from our Field Offices is integrated and shared with those who need it at FBI Headquarters and in the larger Intelligence Community.

We will continue to refine not only the manner in which we collect and share information, but the manner in which we analyze that information, to find links between people, cases, and countries.

**B. Improvements to FBI Technology**

We have also made a number of improvements to the FBI's information technology systems. We cannot gather the intelligence we need, analyze that intelligence, or share it with our law enforcement or intelligence partners, without the right technology.

As you know, we continue to implement Sentinel, our web-based case management system, which makes it faster and easier to access and connect information from office to office, from case to case, and from program to program.

We are also strengthening the IT programs that allow us to communicate and share with our partners. For example, we are consolidating the FBI's Unclassified Network with Law Enforcement Online, or LEO, which is the unclassified secure network we use to share information with registered law enforcement partners. This will provide a single platform that allows FBI employees to communicate and share with their internal and external partners. Currently, LEO provides a secure communications link to all levels of law enforcement and is available to more than 18,000 law enforcement agencies.

As part of the LEO platform, the FBI is delivering the eGuardian system – an unclassified counterterrorism tool available to our Federal, State, local, and tribal law enforcement partners through the FBI's secure LEO internet portal. eGuardian makes threat and suspicious activity information immediately available to all authorized users. The eGuardian system will work in tandem with Guardian, enabling law enforcement personnel to receive the most current information. In return, any potential terrorist threat or suspicious activity information provided by law enforcement will be made available in Guardian entries and pushed outward to the FBI task forces.

We are also in the midst of developing what we call "Next Generation Identification" system, which expands the FBI's fingerprint-based identification, known as IAFIS, to include additional biometric data. This will better enable us to find criminals and terrorists who are using the latest technology to shield their identities and activities.

We are also working to improve our confidential human source management system. Intelligence provided by confidential human sources is fundamental to the FBI mission. To better manage that data, we have implemented a program known as DELTA. DELTA will provide FBI agents and intelligence analysts a uniform means of handling the administrative aspect of maintaining human sources. It will also enable FBI Headquarters and Field Offices to better understand, connect, operate, and protect confidential human sources.

Finally, we are improving our crisis management systems. The Operational Response and Investigative Online Network (ORION) is the FBI's next-generation Crisis Information Management System. ORION provides crisis management services to Federal, State, local, and tribal law enforcement and/or emergency personnel. It standardizes crisis and event management processes, enhances situational awareness, and supports the exchange of information with other command posts.

The ORION application is accessible from almost any desktop with FBINET or UNET connectivity using a standard web browser, or by other secure connections providing access to Federal, State and local law enforcement partners It has been used at both the Democratic and Republican national conventions, major sporting events, to include the Olympics, and last year's Presidential Inauguration.

These improvements are necessary for the work ahead of us, and we will continue to develop and implement the necessary tools to combat today's diverse, dangerous, and global threats together with our partners in the law enforcement and intelligence communities.

**VII. Conclusion**

Over the past 100 years, the FBI has earned a reputation for protecting America that remains unmatched. Many of our accomplishments over the past eight years are in part due to your efforts and your support, and much of our success in the years to come will be due to your continuing support. From protecting the American people from terrorist attack to addressing the growing gang problem to creating additional Legal Attaché offices around the world, you have supported our mission and our budget requests.

Mr. Chairman, I would like to conclude by thanking you and this Committee for your service and your support. On behalf of the men and women of the FBI, I look forward to working with you in the years to come. I would be happy to answer any questions you may have.

# # #

Schneier: Fixing Airport Security

In the headlong rush to "fix" security after the Underwear Bomber's unsuccessful Christmas day attack, there's far too little discussion about what worked and what didn't, and what will and will not make us safer in the future.

The security checkpoints worked. Because we screen for obvious bombs, Abdulmutallab -- or, more precisely, whoever built the bomb -- had to construct a far less reliable bomb than he would have otherwise. Instead of using a timer or a plunger or a reliable detonation mechanism, as would any commercial user of PETN, he had to resort to an ad hoc homebrew, and much more inefficient, mechanism: one involving a syringe and twenty minutes in the lavatory and we don't know exactly what else. And it didn't work.

Yes, the Amsterdam screeners allowed Abdulmutallab onto the plane with PETN sewn into his underwear, but that's not a failure either. There is no security checkpoint, run by any government anywhere in the world, designed to catch this. It isn't a new threat -- it's over a decade old -- nor is it unexpected; anyone who says otherwise simply isn't paying attention. But PETN is hard to explode, as Richard Reid learned and as we saw on Christmas Day.

