

**SHARING AND ANALYZING INFORMATION
TO PREVENT TERRORISM**

HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
ONE HUNDRED ELEVENTH CONGRESS
SECOND SESSION

—————
MARCH 24, 2010
—————

Serial No. 111-116

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://judiciary.house.gov>

—————
U.S. GOVERNMENT PRINTING OFFICE

55-598 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

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California	LAMAR SMITH, Texas
RICK BOUCHER, Virginia	F. JAMES SENSENBRENNER, JR., Wisconsin
JERROLD NADLER, New York	HOWARD COBLE, North Carolina
ROBERT C. "BOBBY" SCOTT, Virginia	ELTON GALLEGLY, California
MELVIN L. WATT, North Carolina	BOB GOODLATTE, Virginia
ZOE LOFGREN, California	DANIEL E. LUNGREN, California
SHEILA JACKSON LEE, Texas	DARRELL E. ISSA, California
MAXINE WATERS, California	J. RANDY FORBES, Virginia
WILLIAM D. DELAHUNT, Massachusetts	STEVE KING, Iowa
STEVE COHEN, Tennessee	TRENT FRANKS, Arizona
HENRY C. "HANK" JOHNSON, JR., Georgia	LOUIE GOHMERT, Texas
PEDRO PIERLUISI, Puerto Rico	JIM JORDAN, Ohio
MIKE QUIGLEY, Illinois	TED POE, Texas
JUDY CHU, California	JASON CHAFFETZ, Utah
LUIS V. GUTIERREZ, Illinois	TOM ROONEY, Florida
TAMMY BALDWIN, Wisconsin	GREGG HARPER, Mississippi
CHARLES A. GONZALEZ, Texas	
ANTHONY D. WEINER, New York	
ADAM B. SCHIFF, California	
LINDA T. SANCHEZ, California	
DEBBIE WASSERMAN SCHULTZ, Florida	
DANIEL MAFFEI, New York	
[Vacant]	

PERRY APELBAUM, *Majority Staff Director and Chief Counsel*
SEAN MCLAUGHLIN, *Minority Chief of Staff and General Counsel*

CONTENTS

MARCH 24, 2010

	Page
OPENING STATEMENTS	
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary	1
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary	2
The Honorable Daniel E. Lungren, a Representative in Congress from the State of California, and Member, Committee on the Judiciary	4
The Honorable Darrell E. Issa, a Representative in Congress from the State of California, and Member, Committee on the Judiciary	6
The Honorable Steve King, a Representative in Congress from the State of Iowa, and Member, Committee on the Judiciary	7
The Honorable Ted Poe, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	8
The Honorable Tom Rooney, a Representative in Congress from the State of Florida, and Member, Committee on the Judiciary	9
WITNESSES	
Mr. Russell Travers, Deputy Director for Information Sharing and Knowledge Development, National Counterterrorism Center	
Oral Testimony	11
Prepared Statement	14
Mr. Timothy J. Healy, Director, Terrorist Screening Center, Federal Bureau of Investigation	
Oral Testimony	17
Prepared Statement	20
Ms. Patricia Cogswell, Acting Deputy Assistant Secretary, Office of Policy, Department of Homeland Security	
Oral Testimony	27
Prepared Statement	29
The Honorable Patrick F. Kennedy, Under Secretary for Management, U.S. Department of State	
Oral Testimony	44
Prepared Statement	47
APPENDIX	
Material Submitted for the Hearing Record	75

SHARING AND ANALYZING INFORMATION TO PREVENT TERRORISM

WEDNESDAY, MARCH 24, 2010

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:15 a.m., in room 2141, Rayburn House Office Building, the Honorable John Conyers, Jr. (Chairman of the Committee) presiding.

Present: Representatives Conyers, Nadler, Scott, Watt, Jackson Lee, Delahunt, Pierluisi, Quigley, Chu, Schiff, Smith, Coble, Goodlatte, Lungren, Issa, King, Franks, Gohmert, Jordan, Poe, and Rooney.

Staff Present: (Majority) Perry Apelbaum, Staff Director and Chief Counsel; Aaron Hiller, Counsel; Renata Strause, Staff Assistant; (Minority) Andrea Loving, Counsel; and Caroline Lynch, Counsel.

Mr. CONYERS. Good morning, ladies and gentlemen. Someone said are we going to start anytime soon? And I know Dan Lungren's voice when I hear it. So let's begin.

We are having an oversight hearing on "Sharing and Analyzing Information to Prevent Terrorism." And I am privileged that this discussion could arise in the Judiciary Committee. The 9/11 attacks, the Fort Hood shootings, and the attempt to destroy Flight 253 headed for Detroit this past Christmas all reveal limits of our government's ability to use information to stop terrorist attacks. These are longstanding issues that predate both the Obama and Bush administrations. So today we have a valuable opportunity to explore what the government has done and what it is doing and what it needs to do to put these problems in perspective and to keep everyone in this country as safe as possible.

Now, it is no secret that the Administration has faced a series of political criticisms in the wake of the attempted Christmas Day airplane bombing in Detroit because FBI agents gave Miranda warnings during their interrogation of the Flight 253 suspect. One of our Members in the other body called it irresponsible and dangerous. Another claims that there will be dire consequences.

Now, in my view, these assertions ignore the reality the suspect was first questioned without Miranda warnings and gave up important information. Some criticisms ignore the fact that the Miranda warnings were not given until after the suspect had stopped talking of his own accord. Some ignore the fact that the suspect has

continued to cooperate and provide valuable information after receiving the Miranda warnings.

They ignore the fact that under the prior Administration Miranda warnings were read to the so-called shoe bomber Richard Reid on four separate occasions. According to reports, the first warning was given 5 minutes after he was taken into custody. The same is the case with many complaints we hear now about trying terror cases in Federal court. Some ignore the fact that the prior Administration tried numerous terrorism cases in Federal court without major incident and pretty good success. It also is notable that in the recent conviction in the Federal court of David Coleman Headley for his role in the Mumbai Hotel attacks, Headley reportedly provided extensive intelligence after being charged and is now serving a life sentence.

There is no issue that we face as a Nation that is more challenging than getting the balance right on terrorism. While none of us can predict the future, I can tell you our constitutional system of checks and balances has served our Nation well for more than 230 years and has been a model for many nations around the world. As a matter of fact, some of us have gone to the countries that were trying to emulate our constitutional and democratic system of government. Now, if we follow that model, I believe we can and will defeat terrorists and protect our citizens' liberties. I suppose that is, for my purposes, ladies and gentlemen, the purpose of the hearing. How do we protect our citizens and still keep our liberties? So in that spirit, some questions that I hope the distinguished national security professionals here today will address.

In early January, the President issued a series of written directives to the executive branch agencies involved in national security. He described this memo as corrective additions and demanded monthly progress reports on their implementation. I hope some of our witnesses can update us as well on the progress of these corrective actions. Second, it seems that one of the biggest intelligence challenges we face is learning to deal with the larger volumes of information that we collect and developing methods to separate the wheat from the chaff.

Do you think there is a point at which we are collecting so much information that we are actually making it harder to identify and separate out the action that really matters? Is there such a thing as collecting too much information? And, finally, we have become very expert here in figuring out what went wrong in a particular instance and fixing those gaps, but I think we have a broader view here.

After 9/11, we improved our information sharing, and now after Flight 253, we will have new analysis teams and better systems to search our databases. I would like to know what you as our experts and guests here this morning are doing beyond this fighting the last war kind of mentality. What are we doing now to identify other possible gaps that may be existing in our security systems? And so I welcome you here this morning. And I would like to yield to my friend, Lamar Smith of Texas.

Mr. SMITH. Thank you, Mr. Chairman.

Umar Farouk Abdulmutallab attempted to blow up Northwest Flight 253 on its way to Detroit on Christmas Day. Thankfully, his

attempt was thwarted and hundreds of innocent lives were spared. After failing in his attempt to murder 288 innocent Americans, Abdulmutallab was questioned for less than an hour and then given the right to remain silent. He then stopped talking to investigators for the next 4 weeks. The Administration brushes off criticism about its decision to Mirandize Abdulmutallab because he has since provided useful intelligence to investigators. But what vital intelligence was missed because of his 4 weeks of silence? Was a plea bargain for reduced sentence necessary to get information, and what questions did his lawyers refuse to let him answer?

At the very least, Abdulmutallab's month of silence gave his co-conspirators time to cover their tracks. So the Obama administration forfeited an opportunity to obtain information that might have identified terrorists and prevented future attacks. That neither the President nor his national security advisors supported treating Abdulmutallab as an enemy combatant is worrisome. As the President has admitted under his new policies, the CIA has "a harder job." The President's policies make it easier for terrorists to get constitutional rights and harder for intelligence officials to keep America safe. Abdulmutallab should never have been allowed to board the plane to Detroit. Despite warnings from Abdulmutallab's father about his son's possible Muslim radicalization, the U.S. Visa he had been issued in 2008 was neither identified nor revoked.

Mr. Chairman, I want to call a piece of legislation to your attention because it goes to the future, as you just were suggesting a minute ago. Earlier this month, I introduced legislation designated to help make the visa process more secure. H.R. 4758, the Secure Visas Act, requires placement of visa security units at U.S. Consular posts in high risk countries such as Algeria, Lebanon, and Syria. The placement of visa security units at U.S. consular posts will help address lapses in the current system and prevent terrorists from gaining access to the United States. H.R. 4758 explicitly grants the Department of Homeland Security Secretary the authority to revoke a visa and to delegate that authority to others in the agency. These are commonsense steps to help ensure that no one who wants to do us harm is able to enter and stay in the United States.

The President says that we are at war with terrorist groups, but many of the Administration's decisions have actually put the American people at greater risk. First, trying to close a terrorist detention facility at Guantanamo Bay has not made America safer. The Pentagon has reported that 20 percent of released Gitmo terrorists have returned to plotting attacks against Americans. Two former Gitmo detainees in Yemen are suspected of organizing the Christmas Day plot. Second, the Administration's decision to try terrorists in Federal civilian court continues the trend of weakening national security.

Bringing terrorists into the criminal justice system limits our ability to interrogate them and get intelligence that might prevent attacks and save lives. Abdulmutallab didn't simply rob a convenient store. He tried to blow up a plane and kill nearly 300 innocent civilians. This was an act of war and should be treated as such. The American people agree. Sixty-seven percent of Americans favor military tribunals to try terror suspects.

And, third, the Obama administration released highly sensitive memos detailing interrogation tactics used against terrorists. The formerly classified Office of Legal Counsel memos gave terrorists a how-to manual on how to resist interrogation tactics. These are just a few of the ways the Administration has weakened our national security.

Richard Cohen, a very liberal columnist, recently wrote in *The Washington Post* that “There is almost nothing the Obama administration does regarding terrorism that makes me feel safer.” Last month, national security officials warned that another terrorist attack is certain within the next 3 to 6 months. But we don’t need national security officials to predict attacks. We need them to prevent attacks. That means we need to apprehend and interrogate terrorists.

Many believe that the war on terror is over and that the threat from al Qaeda and other terrorist groups is nothing more than a vague memory from 9 years ago. The Christmas Day bombing attempt is proof that the war on terror continues and that radical jihadists are as committed as ever to killing Americans. The Administration must be equally committed to stopping them. The time for complacency is over.

Thank you, Mr. Chairman, and I yield back.

Mr. CONYERS. Thanks, Lamar.

I now recognize Dan Lungren, the senior former Attorney General of the largest State in the union.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I understand how serious the issues are that are before us today. I respect the professionals that are here before us. But I would be less than honest if I did not say that I have profound differences with the approach this Administration has taken in a number of different areas. I understand the importance of things such as the Miranda warnings. I recall when I had the opportunity to personally argue a case before the U.S. Supreme Court on an essential concept, what is the constitutional definition of reasonable doubt given to juries in criminal cases, seemingly an elementary question but one that caused the court to grant a case consideration from two states in the union, my state being one of them.

At the same time, I have always understood the distinction between a criminal justice matter and a matter of national security and particularly a matter of national security based on a terrorist threat. And what we have to do is somehow deal with that area where they come into contact, and the question therefore is a serious one, whether it is appropriate for us to take those concepts, some would say that are bedrock in our criminal justice system, and somehow place them over into the national security arena, particularly in the area of terrorism.

The 9/11 Commission told us that one of the major criticisms of our actions before 9/11 was our failure to connect the dots, and there were those that suggested that part of that was our confusion in that area of nexus between the criminal justice system and the national security system. In responding to that, we attempted to make changes. I don’t know anybody who believes what we did in responding to the threat during the Christmas period by this particular bomber—anybody thinks it was sufficient.

Mr. Leitner has told us that Mr. Abdulmutallab should not have stepped on the plane, the counterterrorism system failed. And I told the President we are determined to do better. So our question is how do we do better?

And one of the areas I would I guess directly disagree with the Chairman, with all due respect, is the idea that somehow Mirandizing people makes it more likely that they are going to speak to us than if they are not Mirandized, almost as if there is some psychological impact on people that once we grant them their Miranda rights, they feel obligated to tell us something. In fact, in law enforcement circles, while we know we are required to doing Mirandizing, we recognize that oftentimes that interferes with our ability to gain useful information, but we believe that is acceptable under our Constitution.

But I would suggest that we are in dangerous territory if we blithely transfer the same concept of Miranda warnings that the Supreme Court has put forward into the area of suspected terrorists. One of the things that bothers me, and I think bothers everybody, is why did we not connect the dots here, the information that was there, a father that comes to an American entity and says, I suspect my son may have fallen under the influence of terrorist groups in Yemen.

Somehow that doesn't get through the system and I know we are going to hear some in detail on that. But in response to that, I have been informed that while the previous Administration instructed the government to identify and collect information on individuals "appropriately suspected," or "reasonably suspected" of terrorist connections, or for whom there was an articulate and reasonable basis for suspicion, that we now have adopted a new standard that says this: To meet the reasonable suspicion standard, the nominator, based on the totality of circumstances, must rely on articulable intelligence, or information, which taken together with rational inferences from those facts, reasonably warrant a determination that an individual is known or suspected to be or have been knowingly engaged in conduct constituting in preparation for, in aid of, or related to terrorism or terrorist activities.

And I will inquire of the four of you how you believe that that gets us where we need to go, that somehow that makes it more rational and somehow with that standard that is going to get the information flow unclogged as it was clogged in the case that we are talking about.

I would argue that that kind of legalistic, almost CYA language, is going to make it more difficult. And if I am the person involved in the system and I am told that is the standard to which I will be held, and if I fail that standard, I will be disciplined or perhaps punished, how that is going to encourage people in the Intelligence Community to do the kind of creative thinking and thinking out of the box that is necessary to protect this country so that we don't come here after another incident that may be successful and say, you know, we created a wall that we didn't intend to create that somehow mandated that our people were not creative in their thinking and did not think out of the box and, therefore, because the bad guys thought out of the box, we have lost lives.

I thank the Chairman for the time.

Mr. CONYERS. Thank you very much.

I now turn to Darrell Issa, who is not only the Ranking Member on Government Reform, but served with distinction on the Intelligence Committee itself.

Mr. ISSA. Thank you, Mr. Chairman.

And I want to associate myself in a broad sense with all of you. I think today's hearing for all of us who serve on this Committee and other Committees is the beginning of a process of reevaluating the work we have done over the last 9 years. I am personally a civil libertarian, as the Chairman knows. I very much believe that Miranda is an important right of individuals against self-incrimination. However, when we choose areas of specific protection, not the battlefield, where as an Army lieutenant I was never given a copy of Miranda to read to somebody that if I were so fortunate as to find them on the battlefield, those are opportunities in which investigations begin well afterwards. But our domestic ports of entry are, by definition, controlled environments in which the scenario and the plan of what to do if someone is found entering or exiting with a plan to bomb or in some other way commit a terrorist act is a scenario we can plan and predict.