Additionally, the passengers on the airplane worked. For years I've said that exactly two things have made us safer since 9/11; reinforcing the cockpit door and convincing passengers that they need to fight back. It was the second of these that, on Christmas Day, quickly subdued Abdulmutallab after he set his pants on fire.

To the extent security failed, it failed before Abdulmutallab even got to the airport. Why was he issued an American Visa? Why didn't anyone follow up on his father's tip? While I'm sure there are things to be improved and fixed, remember that everything is obvious in hindsight. After the fact, it's easy to point to the bits of evidence and claim that someone should have "connected the dots." Some of these bits are just wrong: Abdulmutallab had a round-trip ticket, everyone pays for things in cash in Nigeria, and lots of people fly without any checked baggage. And before the fact, when there millions of dots -- some important but the vast majority unimportant -- uncovering plots is a lot harder.

Despite this, the proposed fixes focus on the details of the plot rather than the broad threat. We're going to install full body scanners, even though there are lots of ways to hide PETN -- stuff it in a body cavity, spread it thin on a garment -- from the machines. We're going to profile people traveling from 14 countries, even though it's easy for a terrorist to travel from a different country. Seating requirements for the last hour of flight were the most ridiculous example.

The problem with all these measures is that they're only effective if we guess the plot correctly. Defending against a particular tactic or target makes sense if tactics and targets are few. But there are hundreds of tactics and millions of targets, so all these measures will do is force the terrorists to make a minor modification to their plot.

It's magical thinking: if we defend against what the terrorists did last time, we'll somehow defend against what they do one time. Of course this doesn't work. We take away guns and bombs, so the terrorists use box cutters. We take away box cutters and corkscrews, and the terrorists hide explosives in their shoes. We screen shoes, they use liquids. We limit liquids, they sew PETN into their underwear. We implement full body scanners, and they're going to do something else. This is a stupid game; we should stop playing it.

But we can't help it. As a species we're hardwired to fear specific stories -- terrorists with PETN underwear, terrorists on subways, terrorists with crop dusters -- and we want to feel secure against those stories. So our political leaders are pressured to do something, even if it makes no sense. We implement security theater against the stories, while ignoring the broad threats.

What we need is security that's effective even if we can't guess the next plot: intelligence, investigation, and emergency response. Our foiling of the liquid bombers demonstrates this. They were arrested in London, before they got to the airport. It didn't matter if they were using liquids -- which they chose precisely because we weren't screening for them -- or solids or powders. It didn't matter if they were targeting airplanes or shopping malls or crowded movie theaters. They were arrested, and the plot was foiled. That's effective security.

Finally, we need to be indomitable. The real security failure on Christmas Day was in our reaction. Terrorism isn't an existential threat against our society. Automobiles kill more people than 9/11 did, each and every month. More people died in Haiti last week than terrorism has killed since the beginning of time. Deaths on airplanes due to terrorism was no greater in this decade than in the 1980s. We're reacting out of fear, wasting money on the story rather than securing ourselves against the threat. Abdulmutallab succeeded in causing terror even though his attack failed. If we refuse to be terrorized, if we refuse to implement security theater and remember that we can never completely eliminate the risk of terrorism, then the terrorists fail even if their attacks succeed.

*Testimony of Suzanne E. Spaulding*

for

U.S. Senate Committee on the Judiciary

# Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication

Wednesday, January 20, 2010

***Effective Counterterrorism Policies: Risk Management, Not Risk Elimination***

Chairman Leahy, Ranking Member Sessions, and Members of the Committee, thank you for the opportunity to submit this testimony as part of the record for your hearing on "Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication." I commend the committee for undertaking this essential oversight to assist in establishing the lessons to be learned from recent terrorism events.

I want to start by expressing my deepest condolences for the family, friends, and colleagues of the courageous intelligence officers who were tragically killed in the attack at Khost, Afghanistan. Some measure of the pain they feel echoes in all of us who care about the mission of intelligence and about the men and women who work so diligently to carry out that mission. I have spent 25 years working in various capacities with the intelligence community and have the utmost respect and gratitude for our intelligence professionals and their unwavering commitment and willingness, when called upon, to take significant personal risks on our behalf.

The CIA is undoubtedly conducting a thorough review of what happened and how it happened, with a strong determination to learn lessons that could strengthen counterintelligence efforts in the future. But they also understand that there is no way to completely eliminate risks to their people or their mission.