There is no question that the FBI should have known what they were going to do if a man with explosives in his pants was found and whether or not the best course of action was to Mirandize him, as Mr. Lungren said, in the hope that that somehow would cause him to tell us more or not Mirandize him because ultimately they had what they needed in order to effectively prosecute him for one or more crimes, while at the same time, they had no idea who the other terrorist conspirators could be.

I think that is a point that Government Oversight and Reform will continue to look at. The question of in controlled space, do we really have the scenarios, are they well thought out, and are they leading to the best outcome from prosecution standpoint when appropriate but clearly from a standpoint of safety of American travelers and the American people overall? On that, I believe we can all agree there was a failure. Additionally, I happen to be an Arab American, and so I want to associate myself broadly with the fact Arab Americans have been the victims of a loss of civil liberties. Those who were innocent Americans, including my poor nonArab wife, who just happens to be cursed with the last name Issa, Arabic for Jesus, finds herself on a No-Fly List. I am equally concerned that the No-Fly List can somehow get Katherine Issa onto it and have to be taken off, while somebody's whose own father says he is going to try to commit a crime, he is a terrorist, he is an extremist, don't let him in, somehow does not rise to the level in any one of the many cables alone nor are the cables connected in a way that will lead to that outcome.

I am deeply concerned because I have been reluctantly supporting legislation that often goes beyond my comfort level including some elements of the PATRIOT Act, and yet we don't seem to have gotten what we were promised. Again, beyond the scope of just this Committee, but well within the scope of all of us as people who swore allegiance to the Constitution.

Last, as the Chairman was kind to mention, in my service on the select Select Intelligence Committee and now my membership as

the Ranking Member of Government Oversight, we have invested countless—hundreds and hundreds of billions of dollars in creating databases that can, in fact, serve us to prevent stovepiping. The excuse that the dots were not connected this time is a self-inflicted wound, not created by money—or not prevented by lack of money and certainly not by lack of a directive from all of us on the dais and all of the people in the last Administration that we connect the dots.

I don't think it is a secret by any means that our Intelligence Community can take disparate information, pieces and bits of words, put them together, and with analysis, sometimes automated, sometimes by talented human beings, reach a conclusion that there is a threat. We do that when we look outward.

Today, with the indulgence of the Chairman, I am going to task the individuals here to explain to us in open session why we don't turn that same analysis inward so that disparate cables, as we are being told, each one not being sufficient to cause a triggering of the No-Fly List, were not connected by some sort of software which we certainly have paid for, we certainly own, and we certainly believe failed us on Christmas Day.

Mr. Chairman I thank you for your indulgence and yield back.

Mr. CONYERS. Thank you, Darrell.

I now recognize Steve King of Iowa, who serves in addition to our Committee on Small Business and Agriculture as well.

Mr. KING. Thank you, Mr. Chairman.

I appreciate this hearing and the witnesses coming before this panel today. And as I listened to the opening statements of yours and Ranking Member Smith and others that have discussed this issue, it comes back to me that we had a shoe bomber and that happened years ago. That was the heads-up for something like this. And when we set up our security system, the Department of Homeland Security and all of the pieces of Federal legislation that put the tools in place so that we could prevent terrorists from hijacking airplanes, set up the filters as much as we could, this is one of the things that we had in mind.

I mean it isn't a new tactic. It was a tactic that had already been used when this—when these parameters were set up, when the people that are in charge in the departments are thinking about what could happen bad to the United States, this had to be a model of no more shoe bombers. I mean, I have taken my shoes off so many times I know that is model. And yet the dots weren't connected and I can't understand why the device itself wasn't discovered, and that is a problem. That is a serious problem on how we would actually be able to identify individuals getting on airplanes that are might have devices like that.

So our heads up that is back through the visa program and the visa security program, and when I think about the one reason that was given, one of several, that there was—that the exact spelling of his name didn't exactly match up; so therefore they believed that there wasn't a visa that had been issued to—I always have to look that up—Abdulmutallab—I have got Abdul Farouk Abdulmutallab, and it takes a little practice. But I have to go back and I look at that and I think all right, that is understandable if you are matching up paper records or if you are putting a name in quotes and

sending it off in a software search, but when I do that on a Google page, it comes up and says "didn't you mean" and it will give me an alternative spelling.

One of the things I am going to be interested in now, do we have at least a Google software so we could resolve that problem? And I am also interested in how it was that his father himself who said my son has disappeared and I believe that he has gone over to the other side and been radicalized, that should have been powerful enough for there to be individual attention to follow it.

And the third thing would be he was a high-ranking Nigerian official who had credibility. It wasn't just someone off the street and it wasn't just a lineup of many cases. This was a case that should have had a red flag on it in several different ways. And then I am also interested in the difference in the philosophy of how we are going to go forward and fight their global war on terror. The philosophy of it is a law enforcement action, it has been clear that this Administration has put down marker after marker after marker that they believe it is law enforcement and not a war. And I contemplate what we do when we have terrorists that fit a whole series of different kinds of definitions.

You could have a terrorist that was born, raised, bred, and trained and committed or attempted to commit an act against American interests in a foreign country and never set foot in the United States. You could go clear to the other side, a born, raised, bred and trained American terrorist who never set foot outside the United States but still was radicalized and still was part of that same network.

And I think I could give you about six other definitions that fit in between those two extremes. Yet they are all part of the same movement that is attacking the United States, and we can't do this as just a law enforcement endeavor and we can't have terrorists that are committing similar acts that fit different categories of terrorism that go into a different system in our justice. We have got to look at this as a war and we have got to put the enemies we are fighting in the same category.

So I am going to suggest that as we go through this discussion today, we consider an idea that I generated some months ago, and that is the idea of establishing a new set of laws for our terrorists and to adjudicate them immediately as a terrorist, and not read them their Miranda rights, and let them be subjected to the amount of interrogation necessary to protect the American people, try them all in a military court, get them all off of U.S. soil and out of the hands of our Federal judges as quickly as we can so that we can effectively fight this war.

Those are the parameters that I view this as I listen to this discussion. I am looking forward to the testimony of the witnesses. And Mr. Chairman I appreciate your indulgence and I yield back the balance of my time.

Mr. CONYERS. Thank you, Steve.

I now turn to Judge Ted Poe of Texas. He serves on Foreign Affairs and on both the Crime and Immigration Subcommittees.

Mr. POE. Thank you, Mr. Chairman.

With all of the U.S. resources and money and intelligence and information, our security system in this incident boils down to the

fact that we had to rely on an individual from the Netherlands who saw the underwear bomber doing something he shouldn't be doing, like setting his pants on fire and jump across several other people in an airplane to tackle him and then with the aid of other passengers, he was subdued. But for that person from the Netherlands, I believe we would have had a tragedy. I don't think that is a good security system that we have to rely on passengers to be our hope for defense of preventing airplanes from being blown up.

Everybody wants to say somebody else is at fault. But the bottom line is there is information available and it wasn't used. We have a watchlist. We have a No-Fly List. And it seems like those are just lists that don't do anything except keep certain people from not flying. And the watchlist with the thousands and thousands of other people, I guess we are just watching those folks. I think we need to do some obvious things and that is get our house in order and secure the system so that we keep outlaws from getting on our airplanes.

And it starts all the way back to the embassy that gets information from Daddy that this guy is a threat to the United States. A lot of people fell down on their jobs but some day somebody is going to die because people don't share information and pass information on. So I think excuses, there are no excuses for why the system fails. We cannot let it fail. Otherwise we will have tragedy and maybe we need to rethink some of the ways that we talk to folks who show up at airports. I think the Israelis have set up a model that has been quite successful for their nation.

In any event, we ought to at least talk to them about how they are able to be so successful and maybe we should adopt their procedures in some of our airports. But the American people deserve better. They deserve better from a Nation that is supposed to be the world's superpower, and they deserve better than to expect that some passenger from the Netherlands is going to save us all from disaster.

Thank you, Mr. Chairman. I yield back.

Mr. CONYERS. Thank you. Tim Rooney, did you have a comment? The gentleman from Florida is recognized.

Mr. ROONEY. Thank you, Mr. Chairman. It is Tom Rooney but that is okay. I am a new guy.

Mr. Chairman, it has been almost 9 years since the attacks of September 11, 2001, and I clearly remember in the days following the attacks of 9/11 we committed as a Nation to never allow such a failure of intelligence ever to happen again. I clearly remember the formulation and the makeup of why and what Homeland Security was going to be, that we would never have a communications breakdown again between agencies of the Federal Government so that Americans could feel safer, that the communications between the various agencies would be more fluid. I wasn't sure how creating a new agency was going to do that, but of course had the confidence in our government to be able to figure that out for me as a regular constituent at that time and to keep us safe.

And we have, as the Chairman said, over the last 9 years been kept safe. But in the last year there has been some serious flags that have been raised as you have heard in the various opening statements so far. Fort Hood, Texas, where I was formerly sta-

tioned, we came to know a guy named Major Nidal Hasan, who we have since come to know as a captain was a very substandard Army officer who was communicating with people that should have raised red flags. We have also come to know that these communications separate from his officer evaluation reports were known by people in the Intelligence Agency and may or may not have been shared with the Department of Defense or the Department of Army.

And my immediate question after that is how after 9/11 with Homeland Security and everything that we talked about, that these agencies would communicate better, how does Intelligence Agency not communicate with the Department of Defense and say one of your own is talking with people, Awlaki, who has been in communications with 9/11 pilots, and as we will come to see, Abdulmutallab himself. Then we see, of course, what we are here today to talk about and that is the communications failures leading up to the attack on Christmas.

The President said that after this attempt by the so-called underwear bomber that there was a mix of human and system failures that contributed to this potential catastrophic breach of security. I kind of disagree with that. I think that it was not potential catastrophic. I think it was catastrophic when it comes to you and your jobs. I think there can be nothing more discomfoting to the American people to know that over the last year, we have had these two breaches of security, and I think that they are catastrophic and hopefully that is one of the things that we can try to figure out here today.

But my questions are where is the disconnect? We have heard before by other opening statements, where are the dots not connected? And I have a chart to discuss with you later during Q&A, but when and where are we allowed to do and not to do for the sake of national security? What are we allowed to do? And that goes with, as we said, Miranda. What constitutional protections come to these people? And then juxtapose that to what the American people expect of us.

I have seen the databases. I have seen the Visa VIPER, the TIDE, the Selectee, the No-Fly List, who qualifies, who doesn't qualify, what standard of proof is needed to put somebody on these lists. It is very confusing. And it seems like a lot of people have their fingers in this game. And again, I am just not sure that that was the purpose after 9/11. The sale that was made to the American people that you would be kept safe by a more streamlined system, it doesn't seem that way to me. As was said I am also very concerned about the fact that Abdulmutallab's name was misspelled and that somehow bounced him out of these databases as somebody to keep an eye on. Reports that the NSA reportedly intercepted communications between Awlaki and Abdulmutallab. Again, where were the dots there? Even if the intelligence officials didn't know his full name, how much did they know? What about his dad, a doctor in Yemen, who Petraeus said to us on the Armed Services Committee just last year that Yemen is a place we need to seriously look at and a doctor—and I imagine the people in Yemen aren't very friendly to the people of the United States.

So if a guy goes to the U.S. embassy and he is a doctor and he makes a complaints about his son wanting to blow up—he is taking some risk there I would imagine; so it probably should be taken seriously.

And I don't mean to disparage our Intelligence Community or anybody on this panel. I understand you guys have a very difficult job. I understand that you are trying to do that job and it is not easy. But we have an obligation, as you know, to the American people so that another Christmas Day or another Nidal Hasan does not happen. So being 9 years after 9/11, I personally, as many members on this panel, would love to know how the dots are connected and whether or not it is streamlined enough and if we can and should make it better.

I yield back Mr. Chairman.

Mr. CONYERS. Thanks Tom. I should have mentioned that you were also a military prosecutor in your other career.

Mr. ROONEY. I was actually good at that job, sir. Thank you for mentioning it.

Mr. CONYERS. You underestimate how highly we think of you here in 111th Congress.

Mr. ROONEY. I can feel it. Thank you, sir.

Mr. CONYERS. Bill Delahunt? Oh, he is not here. Bob Goodlatte, do have you a comment?

Well, we want to welcome all of our witnesses here today. Patrick Kennedy, Patricia Cogswell, Timothy Healy. We will start with Russ Travers, Deputy Director for Information Sharing and Knowledge Development for the National Counter Terrorism Center. He has been in the job since 2003 and is in charge of TIDE Terrorism Database and prior to that, he worked in the Defense Intelligence Agency and Army intelligence for 25 years.

All of your statements will be included in the record and we welcome your testimony.

TESTIMONY OF RUSSELL TRAVERS, DEPUTY DIRECTOR FOR INFORMATION SHARING AND KNOWLEDGE DEVELOPMENT, NATIONAL COUNTERTERRORISM CENTER

Mr. TRAVERS. Chairman Conyers, Congressman Smith, Members of the Committee, thanks very much. It is a pleasure to be here.

Mr. CONYERS. Pull your mic up closer.

Mr. TRAVERS. My written statement is going to detail NCTC's role in support of watchlisting and specifically focuses on the attempted attack on Christmas Day. At your staff's request, I am going to expand on that statement and use my opening remarks to address the somewhat broader context that a number of you have addressed in your statements.

I will begin by distinguishing 12/25 issues from those of 9/11, and then I am going to talk specifically about what NCTC has been doing since Christmas. First, the issues raised by 12/25 were not, in any way, like those of 9/11. It was not a failure to share information. The key pieces of intelligence related to 12/25 were broadly available across the Intelligence Community and that is important. Why? Because it highlights the fact that simply sharing information does not guarantee accurate intelligence analysis. In that sense, information sharing is necessary but it is certainly not suffi-

cient. I would also note as a number of you have mentioned information sharing has expanded dramatically since 9/11.

There are difficult legal policy, privacy issues that remain. I would be happy to talk about those in the Q&A if you would like. 12/25 was also not—did not call into question the basic watchlisting architecture that has existed since 2003. It is complicated. I absolutely agree with that. I think it is necessary, though. That architecture that was designed in 2003 was intended to ensure that all screeners had the benefit of any information collected by any collector in the United States Government. That was very different than it was before 9/11.

And in that regard I think we succeeded. In that regard I think, again, we have enhanced information sharing. It is certainly not perfect. It is a names-based system, and 12/25 highlighted a number of seams that my colleagues and I will discuss. For instance, standards as to who gets on a watchlist. We could lower that bar. If we do so, it has significant balance issues. How big do you want the list to get, and what are the associated tradeoffs? Long lines, false positives, and so forth. And we are working through those balance issues. So what did fail on Christmas Day? And here I think the bumper sticker description is that we failed to “connect the dots.” But what does that actually mean?

Personally I do not believe it is a good metaphor. It conjures up the notion of the puzzle that our preschool kids use. You have got a sea of dots. They are numbered from 1 to 29. You follow the line and you get a duck or in our case you get a terrorist plot. Intelligence has never worked that way and it never will. You do have a sea of dots. They aren’t numbered. Lots of them are wrong. Many others are ambiguous or contradictory, and still others are just innocuous. You just don’t know a priori which ones are important, and that was the problem with 12/25.