The same is true for counterterrorism efforts generally. While the goal is to prevent any future terrorist attack, Americans understand that no one can ever provide a 100% guarantee of safety. We are engaged in an exercise of risk management, not risk elimination. Failure to acknowledge that reality will lead to counterproductive efforts and weaken essential public resiliency.

A risk management approach recognizes the complex interaction between the various aspects of our counterterrorism efforts. It reflects the need for a holistic approach to the array of risks and the tools available for addressing them. In seeking to eliminate all risk in one area, you may be increasing risk in another--or even undermining the very tool you seek to perfect.

I understand that abandoning the myth of risk elimination raises fears of complacency. Effective risk management, however, does not mean settling for less than a full-out effort to understand and protect against the terrorist threat. Lee Hamilton, who co-chaired the 9/11 Commission and is strongly committed to preventing another attack, acknowledged this week "You're never going to produce a system that is completely flawless, and when you're sitting at that computer screen day after day looking... you're going to miss some things.... I think we're a lot better at this than we used to be, but you cannot get this down to zero mistakes...." (http://www.swamppolitics.com/news/politics/blog/2010/01/911_comm_leader_flaws_need_fix.html) This kind of realistic assessment of the risks should lead to better policies and ultimately more effective risk reduction.

***Strengthening Terrorist Databases***

One context in which the contrast between the myth of risk elimination and the value of risk management can be seen is with regard to the various terrorist databases. There are many different terrorism-related databases maintained by the US government. The largest is the Terrorist Identities Datamart Environment (TIDE), compiled and maintained by the National Counterterrorism Center (NCTC) and described on their website as including "all information the government possesses related to individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism." This is primarily for intelligence purposes and the criteria for inclusion are intentionally very broad. According to public reporting, there are about 500,000 names in that database.

A subset of that data is sent to the FBI Terrorist Screening Center (TSC) for inclusion in the U.S. government's consolidated Terrorist Watchlist—a single database of identifying information about those "known or reasonably suspected" of being involved in terrorist activity. This list is notoriously unreliable. It is both under- and over-inclusive. The list includes names that should have been removed because the initial derogatory information was wrong and it fails to include individuals who are on the radar of a government agency, such as the FBI, as reasonably suspected of being involved terrorist activity. (See, e.g., *Report of the Department of Justice Inspector General on FBI's Terrorist Watchlist Nomination Practices*, May 2009.) According to recent testimony by the head of the TSC, Timothy Healy, there are approximately 400,000 names on this watchlist.

The "No Fly" and "Selectee" lists are much smaller subsets of the Terrorist Watchlist. There are approximately 3,400 people on the No Fly list, according to Healy's testimony, and as of October 2008 there were fewer than 16,000 on the Selectee list, according to then-Secretary of DHS Michael Chertoff.

In a bid for risk elimination, some voices have called for expanding the No Fly list to include the entire terrorist watchlist. It seems likely, however, that simply adding nearly half a million names will do more harm than good. Adding more hay to the stack does not help locate the needles. In addition, adding all of these names would undermine the reliability and usefulness of the No Fly list. A hit on the list will quickly become too common to be taken with the level of seriousness necessary for effective implementation.

Nor is it clear from this event that we need to lower the standard or burden of proof for adding a name to these lists. The White House Review Summary appears to indicate that the government had sufficient information on Abdulmutallab to meet the current standard for adding him to the Watchlist list, and even to the No Fly list, if the information had been pulled together.

The President called for an effort to "***strengthen*** the criteria used to add individuals to our watchlists...while still facilitating air travel." (President's Remarks of January 7, 2010, emphasis added.) Instead of lowering the standard or adding hundreds of thousands more names in an effort to eliminate all risk, we must better manage the risk by continually reexamining the criteria for all of these lists to ensure that they reflect current knowledge about the nature of the threat, sources of information, and lessons learned. It may well be that more names need to be added to these lists but it must be done in a way that does not undermine their usefulness.

For example, those evaluating whether to include a name on the watchlist or No Fly list must understand the strategic context in which to view the tactical information they receive. Thus, information that Al Qaeda in the Arabian Peninsula was actively seeking ways to attack the US, along with more specific information reportedly from NSA intercepts of conversations among leaders of Al Qaeda in Yemen discussing a plot to use a Nigerian man for a coming terrorist attack, should have been reflected in the watchlist criteria. Then, when a State Department cable is received indicating possible involvement of a specific named Nigerian with Yemeni extremists, it can be viewed in that context.