Father comes into the embassy in Abuja. His son is involved with extremists in Yemen, as a number of you have noted. That given the standards of the time doesn’t come close to getting him watchlisted. It does put him on the screen. It doesn’t get him watchlisted. There was one other piece of information that was out there. It was in the noise. On a daily basis the terrorism intelligence traffic includes something like 10,000 names every day.

In this case we had a partial name, no last name, differently spelled than the name that we got from the father, and that is where we failed. We did not connect those two pieces of information, and that is what we are working very hard to do better in the future.

The question I think is how do we do a better job of exploiting the information that is down in the noise? Is all of that background information in the sea of data that we confront? Conceptually, if you envision that sea of dots, what we are trying to do is lower the bar so there is less information that we are not able to exploit given the resource and time constraints under which we operate. Let me give you three initiatives that we are focused on at NCTC.

First, a presidential directive, we are establishing a record enhancement capability for our terrorist identities database, and that, in effect, is improving our ability to build a fuller dossier on indi-

viduals that are nominated to the National Counterterrorism Center.

Secondly, NCTC has also fenced off about 40 individuals into what we call pursuit teams and these individuals have been relieved of writing intelligence analysis. What they are doing is focusing on data points of potential interest and they are charged with following them through until resolved.

Is this an important piece of information or is it not? And, third, we are continuing to focus on the basic data access, technical infrastructure and tools that are necessary to help find what we call "unknown unknowns." In effect, to help us find linkages between dots when we just don't know a priori that there is any linkage there. A very complicated problem.

In sum, Mr. Chairman, NCTC has been working very closely with all our interagency partners to try to rectify the problems identified by 12/25, and certainly I look forward to answering any questions you may have thank you.

Mr. CONYERS. Thank you.

[The prepared statement of Mr. Travers follows:]

PREPARED STATEMENT OF RUSSEL TRAVERS

Committee on the Judiciary

United States House of Representatives

March 24, 2010

Sharing and Analyzing Information to Prevent Terrorism



Statement for the Record

of

Mr. Russell Travers

**Deputy Director for Information Sharing and Knowledge
Development**

National Counterterrorism Center

Statement for the Record

March 24, 2010

Committee on the Judiciary

Sharing and Analyzing Information to Prevent Terrorism

Chairman Conyers, Ranking Member Smith, and Members of the Committee: Thank you for your invitation to appear before the committee to discuss terrorist screening procedures in light of the attempted terrorist attack on Christmas Day.

It is my privilege to be accompanied by my colleagues from the Federal Bureau of Investigation and the Departments of State and Homeland Security.

Watchlisting Issues Associated with the Incident

Umar Farouk Abdulmutallab was not watchlisted. This statement will explain the reasons why – addressing the post 9/11 changes in U.S. Government watchlisting practices, the associated standards that were adopted by the U.S. Government, and the application of those standards to the case of Umar Farouk Abdulmutallab. It will also address lessons learned as we strive to improve the Intelligence Community's ability to support watchlisting and screening.

- Before the September 11 terrorist attacks, intelligence databases and watchlisting systems were badly disjointed. They were neither interoperable nor broadly accessible and, as a result, two of the hijackers – although known to parts of the U.S. Government in late-1999, were not watchlisted until late-August 2001.
- To fix that systemic problem, the U.S. Government implemented Homeland Security Presidential Directive-6 (HSPD-6) in the Fall of 2003. Under the construct of HSPD-6, all collectors would provide information on known and suspected terrorists (except purely domestic terrorists) to NCTC which maintains a TOP SECRET database called the Terrorist Identities Datamart Environment (TIDE). Every night a FOR OFFICIAL USE ONLY extract of TIDE is provided to the Terrorist Screening Center (TSC) to support all U.S. Government screening operations.
 - The determination of what information is passed from TIDE to the TSC is governed by the “reasonable suspicion” standard which describes the minimum derogatory information for inclusion on the consolidated watchlist.
 - That criteria, approved by the Deputies Committee in the Fall of 2008, notes that “individuals described as militants, extremists, jihadists, etc should not be nominated without particularized derogatory information.”
 - The implementing instructions further state “those who only associate with known or suspected terrorists, but have done nothing to support terrorism” are ineligible for the No Fly List (NFL) or Selectee List (SL).

Mr. Abdulmutallab was in TIDE, but his name was not passed to the TSC for watchlisting. This was due to two factors:

- The TIDE record that existed on Mr. Abdulmutallab was based primarily on information provided to the U.S. Embassy in Abuja, Nigeria on November 20, 2009. The cable included one general sentence of derogatory information related to his possible association with Yemeni-based extremists. The entire watchlisting community agrees that the level of derogatory information contained in the November 20, 2009 cable did not meet the minimum standard highlighted above and was insufficient for any level of watchlisting---much less either the No Fly List or Selectee lists.
 - As a result, Mr. Abdulmutallab was entered into TIDE November 23, 2009, but his name was not passed to the TSC for watchlisting. Additional biographic information was added to the record over the course of the next week, but no additional derogatory information was provided.
 - In order to provide some context, on any given day hundreds of other names are added to TIDE and virtually all of them would have far more alerting derogatory information than Mr. Abdulmutallab's record.
- While the November 20, 2009 cable formed the basis for the TIDE record and the watchlisting status as of December 25, 2009, we learned after the incident of additional reporting that---had it been linked to the November 20, 2009 cable---could have supported a watchlisting nomination.
 - Had this information been linked to Mr. Abdulmutallab's record, his name undoubtedly would have been entered on the visa screening "lookout" list and the border inspection list.
 - Whether Mr. Abdulmutallab would have been placed on either the No Fly List or the Selectee List would have been determined by the strength of the analytic judgment.
 - It is important to note that the linkage of these pieces of information appears far more apparent in hindsight than it would have at the time. The reporting existed in daily intelligence holdings that number well into the thousands. Partial names and different spellings complicated the linkage. To be sure, the Intelligence Community continues its efforts to improve performance, but linking two pieces of fragmentary information can be a very difficult analytic problem. The two cables existed largely "in the noise" and there was simply nothing particularly alerting about either "dot."

Lessons Learned

- First of all, it is necessary to dispel two myths:
 - This situation doesn't implicate the HSPD-6 watchlisting architecture. The National Counterterrorism Center continues to believe it is fundamentally sound.

- This incident does not raise major information sharing issues. The key derogatory information was widely shared across the U.S. Counterterrorism Community. The “dots” simply were not connected.
- The incident does highlight the following issues:
 - The U.S. Government needs to look at overall standards---those required to get on watchlists in general, and the No Fly List and Selectee List in particular.
 - The U.S. Government needs to improve its overall ability to piece together partial, fragmentary information from multiple collectors. This requirement gets beyond watchlisting support, and is a very complicated challenge involving both numbers of analysts and the use of technology to correlate vast amounts of information housed in multiple agencies and systems.

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.

TESTIMONY OF TIMOTHY J. HEALY, DIRECTOR, TERRORIST SCREENING CENTER, FEDERAL BUREAU OF INVESTIGATION

Mr. CONYERS. Timothy Healy is the director of The Terrorist Screening Center at the FBI. And that group is responsible for the maintenance of terrorist watchlist including the No-Fly List. He has been with the FBI for 25 years and helped create the Terrorist

Screening Center. He has received the Director's Award for outstanding work in his responsibilities.

We welcome you here this morning.

Mr. HEALY. Chairman Conyers, Ranking Member Smith, Members of the Committee, thank you for the opportunity to talk about the Terrorist Screening Center and its role in the interagency watchlisting process.

The attempted terrorist attack on Northwest Flight 253 on Christmas Day highlights the ever-present threat to our homeland. Over the past 7 years, the TSC has played a vital role in its fight against terrorism by integrating the terrorist information from the law enforcement intelligence community into a single database known as the Terrorist Screening Center database, the TSDB, or the terrorist watchlist.

Following Christmas Day, the attempted attack provided an increased intensive scrutiny that has been placed on the requirements to nominate individuals to the watchlist, particularly the No Fly and Selectee list, which are subsets to TSDB. These requirements or standards have evolved over time based on the experience of the watchlisting community and the issuance of additional presidential directives. Throughout this process, the TSC has remained committed to protecting the American people while simultaneously protecting privacy and safeguarding civil liberties.

As our efforts have evolved in response to new threats and intelligence, your support has been vital. Let me tell you about the watchlisting process, but understand the Terrorist Screening Center, the watchlisting process is half of it. We work the watchlisting process to get names out to the screeners. We also—when we encounter the terrorists, we coordinate the operational response with the FBI. But with regard to the watchlisting process, it is best described as a watchlisting enterprise that requires the collaboration between the Intelligence Community, the FBI, NCTC, and TSC.

The NCTC relies upon information provided by the intelligence and law enforcement community. The TSC relies upon information that NCTC provides us where they analyze and provide accurate and credible information and the screening community relies on the TSC to manage the information and efficiently export it to their screening systems. Once an onerous suspected terrorist has been identified and included in the TSDB, the TSC ensures the timely dissemination of that terrorist identity data to our screening partners. The utility of the watchlisting process is greatest when the information is efficiently disseminated to those who could use it most.

TSC has subject matter experts who are composed of experienced analysts and from designated agency representatives who review nominations to determine if they meet the criteria for inclusion into the screening systems. Four major U.S. Government systems support the TSC. The Departments of State, Consular Lookout and support systems are CLASS, and that is for passports and visa screening; the Department of Homeland Security tech system for border and port entry screening; the No Fly Selectee list used by the Transportation Security Administration for air passenger screening; and the FBI's National Crime Information Center of

known or suspected terrorist file for domestic law enforcement encounters.

The criteria for inclusion into each one of these systems is tailored to its mission, its legal authorities, its information technology requirements for each particular agency. Before Christmas Day, the TSC had not received a nomination for Umar Farouk Abdulmutallab and as a result, he was not watchlisted. Following the attempted attack, the President issued a directive for the TSC to review all facts surrounding this incident. As a result, the TSC was given two basic instructions. The first was to conduct a thorough review of the TSDB to determine the current visa status of all known or suspected terrorists beginning with the No-Fly List, and that process has been complete.

The second was to develop recommendations on whether adjustments are needed to the watchlisting nomination criteria, including the biographical and derogatory information for inclusion into TIDE and the TSDB as well as the No Fly and Selectee list. To do so, the TSC convened the Policy Board Working Group with representatives from the National Counterterrorism Center, the Central Intelligence Agency, the National Security Agency, the Federal Bureau of Investigation, the Department of Homeland Security, Department of Defense, Department of Justice, and Department of State to achieve this interagency consensus. That process is underway, and TSC is working with our interagency partners to develop appropriate recommendations to the White House. Also at the direction of the White House and in conjunction with NCTC, the TSC has made some temporary and limited additions to the watchlist to counter the specific threat that was observed on Christmas Day. As a result a threat related target group was identified and individuals from specific high-threat countries already residing in TIDE and TSDB were either upgraded, added to the No Fly or Selectee list, and this was to prevent future attacks.

TSC remains focused on fulfilling its presidential mandates and interagency mandates to share terrorist screening information with our domestic and foreign partners. We have a standing commitment to improve our operational processes, to enhance our human capital and technological capabilities, and to continue to protect the Americans from terrorist threats while protecting privacy and safeguarding civil liberties.

The terrorism watchlisting system is a vital tool in the counterterrorism effort for the United States Government and continues to be.

I look forward to answering any questions you may have. Thank you.

[The prepared statement of Mr. Healy follows:]

PREPARED STATEMENT OF TIMOTHY J. HEALY



TERRORIST SCREENING CENTER

STATEMENT OF

**TIMOTHY J. HEALY
DIRECTOR
TERRORIST SCREENING CENTER
FEDERAL BUREAU OF INVESTIGATION**

BEFORE THE

**COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES**

AT A HEARING ENTITLED

"SHARING AND ANALYZING INFORMATION TO PREVENT TERRORISM"

PRESENTED

March 24, 2010

**Statement of
Timothy J. Healy
Director
Terrorist Screening Center
Federal Bureau of Investigation**

**Before the
Committee on the Judiciary
United States House of Representatives**

**At a Hearing Entitled
“Sharing and Analyzing Information to Prevent Terrorism”**

March 24, 2010

Good morning Chairman Conyers, Ranking Member Smith and members of the Committee. Thank you for the opportunity to discuss the Terrorist Screening Center (TSC) and its role in the interagency watchlisting process.

The attempted terrorist attack on Northwest Flight 253 on December 25, 2009, highlights the ever-present terrorist threat to our homeland. Over the past seven years, the TSC has played a vital role in the fight against terrorism by integrating terrorist information from the law enforcement and intelligence communities into a single database known as the Terrorist Screening Database (TSDB), which populates the various terrorist screening systems used by the Government. Following the Christmas Day attempted attack intense scrutiny has been placed on the requirements to nominate individuals to the watchlist and particularly to the No Fly and Selectee lists, which are subsets of the TSDB. These requirements, or standards, have evolved over time based on the experience of the watchlisting community and the issuance of additional Presidential Directives. Throughout this process, the TSC has remained committed to protecting the American public from terrorist threats while simultaneously protecting privacy and safeguarding civil liberties. As our efforts continue to evolve in response to new threats and intelligence, your support provides us with the tools necessary to continue our mission. Let me begin by telling you about the Terrorist Watchlisting process and how this process related to Umar Farouk Abdulmutallab.

Terrorist Nomination Process

The TSDB, commonly referred to as the Terrorist Watchlist, contains both international and domestic terrorist information. The procedure for submitting information on individuals for inclusion on the Terrorist Watchlist is referred to as the nomination process. The nomination process is the most fundamental and singularly important step in the watchlisting process. It is through this process that individuals are added to the Terrorist Watchlist. Nominations originate from credible information developed by our intelligence and law enforcement partners. These intelligence and law enforcement agencies are referred to as Originators in the watchlisting

community because it is through their work that nominations are developed. Federal departments and agencies submit nominations of known or suspected international terrorists to the NCTC for inclusion in NCTC's Terrorist Identities Datamart Environment (TIDE) database, which is the source of all international terrorist identifier information in the TSDB. NCTC reviews TIDE entries and nominates entries to TSC that include sufficient biographical or biometric identifiers and supporting derogatory information that meet the watchlisting standard described below. Similarly, the FBI collects, stores, and forwards to the TSC information relating to domestic terrorists that may not have connections to international terrorism.

When submitting a nomination to NCTC, an Originator may, but is under no obligation to, submit recommendations regarding specific screening systems the nomination should be exported to (e.g., inclusion on either No Fly or Selectee list). If an Originator submits a nomination without a recommendation, NCTC may make an appropriate recommendation based on the totality of associated information. Recommendations made by NCTC will be passed to the TSC for final disposition.

TSC accepts nominations when they satisfy two requirements. First, the biographic information associated with a nomination must contain sufficient identifying data so that a person being screened can be matched to or disassociated from a watchlisted terrorist. Second, the facts and circumstances pertaining to the nomination must meet the reasonable suspicion standard of review established by terrorist screening Presidential Directives. Reasonable suspicion requires articulable facts which, taken together with rational inferences, reasonably warrant the determination that an individual "is known or suspected to be or has been engaged in conduct constituting, in preparation for, in aid of or related to terrorism and terrorist activities." The reasonable suspicion standard is based on the totality of the circumstances in order to account for the sometimes fragmentary nature of terrorist information. Due weight must be given to the reasonable inferences that a person can draw from the available facts. Mere guesses or inarticulate "hunches" are not enough to constitute reasonable suspicion. A TSC interagency group composed of members from the intelligence and law enforcement communities issued clarifying guidance to the watchlisting community in February 2009.

TSC makes the final decision on whether a person meets the minimum requirements for inclusion into TSDB as a known or suspected terrorist and which screening systems will receive the information about that known or suspected terrorist. It is not uncommon for a nomination to have multiple recommendations throughout the watchlisting process. In the end, however, TSC works with NCTC and the Originators to ensure a nomination is exported to as many screening systems as the nomination information supports.

The watchlisting and nomination process can best be described as a watchlisting enterprise because it requires constant collaboration between the Originators, NCTC, and TSC. NCTC relies upon the information provided by the intelligence and law enforcement community, TSC relies upon NCTC to analyze and provide accurate and credible information, and the screening community relies upon TSC to manage that information and to efficiently export it to their screening systems.

Export to Supported Systems

Once a known or suspected terrorist is identified and included in the TSDB, TSC ensures the timely dissemination of the terrorist identity data to our screening partners. The utility of the watchlisting process is greatest when the information is efficiently disseminated to those who need it the most. The TSC's subject matter experts, who are composed of experienced analysts and designated agency representatives, review nominations to determine whether they meet the criteria for inclusion in the screening systems supported by the TSDB. The four major U.S. Government systems supported by the TSDB are: Department of State's Consular Lookout and Support System (CLASS) for passport and visa screening; Department of Homeland Security's TECS system for border and port of entry screening; the No Fly and Selectee lists used by the Transportation Security Administration for air passenger screening; and the FBI's National Crime and Information Center's Known or Suspected Terrorist File (formerly known as the Violent Gang/Terrorist Organization File (VGTOF)) for domestic law enforcement screening. The criteria for inclusion in each of these systems are tailored to the mission, legal authorities, and information technology requirements of the department or agency that maintains the system. Accordingly, each of these systems contains a different subset of data from TSDB.

The TSDB exports most pertinent to Umar Farouk Abdulmutallab – CLASS, TECS, and the No Fly and Selectee lists– are discussed below.

CLASS

CLASS is a database administered by the Department of State's Bureau of Consular Affairs and is used by consular officers abroad to screen visa applicants for travel to the United States. CLASS accepts nearly all records from the TSDB because minimal biographic information is necessary for visa screening. In other words, given where (overseas) and when (well in advance of travel to the U.S.), the Government has time to work through what can sometimes be less than complete biographical information – time that might not otherwise be feasible in other screening situations like a routine traffic stop or a busy overseas airport where the presence of U.S. officials is often minimal. The Department of State also uses a screening system known as CLASS-PASSPORT to screen applications for U.S. passports.

The TSC aids the Department of State in identifying known or suspected terrorists through two different processes. The first is the Security Advisory Opinion (SAO) process, whereby individuals that are watchlisted could be identified at the time of their visa application to visit the United States. When consular officers process visa applications, checks are run in CLASS to determine whether any derogatory information exists to warrant a visa denial. If it is determined that the visa applicant is a possible match to an individual on the Terrorist Watchlist, the consular officer requests an SAO. The SAO request is forwarded to the TSC, where the Department of State's subject matter experts at the TSC review the associated TSDB and TIDE records to determine whether the visa applicant is in fact the same watchlisted individual. The TSC's only role in this process is to determine if the individual applying for the visa is the same individual on the Terrorist Watchlist. In the case of a positive match, the TSC forwards the information to the Department of State's Visa Office, in the Bureau of Consular Affairs, to prepare an SAO in response to the request. The SAO is then forwarded to the consular officer

adjudicating the visa, who has the authority to issue or deny visa applications. Individuals that are watchlisted at the time of their visa application could be identified through this process.

The second State Department process supported by the TSC is the Visa Revocation Program. The Visa Revocation Program was initiated after 9/11 and is designed to identify individuals who may have received visas prior to that person being identified as a known or suspected terrorist. Every day, the Department of State automatically generates a report that identifies all individuals with a valid visa that could potentially match a person in the TSDB. State officers compare information in CLASS (exported from TSDB), to existing records of visa holders in the Department of State's Consular Consolidated Database (CCD). This report is then evaluated by the State Department experts at the TSC who determine whether there is a positive match to a watchlisted individual. If there is a positive match, then the TIDE record and related derogatory information is made available to the Department of State for review. The Secretary of State holds broad discretionary authority to revoke a visa. Therefore, TSC forwards the information to the Department of State's Visa Office to determine whether to revoke the visa. Individuals that are watchlisted in TSDB after receiving their visas can be identified through this process.

TECS

TECS serves as the Department of Homeland Security's primary lookout system and receives daily exports of TSDB records from the TSC. Additionally, TECS receives non-terrorist related subject records from more than twenty federal agencies, including a wide spectrum of data, and provides alerts for a variety of law enforcement needs. U.S. Customs and Border Protection (CBP) is the principal owner and primary user of TECS and uses the system to screen individuals at air ports, land, and sea ports of entry. Through TECS, CBP screens against the Terrorist Watchlist at all 327 ports of entry and by all of the 15 pre-clearance offices located in Canada, the Caribbean, and Ireland. They also use the Terrorist Watchlist to conduct screening operations at international mail and cargo facilities. Similar to CLASS, TECS accepts nearly all records from the TSDB. For subjects in TSDB, CBP is alerted to their travel when a commercial airline forwards the passenger manifest to CBP using the Advanced Passenger Information System (APIS). APIS enhances border security by providing officers with pre-arrival and departure manifest data on all passengers and crew members.

No Fly and Selectee List

The No Fly and Selectee lists are unique among TSDB subsets in that they are the only subsets within the Terrorist Watchlist that have their own substantive minimum derogatory criteria requirements, which are considerably more stringent than the reasonable suspicion standard required for inclusion in TSDB itself. Following the creation of the TSC in 2003, the Homeland Security Council Deputies Committee established the initial terrorist screening nomination criteria for the No Fly and Selectee lists in October 2004. At that time, the No Fly list consisted of substantive derogatory criteria that focused attention on individuals intending to commit acts of terrorism against civil aviation or the domestic homeland. Over time, that initial criteria proved to be too restrictive. Consequently, in February 2008, the Homeland Security Council Deputies Committee approved additional criteria that served to broaden the scope of

terrorists eligible for the No Fly list. In other words, the criteria to place individuals on the No Fly list has broadened to make the No Fly list more inclusive to respond to additional terrorism threats. The Department of Homeland Security Office of Inspector General recognized the significance of the additional criteria when, in a May 2009 report, it stated, "Major security gaps have been addressed by adding No Fly criteria."¹

For international terrorists, the process to be included on the No Fly list begins, as it does with every nomination, with a federal agency nominating an individual to NCTC for inclusion in TIDE. NCTC analysts review the nomination to ensure it meets nomination criteria and then forward the nomination to the TSC. Analysts at the TSC perform a comprehensive review of the nomination, which includes a review of the derogatory information contained in TIDE and the FBI's Automated Case System. During this process, if there is a reasonable suspicion that the individual is engaging in terrorism or terrorist activity, the terrorist would be added to the TSDB. Placement on the No Fly list requires two components, sufficient biographical information and sufficient derogatory information. If additional information existed to satisfy any of the substantive derogatory criteria and the minimum biographic criteria for the No Fly list, the terrorist's name would be exported to the No Fly list as well. If the analyst reviewing the No Fly nomination determines that there is insufficient information to warrant inclusion on the No Fly list, the nomination is forwarded to the TSA (Office of Intelligence and/or the Federal Air Marshal Service (FAMS)) subject matter experts at the TSC for further analysis and a final recommendation. The TSA subject matter expert will review the nomination and all accessible derogatory information associated with the individual and apply the No Fly and Selectee list criteria to that information. Based upon that review and analysis, the TSA/FAMS subject matter expert will then decide based upon that criteria whether the individual will be included on either the No Fly or Selectee list.

Inclusion on the No Fly list prohibits a potential terrorist from boarding a commercial aircraft that departs or arrives in the United States. It also prohibits an airplane carrying an individual on the No Fly list from transiting United States airspace. The Selectee list is used to provide the individual with a secondary screening. Currently, TSA provides the No Fly and Selectee list to commercial air carriers who are then responsible for passenger prescreening against the No Fly and Selectee lists. With the implementation of the Department of Homeland Security's Secure Flight Program, the U.S. Government will assume the responsibility of passenger prescreening against the No Fly and Selectee lists, which will improve the overall effectiveness of this process.

Actions Since December 25, 2009

Before December 25, 2009, TSC did not receive a nomination to watchlist Umar Farouk Abdulmutallab and, as a result, he was not watchlisted in TSDB. Following the attempted terrorist attack, the President of the United States initiated a review of the facts that permitted Umar Farouk Abdulmutallab to board Northwest Airlines Flight 253. In his January 7, 2010 memorandum, the President concluded that immediate actions must be taken to enhance the security of the American people. These corrective actions were also required to ensure that the

¹ US Department of Homeland Security Office of Inspector General, *Role of the No Fly and Selectee Lists in Securing Commercial Aviation*, OIG-09-64, May 2009.

standards, practices, and business processes that have been in place since the aftermath of 9/11 are appropriately robust to address the evolving terrorist threat facing our Nation in the coming years. As a result, the TSC was given two instructions. The first was to conduct a thorough review of the TSDB and ascertain the current visa status of all known and suspected terrorists, beginning with the No Fly list. That process has now been completed. The second was to develop recommendations on whether adjustments are needed to the watchlisting Nominations Guidance, including biographic and derogatory criteria for inclusion in TIDE and TSDB, as well as the No Fly and Selectee lists. To do so, TSC convened its Policy Board Working Group with representation from NCTC, DHS, CIA, NSA, DOD, DOJ, DOS, and NSC to achieve interagency consensus. That process is underway and TSC is working with its interagency partners to develop appropriate recommendations for consideration by the President.

As of yet, however, there have been no formal changes to watchlisting criteria, including the criteria for inclusion on the No Fly list, since February 2008 when those criteria were last expanded. At the direction of the White House and in conjunction with NCTC, the TSC has made some temporary and limited additions to the watchlist to counter the specific terrorist threat observed on December 25, 2009. As a result, a threat-related target group was identified and individuals from specific high-threat countries already residing in TIDE or TSDB were added to the No Fly and Selectee lists, or upgraded to TSDB if necessary, to prevent future attacks.

Conclusion

As the investigation into the events that allowed Umar Farouk Abdulmutallab to board Flight 253 continues, the TSC remains focused on fulfilling its Presidential and interagency mandates to share terrorist screening information with our domestic and foreign partners. We have a standing commitment to improve our operational processes, to enhance our human capital and technological capabilities, and to continue to protect Americans from terrorist threats while protecting privacy and safeguarding their civil liberties. Terrorist Watchlisting has been a vital tool in the counterterrorism efforts of the United States Government and will continue to be so in the future. Chairman Conyers, Ranking Member Smith and members of the Committee, thank you for the opportunity to address this Committee. I look forward to answering your questions.

Mr. CONYERS. Our next witness is Patricia Cogswell, a lawyer, who is Acting Deputy Assistant Secretary for the Office of Policy at the Department of Homeland Security. Most of her career has been spent at the Department of Homeland Security and the INS before that, and she has served as Executive Director of the Department of Homeland Security Screening. Welcome.

TESTIMONY OF PATRICIA COGSWELL, ACTING DEPUTY ASSISTANT SECRETARY, OFFICE OF POLICY, DEPARTMENT OF HOMELAND SECURITY

Ms. COGSWELL. Chairman Conyers, Congressman Smith, and Members of the Committee, thank you very much for this opportunity to testify on sharing and analyzing of information to prevent terrorism.

DHS has a number of screening programs in place and works closely with foreign governments and air carriers in our efforts to strengthen global aviation security. Information sharing and analysis plays a critical role in these programs.

This Administration and all of us here today are determined to find and fix the vulnerabilities that allowed Umar Farouk Abdulmutallab to board a U.S.-bound plane and prevent such breaches in the future. Today I will describe the screening conducted in the aviation environment, including the changes DHS has put in place since December 25, and how we are moving forward to further bolster aviation security.

First, most noncitizens need a visa, or if traveling under the Visa Waiver Program, a travel authorization issued through the DHS electronic system for travel authorization, or ESTA, prior to travel to the United States. DHS screens each ESTA applicant to assess whether he or she could pose a risk to the United States, including potential links to terrorism. At certain embassies and consulates, DHS has also placed Visa security program personnel to assist the State Department in identifying visa applicants who may pose a security concern.

DHS also conducts predeparture screening in partnership with the airline industry. Individuals on the No-Fly List should not receive a boarding pass. Individuals on the Selectee List must go through additional screening before boarding an aircraft.

Through the implementation of the Secure Flight program which is underway now, DHS is checking passenger manifests against these lists directly, a job previously performed by the air carriers. For international travel, carriers are also required to provide DHS with access to certain passenger reservation information, basic identifying and itinerary information referred to as Passenger Name Record, 72 hours prior to departure to the U.S.

Carriers must then transmit their flight manifest containing complete and standardized information on a traveler, as shown on their Official Travel Document, through the Advanced Passenger Information System no less than 30 minutes before the flight. DHS uses both of these data feeds to be able to do risk assessments and conduct checks against the Known or Suspected Terrorist Watch List, lost or stolen passport information, prior immigration or Customs violations, visa revocations, and other records such as State Department records indicating potential terrorism concern.

If the flight departs from an airport where DHS has an immigration and advisory program officer station, the IAP officers make use of this information to interact with individuals, and can make no-board recommendations to the carriers or host governments. In non-IAP locations, DHS will directly contact the airline, when appropriate, to recommend a person not board a flight. This is a change since December 25.

The next step in the process is the physical screening of passengers, their accessible properties, their checked baggage, by utilizing a combination of x-ray systems, walk-through metal detectors, full body pat-downs, explosive trace detection equipment, trained canines, advanced imaging technology, and behavioral detection, depending on the location. In the U.S., DHS conducts such screening. Overseas, the screening is conducted by the foreign government, the air carriers, or their respected airport authority.

Since the 25th, DHS has put in place security directives and emergency amendments for increased use of enhanced screening technologies and threat-based and random screening procedures. These measures have been implemented with the extraordinary cooperation from our global aviation partners.

DHS also conducts security assessments in accordance with standards set by the International Civil Aviation Organization at approximately 300 foreign airports. If an airport does not meet these standards, DHS works with the appropriate host government authorities to raise the airport security posture.

In addition to all these immediate activities we have already taken to further enhance our processes, we are also taking action to address the systemic vulnerabilities highlighted by this failed attack. As announced by the President and Secretary Napolitano, as part of the overall U.S. Government approach, DHS is pursuing five objectives to enhance the protection of air travel through acts of terrorism. These include: Working with our interagency partners to reevaluate and modify the criteria and process used to create the Terrorist Watch List; establishing a partnership on aviation security with the Department of Energy and its national labs to develop future technologies that deter and disrupt threats; accelerating the deployment of advanced imaging technology as well as increasing our use of explosive trained canines and explosive detection equipment, augmenting law enforcement aviation, and working with our partners to strengthen international security measures and standards for aviation security.

While we address the vulnerabilities associated with the December 25 attempted bombing, we must also recognize the evolving threats posed by terrorists and take swift and appropriate action to ensure that our layers of security continue to evolve in order to defeat them.

Thank you for this opportunity to testify. I will be pleased to answer any questions.

Mr. CONYERS. Thank you.