Similarly, information from a parent who comes to authorities with concerns that their child may be involved in extremist activities should be given considerably more weight than an anonymous tip conveying the same information. This is not a step a father would take lightly, given the potential risk not only for his son but also for himself should the suspected terrorist recruiters learn of his action.

Institutionalizing these lessons so as to strengthen the criteria will be more effective than reverting to the immediate post 9-11 practice of treating every bit of information that comes in with equal weight and giving credence to all of them, at the expense of identifying and focusing on more probative and credible information.

Key to a more effective process is ensuring that no part of it becomes a "check the box" effort. Simply moving information from one place to another is not effective "information sharing." What we seek is shared understanding and a sense of responsibility, not just shared documents. Government officials at every step, from consular officers to analysts to TSC administrators must view the policies and procedures as essential but not necessarily sufficient.

As the "after-action" reviews continue, it may emerge that the failure to connect the father's concerns with the other intelligence reports also reflects, at least in part, a traditional bias within intelligence agencies against information that comes in through open sources rather than having been "stolen" using intelligence methods. This mindset is changing, but slowly.

***Appropriate Use of Technology, Not New Collection Authority***

It is also important to recognize that the reviews released to date of both the December 25 failed attempt and the tragic shooting at Ft. Hood have concluded that the government had the information necessary to prevent these incidents. Neither incident reflected a need for greater government authority to collect information, and none of the reviews calls for new collection authority. Instead, both reflect a need to better understand and exploit information already known.

According to the White House Review, a key error in this case appears to be the failure to "search all available databases to uncover derogatory information that could have been correlated with Mr. Abdulmutallab." Improved policies and training can help but sorting through the mountains of data that come in to the IC on a daily basis may ultimately require improved technology.

"Data mining" has been largely a taboo subject for public discussion and debate ever since the disastrous launch of the Total Information Awareness project. However, it can be a powerful tool for enhancing national security, if employed in appropriate ways. This is an area in which privacy and civil liberties concerns fueled an effort to eliminate all risk of government abuse by simply banning the use of this technology. Here, too, we need a risk management approach instead.

We need to bring this range of technologies back into the light and have a serious conversation about how to use them to more effectively sift through government data in ways that allow for appropriate safeguards and oversight. The President has asked his Intelligence Advisory Board to "examine the longer-term challenge of sifting through vast universes of intelligence and data in our Information Age." I would urge the Board to conduct its work with a level of transparency unusual for that body but essential to fostering public understanding and trust.

***Clarifying Roles and Responsibilities***

The President has also called for assigning clear lines of responsibility. Congress has tried for years to clarify the roles and responsibilities of NCTC, CTC, FBI, DHS, and DOD in counterterrorism analysis and collection. This is important not just to prevent turf battles or reduce unproductive duplication but also to ensure that critical tasks do not fall through the cracks. When everyone is responsible, no one is.

The need for clarification is particularly evident with regard to the relationship between NCTC and CIA's Counterterrorism Center (CTC). The CIA center does both operations and analysis. Inevitably, analysts wind up spending a great deal of time on operational support, at the expense of strategic analysis. NCTC, on the other hand, has primary responsibility for strategic analysis, as well as tactical warning. The White House Review concludes that, "both agencies - NCTC and CIA - have a role to play in conducting (and a responsibility to carry out) all-source analysis to indentify operatives and uncover specific plots like the attempted December 25 attack." This does nothing to help clarify the lanes in the road. This overlapping and unclear responsibility can result in things falling through the cracks and permit finger pointing when analysts fail to connect key information.

It may be time to consider narrowing the role of the analysts at CTC, perhaps rotating them through NCTC to do strategic analysis and having them focus on operational support activities when they are assigned to CTC. The task of keeping CIA leadership informed of terrorist threats could rest with strategic analysts assigned to NCTC but sitting at CIA.

The President's call for clarifying roles and responsibilities also presents an opportunity to finally address confusion over the roles of FBI and DHS's Intelligence and Analysis shop, as well as the role of the Defense Department both in analysis and in operations overseas and at home. Some of the confusion in these relationships seems evident in the preliminary findings related to the Ft. Hood shooting. (See White House's "Public Summary of the Inventory of Files

Related to Fort Hood Shooting" and the Report of the DoD Independent Review, "Protecting the Force: Lessons from Fort Hood," both released on January 15, 2010.)