[The prepared statement of Ms. Cogswell follows:]

PREPARED STATEMENT OF PATRICIA COGSWELL



**Statement of Patricia Cogswell
Deputy Assistant Secretary – Policy (Acting)**

U.S. Department of Homeland Security

Before

**United States House
Committee on the Judiciary**

on

Sharing and Analyzing Information to Prevent Terrorism

Wednesday, March 24, 2010

**2141 Rayburn House Office Building
Washington DC**

Sharing and Analyzing Information to Prevent Terrorism
Patricia Cogswell Testimony

Chairman Conyers, Congressman Smith, and members of the Committee: Thank you for this opportunity to testify on sharing and analyzing information to prevent terrorism

The attempted attack on December 25, 2009, was a powerful illustration that terrorists will go to great lengths to try to defeat the security measures that have been put in place since September 11, 2001. The Department of Homeland Security (DHS or the Department), along with our interagency partners, 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 or bound for the United States, or, in appropriate cases, to identify travelers for additional screening. We work with foreign governments and with air carriers to strengthen global air travel security by advising them on security measures and on which travelers may pose 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 attempted 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 address these vulnerabilities is well underway, with cooperation among DHS, the Department of State, the Department of Justice, the Intelligence Community, and our international partners, among others. As a consumer of terrorist watchlist information, DHS 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 December 25 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 to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities. In addition, other countries and the private sector – especially the air carriers themselves – have important roles to play.

DHS has several screening programs in place to prevent individuals with terrorist ties from boarding flights that are traveling to or within the United States or, in appropriate cases, to identify them for additional screening. Specifically, DHS:

- uses information in the Terrorist Screening Database (TSDB), managed by the Terrorist Screening Center (TSC), as well as other information provided by law enforcement and 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;
- works with foreign governments, international and regional organizations, and airlines to design, improve, and implement security standards worldwide;
- conducts routine checks against Interpol databases on wanted persons and lost or stolen passports for international travelers traveling to the United States; and
- performs checkpoint screening 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

¹ The 36 countries in the Visa Waiver Program are: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, 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).

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 a visa, travel authorization, and a boarding pass. To apply for entry to the United States prior to boarding flights bound for the United States or arriving at a U.S. port of entry, most foreign nationals need a visa issued at a U.S. embassy or consulate or, if traveling under the VWP, a VWP travel authorization issued through the Enhanced System for Travel Authorization (ESTA).²

Issuing visas is the responsibility of the Department of State. At certain embassies and consulates the U.S. Immigration and Customs Enforcement (ICE) has stationed Visa Security Program personnel to assist State Department personnel in identifying visa applicants who may present a security threat or national security concern. 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. DHS screens each ESTA applicant to assess whether he or she could pose a risk to the United States or its citizens, including possible links to terrorism. DHS has transitioned to enforced ESTA compliance where air carriers confirm that VWP travelers have an approved ESTA prior to boarding a flight to the United States. DHS also checks to make

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.

sure that the person's visa has not been denied or revoked. If it has, DHS will notify the carrier to prevent boarding.

The Department works closely with other federal agencies and our foreign partners to prevent possible terrorists from boarding aircraft bound for the United States. 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, to determine who may board, who requires additional screening, 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 prior to boarding an aircraft.

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. Under the Secure Flight program, DHS will conduct these checks directly. Implementation is well underway. DHS expects to complete the transition for domestic flights later this spring and complete the transition for international flights by the end of this calendar 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.

For international travel to the United States, DHS also uses the Passenger Name Record information (PNR), the Advanced Passenger Information System (APIS), and the Immigration Advisory Program (IAP) to assess passengers' level of risk and, when necessary, flag them for further inspection. PNR data, obtained from the airline reservations systems up to 72 hours before travel, 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, also referred to as "manifest data," which carriers are required to provide to DHS at least 30 minutes before departure, contains important identifying information that may not be included in PNR data, including verified identity and travel document information, such as a traveler's complete name, date of birth, citizenship, travel document number, and document's country of issuance. 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 stolen and lost travel documents 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. IAP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may be deemed inadmissible upon arrival at a U.S. port of entry, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

Checkpoint screenings and in-flight security

A further 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 either the foreign government, air carriers, or the respective airport authority—depending on the location—as required for compliance with the International Civil Aviation Organization (ICAO) and TSA requirements for flights to the United States.

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 using a variety of 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 to screen checked baggage, Bomb Appraisal Officers, and Behavior Detection Officers – at both 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 tools that enhance our abilities to detect threats.

In an effort to enhance international screening standards, TSA conducts security assessments in accordance with security standards established by 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 effectively carry out these standards, TSA works with the appropriate host government authorities to rectify the deficiencies and raise the airport's security to an acceptable level. Ultimately, it is the foreign government that must work to address any security deficiencies. In long-term or significant circumstances of non-compliance with international standards, TSA may recommend suspension of flight service between these airports and the United States. In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each foreign airport to ensure compliance with TSA regulations, standards, and security directives. Should air carrier security deficiencies exist, TSA works with the air carrier to achieve compliance. If an airport is located within one of the 36 VWP countries, DHS conducts additional audits and inspections as part of the statutorily mandated VWP designation and review process.

To provide immediate response on flights, TSA's Federal Air Marshal Service (FAMS) deploys air marshals 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 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 December 25 Attempted Attack

The facts of the December 25 attempted bombing are well established and were relayed in the report on the incident that the President released on Jan. 7, 2010. On Dec. 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 Dec. 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 a security contractor at Schiphol, when transiting through Amsterdam and boarded Northwest Flight 253 to Detroit, and presented a valid Nigerian passport with a U.S. visa. Abdulmutallab was not on the No-Fly or Selectee Lists. Accordingly, the air carrier was not alerted to prevent him from boarding the flight or to require 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 and the other passengers' 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.

Immediate DHS response

The attack on board the flight failed in no small part due to the brave actions of the crew and passengers aboard the plane. 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 United States, which mandated enhanced screening prior to departure and additional security measures during flight.

Shortly after the attempted bombing, TSA issued a new Security Directive and Emergency Amendment, which put in place new screening requirements that increased the use of enhanced screening technologies and mandated threat-based and random additional screening for passengers on U.S. bound international flights. These measures have been implemented with extraordinary cooperation from our global aviation partners, both in government and industry.

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 22 countries were aboard Flight 253. Accordingly, DHS has embarked upon an aggressive international program designed to raise international standards for airports and air safety. Since January, Secretary Napolitano has participated in three international meetings hosted, respectively, by the Spanish Presidency of the European Union, Mexico, and Japan, to build consensus on strengthening global aviation security, to bolster international aviation security measures and standards, and identify specific steps that nations can take individually and collectively to protect all passengers. These meetings have resulted in joint declarations to strengthen the international civil aviation system among the participating countries. In the near future, the Secretary will travel to the Africa and the Middle East to meet with countries in those regions on the same issues. Additionally, DHS, in cooperation with the Department of State, is leveraging the G-8, including by assuming the chair of the Transportation Security Subgroup; the 5 Countries Conference; Asia-Pacific Economic Cooperation (APEC); ICAO; and other established international fora to press for enhanced security standards, information sharing, and screening measures throughout the entire international aviation system.

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 Jan. 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 is pursuing these five objectives to enhance the protection of air travel from acts of terrorism.

First, DHS is working with our interagency partners to re-evaluate and modify the criteria and process used to create the 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. As a consumer of this intelligence and the operator of programs that rely on these lists, the Department is working closely with our partners in the Intelligence Community to make clear the kind of information needed to ensure the watchlist system is an effective tool for DHS.

Second, DHS is establishing 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 is accelerating deployment of Advanced Imaging Technology to provide enhanced 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. At the end of February, TSA had 40 machines deployed at nineteen airports throughout the United States. Earlier this month, , TSA began deploying 150 backscatter imaging technology units purchased with American Recovery and Reinvestment Act (ARRA) funds. TSA plans to deploy a total of approximately 450 imaging technology units in 2010. TSA continues to work to ensure that Advanced Imaging Technology is implemented in a way that protects travelers' privacy, civil rights and civil liberties. DHS will also seek to increase our assets in the area of explosives-trained canines, explosives detection equipment, and other security personnel.

Fourth, DHS is strengthening the presence and capacity of law enforcement in the aviation environment. As an interim measure, we are deploying law enforcement officers from across DHS to augment Federal Air Marshals to increase security aboard U.S.-flagged 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 is working 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 determination to safeguard the privacy, civil rights, and civil liberties of travelers.

Conclusion

The attempted attack on December 25 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 swift and appropriate 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.

Chairman Conyers, Congressman Smith, and members of the Committee: Thank you for this opportunity to testify. I would be pleased to answer any questions.



Mr. CONYERS. Mr. Patrick Kennedy, Under Secretary for Management at the Department of State, has been a career Foreign Service officer for more than 30 years. And in addition to other responsibilities, heads the Bureau of Consular Affairs, which issues visas overseas. Welcome.

**TESTIMONY OF THE HONORABLE PATRICK F. KENNEDY,
UNDER SECRETARY FOR MANAGEMENT, U.S. DEPARTMENT
OF STATE**

Mr. KENNEDY. Thank you very much, Chairman Conyers, Ranking Member Smith, distinguished Members of the Committee.

After the attempted bombing of Flight 253, Secretary Clinton stated that we are all looking hard at what did happen in order to improve our procedures, to avoid human errors, mistakes, oversights of any kinds, and we are going to be working hard with the rest of the Administration to improve every aspect of our efforts. This introspective review and the concurrent interagency review are ongoing. We appreciate this Committee's interest and support as we continue the review process.

We recognize fully the gravity we face, and we consider ourselves the first line of defense in our national security efforts. We acknowledge that processes need to be improved, and here are the steps we have already taken.

The Department of State misspelled Umar Farouk Abdulmutallab's name in our Visa VIPER's report; as a result, we did not have the information about his current U.S. visa. To prevent this from occurring again, we have instituted new procedures to ensure comprehensive visa information is included in all Visa VIPER reporting. This will highlight the visa application and issuance material also available in the data already shared with our national security partners.

We are also reevaluating the procedures and criteria used to revoke visas. The State Department has broad and flexible authority in this matter. Since 2001, we have revoked 57,000 visas for a variety of reasons, including over 2,800 for suspected links to terrorism.

New watchlisting information is continuously checked against the database of previously issued visas. We can and do revoke visas in circumstances where an immediate threat is recognized. We can and do revoke visas at the point that people are seeking to board an aircraft, preventing their boarding. In coordination with the National Targeting Center, we revoke visas under these circumstances almost daily. We have standardizing procedures for triggering revocations in the field, and we are adding revocation recommendations to the Visa VIPER report. Visa VIPER reports received since December contain this fuller information.

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. Although not the case here, in those circumstances, the individual is under active investigation, and our revocation would have disclosed the United States Government's interest in that individual and ended our law en-

forcement colleague's ability to quietly pursue the case and to identify the terrorist plans and co-conspirators.

We will continue to closely coordinate visa revocation processes with our intelligence and law enforcement partners while also constantly make enhancements to the security and integrity of the visa process. Information sharing and coordinated action are foundations of the border security systems put in place since 9/11, and they remain sound principles.

The Department has close and productive relationships with our interagency partners, particularly within the Department of Homeland Security. The State Department brings unique assets and capabilities to this partnership. Our global presence, international expertise, and highly trained and language-qualified personnel provide a singular advantage in supporting the visa function throughout the world. We developed and implemented an intensive screening process requiring personal interviews and supported by a sophisticated global information network. Our front line of border security has visa offices in virtually every country in the world, and they are staffed by highly trained, multilingual, culturally aware personnel of the Department of State. We support them with the latest technology and access to information and screening tools. We are introducing a new generation of visa software to more efficiently manage our growing mission and the increasing amounts of data we do handle.

We are pioneers in the use of biometrics, a leader in the use of facial recognition, and we are expanding into the field of high risk screening. We have and will continue to automate processes to reduce the possibility of human error.

The State Department makes all our visa information available to other involved agencies, giving them access to over 13 years of data. We introduced online visa applications in 2009, which expanded our data collection tenfold and provides new information that is readily available for analysis by State and other agencies. This system will be rolled out worldwide by the end of this fiscal year.

We have embraced a layered approach to border security screening which results in multiple agencies having an opportunity to review information, and requires separate reviews at both the visa and admission stage. No visa is issued, no visa is issued without it being run through security checks against our partners' database. We screen applicants' fingerprints against U.S. databases, and we run our facial recognition software against a photo array provided by our law enforcement and intelligence colleagues as well.

At the same time, we believe that U.S. interests and legitimate travel, trade promotion, and educational exchanges are not in opposition to our border security agenda. In fact, the United States must strive to meet both goals to guarantee our long-term security. Again, the multi-agency team effort, to which each agency brings its particular strengths and expertise, results in a more robust and secure process, a process based upon broadly shared information.

We remain fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information. We fully recognize that we are not perfect in our reporting in con-

nection with this incident; however, we are working and will continue to work not only to address shortcomings, but to continually enhance our border security screening capabilities and the contributions we make to the interagency effort.

Thank you very much, Mr. Chairman. I would be pleased to take any questions that you or your colleagues might have.

[The prepared statement of Mr. Kennedy follows:]

PREPARED STATEMENT OF THE HONORABLE PATRICK F. KENNEDY



DEPARTMENT OF STATE

STATEMENT
OF
PATRICK F. KENNEDY

UNDER SECRETARY OF STATE FOR MANAGEMENT,
DEPARTMENT OF STATE

BEFORE THE
HOUSE OF REPRESENTATIVES COMMITTEE ON THE
JUDICIARY

HEARING
ON
SHARING AND ANALYZING INFORMATION TO PREVENT
TERRORISM

MARCH 24, 2010

Chairman Conyers, Ranking Member Smith and distinguished Members of the Committee, thank you for the opportunity to address you today. As a result of the 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 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, the Office of the Coordinator for Counter Terrorism, and the Bureau of Intelligence and Research that add valuable law enforcement and investigative component and intelligence analysis to our capabilities. We 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. Additional reporting on this case carried the correct spelling, with both reports reaching the same file in Washington.

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) in Visas Vipers cables. This guidance includes specific methods to comprehensively and intensively search the database of visa records so that all pertinent information is obtained. I can confirm that these new requirements are being followed in the Visas Viper cables submitted since December.

In addition to this change in standard procedures on searching visa records, we immediately began working to refine the capability of our current systems. For visa applications, 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 search capability has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We are using this significant experience with search mechanisms for visa applications to improve the systems for checking our records of visas issued.

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 Consular Consolidated 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 address urgent requests, such as when the person is about to board a plane. In those circumstances, the State Department can use its authority to prudentially revoke the visa and prevent boarding.

Since the Presidentially-ordered Security Review, individuals have been added to the Terrorist Screening Database, No Fly, and Selectee lists to counter the specific vulnerability observed on December 25, 2009. The number of revocations has increased substantially as a result. 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 visa officers have 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 57,000 visas for a variety of reasons, including over 2,800 for suspected links to terrorism. We have been actively using this authority as we perform internal reviews of our data against updated watchlist information provided by partner agencies. For example, we are re-examining information in our CLASS database regarding individuals with potential connections to terrorist activity or support for such activity. We are reviewing all previous Visas Viper submissions and 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 identified cases for revocation and we 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 with the desired goal, that no person who may pose a threat to our security, holds a valid visa.

Revocation is an important tool in our border security arsenal. We will use revocation authority prior to interagency consultation in circumstances where we believe there is an immediate threat. 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 over 2 million visas out of some 8 million applications 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 ever issued without it being run through security checks against our partners' data, including screening 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 (VSUs) 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 (VSUs) established abroad and with domestic elements of DHS, such as CBP's National Targeting Center. VSUs currently operate at 14 visa adjudicating posts in 12 countries. Since January 19, 2010, we received requests from DHS's Immigration and Customs Enforcement to open four additional VSUs and to augment staff at two existing VSUs. The Chiefs of Mission at those respective posts approved the four new VSUs and one request for expansion; with one request for expansion pending.

DHS has 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. Other agencies have 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 Departments of Defense (DOD) and Commerce, and the FBI 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 have 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 integrated 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. While national security is paramount, the issuance and refusal of visas has a direct impact on foreign relations as well. 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 75 Assistant Regional Security Officer Investigators assigned to 73 consular sections overseas specifically devoted to maintaining the integrity of the process. This year, the Bureau of Diplomatic Security approved up to 48 additional investigator positions to work in consular sections overseas.

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.

Mr. CONYERS. I want to sincerely thank all the witnesses and ask Subcommittee Chairman Jerry Nadler to begin the questioning.

Mr. NADLER. Thank you very much. I am not sure which witness I will address the first two questions to.

The Christmas bomb plot obviously exposed certain longstanding gaps in how we use and analyze threat information, and we are told you are working to fix these.

What are you doing to identify any other gaps, ones that weren't revealed by this plot, but maybe the next plot? In other words, ones you haven't thought about yet.

Mr. KENNEDY. If I could, sir. One of the things that we are doing is, in the past, the State Department received a visa application, and then we ran the individual's name and other particulars against a 27-million-count database that we received from our colleagues and information that we have developed ourselves. We have turned that into now—and we will have, by the end of this fiscal year—a completely automated process where the visa application will come into us electronically. We are then going to push that visa application information immediately to all of our partners in the Intelligence Community and law enforcement community so they can look at that data in real-time, as we are also looking at it, to see if there is information they may have in the broader fields of information submitted by the applicant, not just the name, date and place of birth, passport number, and other data. So our goal is to push off all the information we can to our colleagues and enable them to provide us with more and fuller information that they might have in their possession so we can make decisions. We already reject almost 2 million visa applicants a year, and we want to make sure that we reject everyone who would threaten our national security.

Mr. NADLER. Thank you. As long as you added those last few words.

After the Christmas bomb plot, the Administration announced that travel to 14 nations would be subjected to heightened scrutiny. Most of these 14 nations are Muslim nations. Some have said that terrorists will be able to plan their travel to avoid these countries, but innocent travelers will not. Why do you think this is not the case, and how does this really increase our national security? Some have said this is simply religious profiling. How does this really increase our national security?

Ms. COGSWELL. Thank you very much. I would just like to note that the 14 countries, we do not consider the objective of the 14 countries to be a permanent list of countries. It was a way to have a quick mechanism in response to the immediate threat. They were compiled through a list of individual countries who are currently on the list of State Sponsors of Terrorism, state havens, or otherwise linked to the current threat streams that are being tracked.

As I noted, we at DHS are going to continue to evaluate these designations and we will update them when appropriate. I think it is important to note that it is unrelated to religion; it is focused on individuals who are traveling to, from, or through countries where, again, we have noted that there is a safe haven, a state sponsor of terrorism, or something linked to the current threat stream.

Mr. NADLER. Thank you. Let me ask you a different question. Everything we have heard thus far is about information linked to visas or air travel. What about train travel within this country? What are we doing to make train travel safe? I take the train every week from New York to Washington and back. It is a great convenience that I don't have to be screened, I am very happy about that. On the other hand, I could bring almost anything I wanted onto that train and no one would be the wiser.

Ms. COGSWELL. Thank you very much. We do recognize very much that aviation tends to occupy an awful lot of our attention and resources. This is in part because of the continuing threat streams that we are seeing. At the same time, we very much do recognize there are threats to other modes of transportation in particular. Congress has directed specific legislation also around areas such as maritime ports for us to follow. These are very much a focus of ours, and something we do look into very closely in terms of what are the appropriate measures to take in each of these environments to work through, what is a sustainable process? Perhaps it might be appropriate to set up a follow-on conversation to talk more specifically.

Mr. NADLER. Let me just ask one further question on that, since you brought it up—I was going to ask it anyway, it was my next question in any event. I was the chief author of the legislation 3 years ago to require that every container be inspected and sealed before it is put on a ship bound for the United States in the foreign port, given that it would be a little late to find a nuclear device while being inspected in an American port.

The Bush administration, as far as I could tell, made no effort to implement that. The Obama administration, as far as I can tell, has made no effort to implement that legislation. It has told us that it will not be able to do it within the time frame—although the legislation provides for waivers up to a certain point—but I see no evidence that the Administration is making any attempt actually to implement that legislation. Could you tell us differently?

Ms. COGSWELL. I would just like to note that we have got several programs in this arena, Container Security Initiative being a key one. It is an environment where we work both with the various individuals here in the United States and overseas.

Mr. NADLER. Excuse me. Let me stop you right there. There is a fundamental difference. On the one hand, there are people in the security field under both Administrations who have told us that it is impractical to inspect every container. We will look at threats, we will inspect five or 6 percent of the containers based on threat analysis and so forth. On the other hand, Congress made the judgment—and the President signed the bill—that is not sufficient, that we want to inspect every container, we want to get to that capability in a reasonable period of time. So my question is, what is the Administration doing to implement that determination?

Ms. COGSWELL. Sir, I cannot answer that question to your satisfaction. As you have stated, the Administration's position is that we are focusing on the risk procedure. And given the resources, we are—

Mr. NADLER. Surely you are not telling us you are ignoring the congressional directive?

Ms. COGSWELL. Of course not, sir. I would not say that.

Mr. NADLER. But you would say what?

Ms. COGSWELL. I would say that the Administration is working very hard to implement in a way that it believes is risk based and appropriate to the threat, understanding that the direction is 100 percent.

Mr. NADLER. Okay, thank you.

Mr. CONYERS. Thank you, Jerry Nadler.

Lamar Smith.

Mr. SMITH. Thank you, Mr. Chairman.

I actually have several questions about the same subject, and I think the questions will go to Mr. Kennedy and Ms. Cogswell. This is the subject of the 2,800 individuals with suspected ties to terrorism whose visas have been revoked since 2001, I think that is around 350 a year. Mr. Kennedy, the first question is, how many of these individuals are still in the country, to your knowledge? These are the individuals with ties to terrorism whose visas we revoked.

Mr. KENNEDY. Sir, who is in this country or not, I would have to defer to my colleagues at DHS. They keep the records of individuals who are or are not in the United States.

Mr. SMITH. Ms. Cogswell.

Ms. COGSWELL. We have analyzed all those records and forwarded out to certain individuals to the fields for investigation. If possible, perhaps we can follow up with your staff for a more restricted briefing on the results of that analysis.

Mr. SMITH. Why can't you tell me now? Do you consider that to be classified information?

Ms. COGSWELL. We consider the results related to how the reviews are going to be restricted, yes.

Mr. SMITH. I am not asking about how the reviews are going, I am just wondering how many are still in the country.

Ms. COGSWELL. I cannot answer that at this time; I just don't have the number with me.

Mr. SMITH. Can you get it from staff in the time we are in the hearing today?

Ms. COGSWELL. We can.

Mr. SMITH. How many of these individuals have appealed their revocation of the visa? Is that a number you need to get as well?

Ms. COGSWELL. We would not have that.

Mr. SMITH. Who would have that?

Mr. KENNEDY. Mr. Smith, if I could, we would not entertain an appeal for revocation of visa. We would not reinstate. Once a visa is revoked, it is revoked. The individual is free to apply for a new visa, but after that circumstance—

Mr. SMITH. How many of these individuals then have been removed, deported?

Mr. KENNEDY. Again, sir, that is a question for Homeland Security.

Mr. SMITH. Okay. Ms. Cogswell, my other question was, of the individuals with suspected ties to terrorists whose visas have been revoked, how many of those individuals have actually been removed from the country?

Ms. COGSWELL. I would need to follow up, sir, I am not aware at this time. We were evaluating how many have stayed and then referring those for investigation—

Mr. SMITH. Of those 2,800, how many have been removed from the country? You don't know that either?

Ms. COGSWELL. It is important to note that of most of those, very few were even in the country in the first place.

Mr. SMITH. And the ones who were in the country, you are going to get that for me later, and then how many were removed of that figure?

Ms. COGSWELL. Sir, right now we are in the process right now, so I don't believe of the very small number who are still here, we have not reached that stage yet in the investigation, but I will need to follow up.

Mr. SMITH. And what are you doing to try and find these individuals and remove them?

Ms. COGSWELL. Sir, these have been forwarded out to the Immigration and Customs Enforcement, ICE agents, to evaluate the information and go after and investigate these in conjunction with the FBI's part of the terrorism review.

Mr. SMITH. And the earlier figures you can give me in the next few minutes from staff you think?

Ms. COGSWELL. I will attempt to do so; otherwise, we will follow up.

Mr. SMITH. I am sure your staff will be able to do that. Thanks.

Mr. Healy, a couple of questions for you. The first is, in regard to the watchlist system, should the system be changed so that if we had the equivalent information again that we had about Abdulmutallab, should we change the system so that that would trigger action that was not triggered this time? Or is the failure that we had the information, we just didn't have the right spelling, and if we had had the right spelling, that would have triggered action? Which is the case?

Mr. HEALY. Congressman, as I mentioned, we are in the process of reviewing the issues that occurred as a result of the Christmas day event. Some of those, not necessarily in terms of the watchlisting standard, but more so in terms of the implementation and how that process worked.

Mr. SMITH. It was an implementation problem, not a standards problem?

Mr. HEALY. That is one of the things that we have taken a look at and we are leaning toward. There are issues, as you have mentioned and some of the Congressman here have mentioned, regarding the ability to credit Dr. Mutallab when he first came into the embassy. There was specific implementation regarding sole source, and it has to be credited, you have to define credibility. We are recommending that with that particular case, we leave it up to the Consular Affairs to assess the credibility of the source in situations like that. Based on his standing with the community, he would be deemed credible, and that would move up as well. Things like that we are taking a look at and making recommendations.

Mr. SMITH. Trying to decide whether a human error or a lack of standards, or standards that might be too high and we might need

to adjust the standards to trigger action next time; that is what you are studying.

Mr. HEALY. Based on the President's report, they talked about the difficulty in connecting the dots. As my colleague, Russ, has mentioned, there is a lot of noise out there. There was a result of, we believe, one of connecting the dots issue—

Mr. SMITH. As opposed to standards.

Mr. HEALY. As opposed to standards. But we are looking at the standards and we are making some adjustments or recommendations for the implementation of that, sir?

Mr. SMITH. Mr. Healy, a final question. You mentioned a minute ago in your testimony that you conducted a thorough review of the Terrorist Screening database to ascertain the current visa status of all known or suspected terrorists. What are the results of that?

Mr. HEALY. We identify those individuals and refer to our State colleagues. I believe most of those have been revoked. They are under review right now. There were approximately 1,100 individuals that had received visas that were in the Terrorist Screening Center database, and that information was coordinated with our Department of State colleagues.

Mr. SMITH. Okay. And do we know where those individuals are? Have they been removed or not? That gets back to the same question I was asking Ms. Cogswell.

Ms. COGSWELL. That is the number I asked for.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. CONYERS. Thank you.

Bobby Scott, Chairman of the Subcommittee on Crime.

Mr. SCOTT. Thank you, Mr. Chairman.

Just a brief question. We are getting all this information, some of it in foreign languages; do we have enough foreign language people on staff to listen to some of these wiretaps, or do we need more staff knowledgeable in foreign languages?

Mr. TRAVERS. I would just say, sir, that foreign language training has been an issue for the community about as long as I have been in that community. We have obviously spent a great deal of money focused on many of the difficult languages in particular, but at the same time, I think everyone would acknowledge that there are shortages in a number of languages.

Mr. SCOTT. Have you asked for us to do anything in response, like more funding, more scholarships, more courses?

Mr. TRAVERS. From NCTC's perspective, no, sir. I would have to check with ODNI and the various organizations—

Mr. SCOTT. Well, you recognize the shortage, and you haven't recommended that we do anything about it.

Mr. TRAVERS. It wouldn't be NCTC to make that recommendation, sir. I can check with the broader community and get back to you on what requests have been made.

Mr. SCOTT. Ms. Cogswell, if the Christmas bomber had been on the extra search list, would the extra search have revealed his plan?

Ms. COGSWELL. Sir, when you say "extra search" list, you mean the changes that we have made since December?

Mr. SCOTT. Well, you have a No-Fly List and you have a selectee list; and selectee means you have got extra screening.

Ms. COGSWELL. Correct.

Mr. SCOTT. If you had been given extra screening, could we have revealed the threat?

Ms. COGSWELL. If he would have been given extra screening, there would have been a greater likelihood we would have found the threat. As has been noted, given where we believe or how he was transporting the material—if, for example, it was in his carry-on baggage and his baggage was hand searched, it is highly likely it would have been found. Given if he was holding it where it eventually was detonated, that takes a very personal type of pat-down in order to find that. That is something since the 25th we have been focusing very much with our foreign partners on, as well understanding how can you best find these types of threats.

Mr. SCOTT. Would the x-ray machine, the see-through thing, would that have revealed it?

Ms. COGSWELL. Thank you. This is an important distinction from what has been our current process. Under a traditional magnetometer and x-ray machine, it is primarily looking for metal. The advanced imaging technology has the benefit in that it identifies any foreign material by the fact that it shows up as an anomalous object on the body as a way to identify material. Again, given the location, we cannot say with certainty that it would have found it, but it is a significant improvement enhancement over what we have today.

Mr. SCOTT. Does that mean he could have gotten it through anyway?

Ms. COGSWELL. In all of these circumstances we say that we can never say any specific layer and any specific technology is 100 percent solution. We do also say this is why we must have the various layers so that you would have both these types of advantaged technologies in order to scan as well as things like behavior detection or canines so that you have the best likelihood of identifying these threats rather than relying on one single aspect.

Mr. SCOTT. When we started the debate on the Department of Homeland Security, the problem we were trying to solve was the fact that the Department of Justice had information, CIA had information, Department of Defense and Department of State all had information but they weren't talking to each other. Our solution for four people not talking to each other was to establish a fifth organization in which none of the other four landed. So now you have five people not talking to each other. Can you explain to me how the Department of Homeland Security has actually helped things?

Ms. COGSWELL. I would like to start out by noting that the Department of Homeland Security was made up of 22 separate agencies who were originally part of that larger group. So I would say that, while it does look like a fifth new agency, all of the components within DHS—such as Customs and Border Protection, Immigration and Customs Enforcement, the Secret Service, all were very much part and parcel of this process well before these events, so that it is important to understand that these relationships, these processes have really advanced and improved. We have streamlined many of them, and very much inculcated a number of these to enhance our screening processes since that time.

Mr. KENNEDY. Sir, can I add something to that?

Prior to 9/11, the State Department had a screening database that we used before we issued visas, somewhere on the order of 9 or 10 million hits, and obviously that number has grown in the last years. Right now, sir, before we issue a visa, we run that database against 27 million possible individuals of concern. It is a 400 percent increase since 9/11. Five million of those records come from the Department of Homeland Security, 11 million of those records come from the FBI, others come from elsewhere in the community.

We also now have full access to the FBI's fingerprint database, other material provided to us from elsewhere, including Homeland Security. When we run our facial recognition software, that is 83 million facial images, including material received from throughout the law enforcement and Intelligence Community.