An early warning sign of overlapping responsibilities was the request several years ago of DOD and CIA to have the same authority as FBI to issue their own national security letters. When everyone feels that they need everyone else's authorities, it is an indication that the notion of specialization, in which each entity fulfills a role on behalf of the common mission, is falling by the wayside, with consequences for coordination and effectiveness.

Risk elimination might suggest that everyone should do everything, in the hope that at least one of the players will discover the plot or take the key action. Risk management recognizes that this approach carries its own risks.

***Reducing Recruitment***

The focus on detecting terrorists and better securing aviation and our borders should not obscure or distract from the fundamental need to find ways to prevent young men like Abdulmutallab, and Malik Nidal Hasan, from being recruited in the first place. Key to this is reducing the appeal of violent extremism. The recent report from the Combating Terrorism Center at West Point documenting the reality that the overwhelming majority of the victims of terrorist attacks are Muslims highlights an important piece of that effort. ("Deadly Vanguards: A Study of Al Qaeda's Violence Against Muslims") The way in which we conduct our counterterrorism policies also can either strengthen or undermine the narrative that terrorists use to appeal to potential recruits. Fully understanding this risk is essential to defeating the terrorist threat.

***Managing Guantanamo Detainees***

The December 25 event has led to suggestions that no more detainees should ever be released from Guantanamo, because the al Qaeda group in Yemen claiming responsibility for this attempted attack reportedly includes in its leadership a released detainee. This also reflects a "zero risk" mentality that would ultimately harm counterterrorism efforts.

There are risks inherent in the transfer or release of detainees. However, there are also risks in indefinitely detaining all detainees, including those cleared for release by the courts or by an Administration review. A bipartisan group of national security and counterterrorism experts agreed, in a message to Congress this past summer (attached), that the security gains from an absolutist policy of no transfers are illusory because it will feed the terrorist narrative and provide ammunition for recruitment of far more potential terrorists than reside in Guantanamo. (See also "The real threat is terror itself," by Charles C. Krulak and Joseph P. Hoar, *Philadelphia Inquirer*, January 15, 2010: "Guantanamo gives our enemies a potent recruiting tool. We must deny them this powerful weapon, or the struggle against terrorism could be truly unending.")

A risk management approach would recognize the risks inherent in transfers and develop smart policies to reduce those risks without losing the significant counterterrorism benefits that

come from undermining the terrorist narrative about Guantanamo. This approach, for example, would seek ways of placing detainees who are cleared for transfer or release into a careful program of assessment and assistance in order to reduce their vulnerability to recruitment. This is consistent with the recommendation made last March by another bipartisan group of experts after visiting the program in Saudi Arabia for transferred Guantanamo detainees. (See attached memorandum from the independent *Task Force on Released Guantanamo Detainees*.)

We should continue to work with the Yemeni government and others in the region to find a more satisfactory solution to the security issues related to transferred detainees. The Saudi program for dealing with detainees released from Guantanamo has been oversold and is not perfect, as demonstrated by the 11 graduates of the program who reportedly joined or rejoined the fight after their release. That said, it has a far better track record than US prison recidivism rates. Some sort of regional center may be appropriate for detainees from Yemen and other countries in the area who are cleared for transfer.

***Conclusion***

The dream of zero risk caused us to view the December 25 incident as a massive failure on our part, prompting calls for resorting back to policies like those adopted immediately after the attacks of 9/11. I worry that this reaction, ironically, contributed to turning a terrorist's failed attempt into a terrorist victory, as evidenced by the groups now clamoring to take "credit".

Perhaps most importantly, pretending that all risk of terrorist attack can be eliminated undermines the resilience of the American public. For too many years we were told that another terrorist attack represented an existential threat that must, and could, be avoided at all costs. Many Americans became convinced that "balancing civil liberties and national security" meant these were mutually exclusive objectives on opposite sides of a scale; that if we were just willing to give up enough of our civil liberties we could buy security. Fear, and the corresponding promise that absolute protection could be purchased with the sacrifice of liberties, was used to gain support for policies. Over time, this fear-induced desperation becomes debilitating.

Americans are naturally resilient. We cope best with risks we understand. Our leaders should accurately convey those risks and craft policies that effectively address them.

Thank you for this opportunity to submit testimony and for the committee's commitment to conduct the oversight necessary to learn lessons from these events. In the wake of the December 25 incident,we have a relatively unique opportunity to significantly advance our efforts without the preceding loss of lives that is typically required to get the necessary attention--and which often provokes a sense of crisis that can cloud judgment. I hope we are able to capitalize on this good fortune to implement wise, effective changes that make us all safer.