I am not saying that we are there or it is perfect, but by bringing all this information together in the sharing process that we have, at least from the State Department's view, we have access to an incredibly expanded and diverse database that we never had before in order to help us make our decisions.

Mr. SCOTT. And the Department of State didn't end up in the Department of Homeland Security, so you didn't need the Department of Homeland Security to do that.

Let me ask another question, because I am running out of time. The issue of torture has come up, and my question is, if Timothy McVeigh had been caught either shortly before or shortly after the Oklahoma bombing, if we are going around torturing people, how would we have known whether he should have been tortured as an American citizen or not?

Mr. TRAVERS. Sir, I think I probably speak for all of us that that question would be way outside the lane of responsibility for any of our organizations. NCTC, for instance, looks at analysis and integration of information—

Mr. SCOTT. If he had been captured and if he was kind of foreign looking, people have suggested he shouldn't have been given Miranda rights and ought to have been tortured to get information. Are you suggesting that torture is always outside the line?

Mr. TRAVERS. No, sir. I am just saying that that particular question is outside the lane of any of our organizations here.

Mr. SCOTT. Any of your organizations, it was not outside the lane of the United States policy.

Mr. TRAVERS. I would refer you to Department of Justice and operational organizations.

Mr. SCOTT. Mr. Healy, you are in the Department of Justice. Is torture outside the lanes? We need to get information.

Mr. HEALY. Well, sir, as a father of seven, when you talk about torture, I think about what my children would say. I would not, with the word "torture," condone torture, but with regard to your question, sir, I would refer you to the Department of Justice or my director.

Mr. SCOTT. So how would you know whether to use—what do you call it—enhanced interrogation techniques, how would you know whether to apply those techniques or give Miranda warnings to someone—if it is an American citizen, I would assume they would be entitled to Miranda warnings; is that right?

Mr. HEALY. In a law enforcement action—and I go back to my 24 years as an FBI agent—in a criminal matter, if I arrest someone, as a matter of policy prior to interrogating him, I would issue Miranda warnings.

Mr. SCOTT. If they look foreign, does that—

Mr. HEALY. Sir, I am talking in general in my law enforcement days.

Mr. SCOTT. Would a person's right to the Miranda warning be less if they looked foreign?

Mr. HEALY. Again, sir, the policy for law enforcement actions, if I have two components, custodial and interrogation, as part of my policy that I follow in any type of law enforcement case, I would Mirandize them. With regard to specific cases or operational decisions, I would refer you to, if it's a counterterrorism case or on a particular case, I would refer you to the assistant director over that particular case.

Mr. SCOTT. So you would not treat someone who looked a little different than everybody else different than Timothy McVeigh?

Mr. HEALY. Pardon me, sir?

Mr. SCOTT. You would not treat someone who looked foreign differently than you would have treated Timothy McVeigh.

Mr. HEALY. Yes.

Mr. SCOTT. Yes, you would treat them differently—

Mr. HEALY. No, sir. I am acknowledging.

Mr. SCOTT. I guess we are in the 5-minute honor system, I think my 5 minutes is up.

Mr. CONYERS. Does the gentleman need more time?

Mr. SCOTT. Well, let me ask another question then since you have invited the other question.

With all the information we have, how do we limit the number of people who can see the information that may be embarrassing—medical, mental health—about people; how do we limit the number of people that have access to that information and at the same time, have enough people connecting the dots?

Mr. TRAVERS. Excellent question, sir.

As all of my colleagues have indicated, I believe that by any objective standard every department and agency in this government is pushing more and more electrons to relevant organizations to help do this “connect the dots.” While we do so, we are also incredibly careful about what information is being passed. And so issues of privacy concerns are foremost on all of our minds. We have significant conversations with any organization, for instance, that has a database with commingled data, a database that may have U.S. persons as well as foreign individuals in that data set; how do we get that information; what can we do with it; how long can we keep it? We have extensive auditing to ensure that information is being properly utilized. And so we have gone to great strides to both promote information sharing, but at the same time, be good stewards of information.

Mr. SCOTT. And confidentiality, because a lot of information you get will certainly be embarrassing, confidential. I mean, you are talking about medical information, mental health, family situations, a lot of things that people would just assume not be public and not have a lot of people—I mean, if you are in Northern Vir-

ginia, it is very likely that some of your neighborhoods and friends may be government officials. How do you limit the number of people who can actually see it and at the same time make best use of it?

Mr. TRAVERS. Just speaking from the intelligence and national counterterrorism perspective, we would not be privy to that information. The only information that I get from the Federal Bureau of Investigation is related to terrorism investigations, for instance, or information that could be associated with terrorism. And the same thing with Homeland Security, I am not getting any medical records or anything like that at NCTC.

Mr. HEALY. And Congressman, if I may also point out, the way the system is set up, NCTC or TIDE actually holds identifying information and the derogatory information, so they withhold that, and it is a very highly classified system. The process that we set up with the Terrorist Watch List was that that identifying informational alone would be forwarded down to our screening partners. So the detail and information that you are talking about would not be available to the State or local law enforcement officer, it wouldn't be available to the thousands of Customs Border Protection people or the Consular Affairs. The way the process is set up is taking into consideration privacy, liberty, civil liberties, and things like that as well so that once a name goes through that process or an individual goes through that process, it gets vetted with NCTC, and they push down only identifying information.

Once we look at it, we push down only identifying information. So the only information that is available to a law enforcement officer is the individual that I have stopped may or may not be a known or suspected terrorist. For additional action, call the Terrorist Screening Center and confirm that. Once that confirmation is made, a series of events occurs—again, as I spoke before, a coordination between the FBI for some type of operational response.

So the whole system was set up to, one, allow every law enforcement officer that queries into NCIC, every Border Protection officer and every Department of State person when someone applies for a visa to have that terrorist information available to them in their existing system, but yet balance civil liberties. And I think that we have really worked hard to strike that balance collectively with all of us.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. CONYERS. Thank you, Mr. Scott.

We now turn to Dan Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I appreciate that.

And just an observation I had listening to all this, I have often wondered why some people think that telling someone that “you have the right to remain silent” would make it more likely that they would talk to you. That is the only thing I never tried with my kids, I guess, but maybe the world works differently than my experience has been.

I also say, to ask someone questions without Mirandizing them is not torturing them. One of the questions previously was do you Mirandize them or do you torture them? There is a whole world in

between that, and it sort of goes to some of the confusion we have here.

Would the gentleman from Florida allow me to use his slide? Can we put that up? It helps me visually to be able to see exactly how this information flow goes. Can you read that? This is a schematic that Mr. Rooney has that was taken from some testimony by the State Department previously and CRS actually put it together. It tries to show the flow of information. And the reason I ask that is, in my opening statement, I mentioned that I have some concern about us using a different standard for watchlisting, and that in the previous Administration, as I understand it, the standard was “appropriately suspected” to now this new “reasonable suspicion” standard that appears to me to come right out of Terry versus Ohio, which is a criminal justice standard.

And so Mr. Healy, I guess I would ask you, why has the Administration decided that the Terry standard should apply to aliens outside the United States who, by my understanding of the Supreme Court decisions, have no right to Fourth Amendment protections?

Mr. HEALY. Thank you, Congressman. Prior to the reasonable suspicion standard that began—actually, it was enacted with the community in February of 2008, there wasn’t a standard. I had the unique position of being at the Terrorist Screening Center during those early days when we started learning how the watchlisting process was. What occurred, actually, was as we progressed through the process, we identified an issue of making a standard so that the community could agree with it.

As you mentioned, Terry versus Ohio is a legalistic opinion by the Supreme Court, but that was used as a baseline to help define reasonable suspicion. And from there, it was adopted and adjusted to meet the intelligence and law enforcement requirements. That process was very similar to the process that we are ongoing right now, Congressman, that involved all of the different agencies to come up with a unified standard so that they knew.

The problem before that, Congressman, was that the CIA felt an individual should have been watchlisted that went through the process and it was or wasn’t and it was inconsistent.

Mr. LUNGREN. Here is my question, as I understand what you said in response to Mr. Smith’s question, you indicated the Christmas bombing response as a failure to connect the dots. And I thought Mr. Travers suggested it wasn’t so much a question of connecting the dots, but actually establishing what the dots were. And if I understand that correctly, there seems to be somewhat of a difference.

And my question would be then to both of you, does the standard that has been adopted, the one that you articulated, which is the nominator, based on the totality of the circumstances, must rely on articulable intelligence or information which, taken together with rational inferences from those facts, reasonably warrant a determination that an individual is known or suspected to be, or have been knowingly engaged in conduct constituting in preparation for, in aid of, or related to terrorism or terrorist activities. Does that definition help you in the case of the Christmas bomber or hinder you, or make no difference whatsoever?

Mr. HEALY. With the review process, that particular standard, the reasonable suspicion standard that we have identified that we have been using, based on the review, we feel that the reasonable suspicion standard is adequate. We have looked at some of the implementation that we used—

Mr. LUNGREN. Well, adequate for what purposes? Adequate for protecting you against legal action later on or adequate for purposes of putting the people on the list who ought to be on the list? Because this was an individual who wasn't on the list.

Mr. HEALY. Right. With regard to the Terrorist Screening Center and NCTC, and all of my colleagues here, we work with this terrorism issue every day. It is not an issue of I am concerned about being prosecuted, it is an issue of every day I sit down and talk to my staff and tell them this: If we make a mistake, people die. It is that easy. And as a result of that, we work to ensure that we don't have people get on planes and hurt people.

The reasonable suspicion standard that we have, based on what occurred and based on the review, I think collectively we feel that that is a reasonable standard. It is low enough to be able to include people, it is high enough to make sure that we balance civil liberties and protection of the American people.

Mr. LUNGREN. So, should Mr. Abdulmutallab have met the standard based on the totality of circumstances relying upon articulable intelligence or information which, taken together with the rational inferences from the facts, reasonably have warranted a determination that he was known or suspected to be or had been knowingly engaged in conduct constituting in preparation for or in aid of or related to terrorism or terrorist activities?

Mr. HEALY. And the question was, sir?

Mr. LUNGREN. The question is very simple. I asked you whether or not Mr. Abdulmutallab meets that standard. That is my question. That is what we are here for.

Mr. HEALY. If all of the intelligence was put together, he would have met that standard in my view.

Mr. LUNGREN. Well, here is my whole question: if someone is starting off with that standard, does he even begin to go into the process? Does the person at the consulate in Kenya or Yemen, or wherever, if they get that information from his father, does this standard give them a reason to put him in the system, or does this standard become so restrictive that if I take that information and knowing nothing else, I don't begin to put it into the process. That is my question.

Mr. HEALY. Actually, it does. The way the process is set up with TIDE and NCTC—and I will let my other colleagues speak as well—and with the Terrorist Screening Center, TIDE actually has a lower standard and it starts the process.

Mr. LUNGREN. Okay. That is what I want to know. So what should the standard have been that the State Department should have paid attention to to at least enter that bit of information with enough significance so that you would have put it into the system? I mean, that is what I am trying to get at. We have heard a lot of stuff here, but I am trying to get at what happens in this case if it is repeated, what standard is used at that entry point that would start it going?

Mr. TRAVERS. And I think the complexity here, sir, is that, with respect to Umar Farouk, the information that came in from the State Department on the 20th of November with everything they had with respect to the derogatory, that amount of derogatory at the time—as you, I think, correctly quoted—under the influence of extremists in Yemen, or something along that line—would not have been sufficient to get him watchlisted. The failure on the part of NCTC was there was this other piece of information that had we, in fact, connected it to the Visa VIPER cable, I think everyone agrees would have crossed the bar, would have gotten—

Mr. LUNGREN. Okay. My question is very precise—I hope—which is, was it the failure of the intake officer—I will call him the intake officer, whoever got that information from his father—was it the failure of him to put significant facts into this entry point, or was it that the system didn't automatically take that bit of information and connect it with several other pieces of information?

Mr. TRAVERS. The system at the time said, Militants, extremists, jihadists should not be nominated without particularized derogatory. The State Department had no other information from the father that would have come to me that would have led my analyst to nominate the individual.

Mr. LUNGREN. So what is the difference now? Same scenario, comes in today, same information, no more information, it is not after the fact, it is before the fact, the father comes in with that information, what difference would it make today?

Mr. TRAVERS. And that is the discussions ongoing within the interagency right now, but I think that as a general proposition, the quality of the source coming in would weigh quite heavily.

Mr. LUNGREN. The father?

Mr. TRAVERS. The father, exactly. And so that you could have sufficient flexibility to get an extremist nominated to a watchlist.

Mr. HEALY. And additionally, sir, the label “extremist,” we are taking a look at that as well and—again, the implementation process, judging that as well.

Mr. LUNGREN. My other question will be on this: When you folks got the information from State Department, did you not know the source? That is, did you not know it was his father and the significance of his father being a reliable source, someone who—if you look back now, and I know it is easy to look back now, if you look back now, it is the father, he's got some prominence. He obviously is putting himself in jeopardy by bringing this information forward or maybe bringing his son into jeopardy. That, to me, if I am an investigator, even in law enforcement, suggest, hey, this guy might be credible. So was that information passed on to you?

Mr. TRAVERS. I have actually forgotten whether or not that fact was in the Visa VIPER cable itself. I don't think it was. But, frankly, that would not have, at the time, given the standards and the way we were interpreting the standards, would not have been sufficient. The father was concerned. He, frankly, wasn't concerned that his son was going to go blow up an airplane, wasn't concerned his son was going to be a terrorist.

Mr. LUNGREN. I know, but he was concerned enough to come to us to tell us there was a problem.

Mr. TRAVERS. Sure. But I will tell you that we get tons of data pieces over the course of days and weeks about extremists and people being concerned about relatives and so forth. It is a function of separating the real important ones from those that are of less importance.

Mr. LUNGREN. I understand that, and I have heard this before. My question, is it going to be different next time? I realize you get all kinds of information, I realize that.

Mr. HEALY. Congressman, one of the things that we've looked at and recommended changes for is that single source coming in and the ability for that receipt officer to be able to judge the credibility of the source. In this case, because of the prominence of the individual, because of the fact that he is reporting on his son, that would give additional weight to the nomination process.

Mr. LUNGREN. My concern is this—and you know this, being in the FBI for your career and having any exposure to law enforcement, particularly at the local level, often it is a small piece of information from an investigator, from someone who has got some sense that something is wrong that triggers an entire investigation.

Goodness gracious, Watergate. We know that started with somebody who put something together. You put a piece of tape on a door jam and the government implodes. No one would have figured that.

My point is, we understand the significance of an intuition by trained people in the field. I just want to make sure that this standard doesn't go counter to that. That is all I am trying to do is to make sure we are not putting a harness on good people in the field who are beginning to sense that something is wrong, and I don't want them to have this fear that, oh, my God, you are going to be accused of this, that, or the other thing by not entering it into the system. That is my fear, and that is my concern. And that is all I am trying to get to here.

Mr. KENNEDY. Sir, if I might add, when the information came to the State Department—we get lots and lots of poison information every day, former business partners, former boyfriends, former girlfriends come in all the time and attempt to—using a law enforcement term—dime out their people. The State Department took this seriously enough, as we do things, and that is the entire purpose of the Visa VIPER program.

Somebody comes in and we say, this doesn't look right. We then send that information off to Washington so that our colleagues in the law enforcement and Intelligence Community can integrate that single piece of information, just as you said, the investigator seeing something—

Mr. LUNGREN. Did the VIPER report indicate that it was the father and that the father was prominent?

Mr. KENNEDY. It was collateral reporting that we can discuss in another venue, sir.

Mr. LUNGREN. Well, I mean, that is pretty important. That is pretty doggone important.

Mr. KENNEDY. There is collateral reporting that—

Mr. LUNGREN. And I appreciate everything you have done, I appreciate the entire panel, but, sir, you said we took it seriously, or seriously enough, or something; obviously we didn't take it seriously enough.

Mr. KENNEDY. I was talking about the State Department's taking the father's reporting to us, the sufficient severity descended into Washington and not dismiss it as raving.

Mr. LUNGREN. I hope the State Department has purchased the Yahoo software that if you have a different spelling—

Mr. KENNEDY. We have that already installed.

Mr. CONYERS. Thank you, Dan Lungren.

Sheila Jackson Lee.

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

Let me ask Mr. Healy, how many years have you served at the Bureau?

Mr. HEALY. Approximately 24.

Ms. JACKSON LEE. So you were at the Bureau during the Bush administration?

Mr. HEALY. Yes, ma'am.

Ms. JACKSON LEE. And to your knowledge, Miranda was used in previous Administrations on alleged terrorists, Miranda?

Mr. HEALY. Yes. I believe in previous cases when individuals were arrested, they Mirandized them, yes, ma'am.

Ms. JACKSON LEE. And do you feel that the security of the Nation was diminished because Miranda was used in certain instances?

Mr. HEALY. I don't think I had an opinion on it, ma'am.

Ms. JACKSON LEE. Would you use it? I don't see why you don't have an opinion, I don't understand that. Do you believe that the security of the Nation was diminished at times that Miranda was used? Your title seems to be over the Director of Terrorism Screening, so you have some sense of terrorism. I don't know what you mean you don't have an opinion. Does Miranda equal the diminishment of national security for the United States if it is used?

Mr. HEALY. I don't think it is a factor. I have never seen it used where it is a factor in that, ma'am.

Ms. JACKSON LEE. And where it is a factor in that it can be considered a problem in the security of America; is that my understanding?

Mr. HEALY. Again, with my experience in criminal matters, I have not worked terrorism cases other than my involvement 6 years ago with the shift in the direction of the Bureau. Whether a Miranda warning was issued or not is an operational decision that is made at the time.

Ms. JACKSON LEE. And so you would not oppose operational decisions like that if the parties involved felt that Miranda was appropriate?

Mr. HEALY. I would refer decisions like that to the operational components on the ground and my superiors. As the Director of the Terrorist Screening Center with regard to this particular case, my involvement didn't involve the operational component, it was already ongoing. The only time that my involvement with the Terrorist Screening Center and any type of terrorist subjects that are watchlisted, the operational component is during the screening process.

The extent of my involvement in that is to coordinate with the FBI to get the operational components on the ground connected with the screening entities. Once that has occurred, then they take

over the investigation or whatever results of that. As a result of that, they report—

Ms. JACKSON LEE. I will pose a question to others on the panel and see whether they have an answer, but let me continue to work with you on this question, particularly the Christmas Day bomber.

What was the breakdown between the information received in Nigeria with the State Department—the State Department is here, I know—in getting this information transferred and interpreted such that this alleged perpetrator could be on the watchlist?

Mr. HEALY. The initial information, as my colleagues have said, based on the father coming into the embassy, resulted in a Visa VIPER. That Visa VIPER was referred to NCTC and entered into TIDE. That Visa VIPER, as Mr. Travers has said, had enough biographical information to be in TIDE, or watchlisted, lacked enough derogatory information to put it into the reasonable suspicion standard. So from that standpoint, the name wasn't watchlisted based on that single reporting piece of intelligence and it wasn't pushed over to the Terrorist Screening Center database.

Ms. JACKSON LEE. So where do you think the collapse came or the failure came?

Mr. HEALY. As I have said, if we have a magic ball, if there was something that would allow us to connect the dots on everything, every piece of intelligence that came in and it automatically connected to everything else that we had, that would be very beneficial. If you could look at the totality of the facts to be able to make a nomination, that would be helpful.

Unfortunately, right now what we get from NCTC is between 400 and 1,200 add, modifies, and deletes a day. What they look at is significantly bigger than that.

Ms. JACKSON LEE. Do we need more resources, more trained professionals in human intelligence? Let me try to, without probing into classified information, I assume that the father publicly told the point person in Nigeria that the individual had been to Yemen and that he felt he was being trained in Yemen. Was that not information that the desk officer had?

Mr. HEALY. I would have to refer to the desk officer on that, ma'am, I am not sure.

Ms. JACKSON LEE. So you are not privy to what information was then sent through Visa VIPER and then on to the various areas?

Mr. HEALY. The way the process works, the information, the derogatory information is in TIDE. And I will refer to my colleague to talk about the TIDE information.

Ms. JACKSON LEE. All right. Colleague, would you answer that, please, Mr. Travers?

Mr. TRAVERS. The Visa VIPER cable that came in, Umar Farouk Abdulmutallab, came into one of my desk analysts with a Viper cable that had a pretty short statement of derogatory—under the influence of extremists in Yemen, or something to that effect. What she did was exactly what she has been taught, she went and searched Umar Farouk Abdulmutallab across all the other databases and got exactly zero hits. Why? Because there was no other Abdulmutallab anywhere in the database.

The problem came that there was other information out there associated with Umar Farouk, that is all—spelled differently. And

the challenge for her, the challenge for all of my analysts is that roughly 350 names are nominated to the National Counterterrorism Center every day, and they span a wide range of derogatory information—suicide bomber, facilitator of terrorism, extremist. In the case of Umar Farouk Abdulmutallab, he would have been at the very, very low end of our level of concern. That is why in my opening statement, I said the two things that we are trying to do to enhance our ability to catch the next one of these kind would be to bolster the resource base associated with populating TIDE so that instead of a relatively rudimentary data set, we are enhancing the record so that the analysts will go out and search for other information that might enhance the record so that we would cross that reasonable suspicion bar to push the information to Director Healy.

Similarly, we have a pretty substantial organization that is being built within our Director of Intelligence to help us with these random dots. It may not be a name, it may be a concept, but these are the kinds of things that are designed to help us exploit the tremendous amount of information that is out there. Are there resource implications? Yes, ma'am, absolutely.

Ms. JACKSON LEE. Let me just quickly move to Mr. Kennedy of the State Department. Have you had any change in procedure based on what happened in Nigeria?

Mr. KENNEDY. Yes, Congresswoman. What we have done is we have increased the information that we put into the Visa VIPER reporting cable. There was an interagency-agreed process that we provide the following data points.

Ms. JACKSON LEE. What about training of your staff? Because I am still concerned that the staff in Nigeria, obviously they are not terrorist experts, but I think if someone indicates that I believe my son is being trained in Yemen, that it should raise the level that maybe rather than you inputting it, you get on the phone and call, and maybe your call could convince the other receivers of information to heighten their sensitivity to the information.

Mr. HEALY. Congresswoman, we have added additional information, but just as a matter of technicality, by turning this into a Visa VIPER cable and reporting it, this information goes to the entire intelligence and law enforcement community.

It is like a broadcast. Calling one person is good but we might call the wrong person and that person may not have—so we prefer as a matter of course to send it to the entire law enforcement and Intelligence Community so that if anyone is aware of concerns about this individual, we are raising the flag throughout that entire community rather than just with one individual who may or may not have that next piece that Mr. Lungren referred to. We are the frontline. We are out there—

Ms. JACKSON LEE. Let me just finish up on my question so I can yield back. Can you tell me what determination brings about the 14-country list? Did that come after the Christmas Day bomber? There is a 14 country list that Pakistan is on.

Mr. KENNEDY. That is a list that was proposed by the Department of Homeland Security.

Ms. JACKSON LEE. Let me move to the Department of Homeland Security. Would you explain that list and why, please.

Ms. COGSWELL. Yes, ma'am.

Ms. JACKSON LEE. Thank you, sir.

Ms. COGSWELL. Immediately after the event DHS moved to put in place immediate enhancements to our security and screening posture in order to address the immediate threat stream. In doing so, we looked at a process we already had in place, the ability to issue those security directives and enhanced emergency amendments to increase the level of screening, and we focused on a way to designate certain individuals for that enhanced screening. We selected the countries based on those that were designated as state sponsors of terrorism, safe havens or links to the current threats streams that were in the environment. These were meant to be not permanent but near term to address the threat. They will evolve. They will change and—

Ms. JACKSON LEE. When did you establish the list?

Ms. COGSWELL. I would have to check the date, but within a couple days. I think it was like 3 days after the event.

Ms. JACKSON LEE. I would ask that you submit the full list to the Committee and the analysis short of being classified, I assume, the general analysis that you utilized. Do you have a recollection of some of them without the whole list? I know you couldn't recite the whole list.

Ms. COGSWELL. Other than remembering, of course, that Nigeria and Yemen are on the list, I cannot recall the full list.

Ms. JACKSON LEE. Would you provide us with that list, please?

Ms. COGSWELL. I will.

Ms. JACKSON LEE. It seems that my good friend from California was diminishing the Miranda as a basis of getting information. I don't know why Mr. Healy—I guess he is limiting himself to the terrorists, but I know that he was an FBI agent previous to that, and I am not sure why he is not able to give some sense of why the Miranda would diminish the rights—or the ability to secure America.

But I would suggest that the problem that we have—and I am prepared to yield back, Mr. Chairman, and I thank you for this hearing, and I sit on the Homeland Security Committee—is the unfortunate sense that I get is that we are repeating post-9/11. It was the same lack of transfer of information that did not transfer a memo from an agent in the Midwest to the understanding of individuals who were training and used cash to be trained in Florida to take off and not land.

So I don't know where we are going to go with this sharing of information. We put more layers on, Mr. Chairman, but I don't know if the layers are more effective. I think it will be interesting for us to continue to pursue this and collaborate with other Committees because our responsibility on securing the Nation is based on, I believe, human intelligence and the transfer of such.

And as I listened to Mr. Healy talk about from Visa VIPER to so many acronyms, I don't know where you get to the point where somebody stops and says this is enough for me to pick up the telephone, something that we don't use anymore because we are too busy e-mailing and people are too busy not reading their e-mail, pick up the telephone and say I may be in error, but let's move for-

ward and put Mr. X—Ms. XYZ on this watchlist. I believe privacy is crucial and I don't believe we should do this willy nilly.

And I will be meeting with a group who are very concerned about the terrorists, about the list that DHS has put on, and I am concerned about that list because I don't think it was done with thoroughness. But the point is that we have got to find some way to be more keen on how we transfer information to avoid Fort Hood, the devastating loss of life, and to avoid what could have been another devastating loss of life.

Mr. Chairman I yield back

Mr. CONYERS. Ladies and gentlemen, the bells are not working, but the voting has commenced on the floor.

We will stand in recess until floor votes are disposed of and then we will resume.

The Committee stands in recess.

[Whereupon, at 12:20 p.m., the Committee recessed for votes on the House floor and the hearing was not resumed.]

A P P E N D I X

MATERIAL SUBMITTED FOR THE HEARING RECORD

Congressman Henry C. "Hank" Johnson, Jr.
Statement for the Hearing on
Sharing and Analyzing Information to Prevent Terrorism

March 24, 2010

Thank you, Mr. Chairman, for holding this important hearing on sharing and analyzing information to prevent terrorism today.

Preventing terrorism is contingent on both the sharing of information across the intelligence and counterterrorism communities and on the ability to analyze information adequately in order to act swiftly on threats as they emerge.

This hearing will give us the opportunity to examine the steps that agencies are taking to better share and analyze information to prevent future terrorist attacks.

National security is, and has always been, a priority. This is especially true in the aftermath of the September 11th attacks. The recent attempted Christmas Day bombing, on Northwest Flight 253, is a serious reminder of the dangers we face and the intent of those who threaten our nation.

This Christmas Day attack was not the fault of inaction by one agency or individual, but the result of systemic failure across various intelligence agencies to connect the dots. Our first line of defense against acts of terror is the acquisition of timely, accurate intelligence that must be shared among international agencies and quickly acted upon to identify and neutralize potential threats. It is incumbent upon the intelligence community to analyze the information it collects to predict future terrorist attacks.

Keeping Americans safe has got to be our priority. It is important to remember that the Obama Administration is working with Congress to do all he can to keep Americans safe.

This hearing will give me and my colleagues the opportunity to learn from this incident in order to prevent future terrorist attacks like this from happening.

I thank the Chairman for holding this hearing, and I look forward to hearing from our witnesses today.

Ted Poe Statement
for Judiciary Hearing on March 23, 2010

In the years since September 11th, we have undoubtedly made tremendous strides in the war on terrorism. We have disrupted terrorist networks abroad in Afghanistan and Iraq, and we have them on the run all over the world. Domestically, we have re-organized our law enforcement and intelligence communities to more effectively communicate and work with each other to help identify, target, and eliminate threats quickly. Congress has passed legislation like the Patriot Act that gives the intelligence community the tools they need.

However, a disturbing trend has been boiling up over the past few years. A trend that indicates to me that we are still making the same old mistakes we did in the past. A trend that indicates we are missing warning signs and failing to connect the dots, just like we did before September 11th.

On Christmas Day, Umar Farouk Abdulmutallab hid a small explosive device in his underpants with the intention of blowing up Northwest Airlines Flight 253

flying from Amsterdam to Detroit. Disaster was averted by luck mostly----the bomb didn't go off and passengers on the flight subdued him before he could do more harm. 289 souls were on that plane and could have easily lost their lives that day had things played out just a little different.

In the days after the attack, it became clear that Umar was not unknown to US intelligence. On November 11 2009, before the attack, British intelligence notified us that Umar was associating with Al-Awlaki, a known terrorist, and that he had pledged his support to jihad. A few days later, Umar's own father walked into the US embassy in Nigeria and told them that his son had come under the influence of religious extremists. These warning signs did not cause US intelligence to flag Umar and he was still allowed to board a plane headed for the United States filled with Americans.

On November 5th, 2009, Nidal Malik Hasan, a US Army Major, went on a shooting spree at Fort Hood, TX killing 13 and wounding 30 others. The shooting spree would not have ended had it not been for the brave actions of the US military police who responded to the incident. Considering Hasan had access to military

weapons at Fort Hood, it is quite possible the horrific shooting could have been even worse.

Again, in the days after the incident it became clear that Hasan's actions should not have come as a surprise. It turns out that the FBI had intercepted at least 18 emails between Hasan and Al-Awlaki --(the same terrorist who communicated with the underwear bomber)-- in December 2008 and June 2009. Additionally, many of Hasan's military supervisors were well aware of bizarre behavior on his part, as well as his sympathy towards Jihad. Despite these huge warning signs, Hasan retained his security clearance and continued to work at our nation's largest military base for years. He had access to classified information and weapons. How was this allowed to occur for so long?

These are not the only examples either. David Headley, an American, travelled with ease back and forth to India to help plan the Mumbai attacks of November 2008. Despite many warning signs, he never had any trouble coming in and out of the United States to plan terrorist attacks abroad.

While we have dodged a few bullets, and avoided another large scale, mass casualty terrorist attack in the years since September 11th, we need to remain vigilant and determine the reasons why we are still failing to connect the dots in a lot of these cases. When there is smoke, there is fire, and I worry that these incidents could be signs that we are missing other plots that are in development. Congress, the Administration, and the intelligence community need to work together to address these issues. I look forward to the testimony and questions today to explore these important issues.



**Questions for the Record for
Under Secretary Patrick Kennedy
The Honorable Lamar Smith (#1 - #4)
House Committee on the Judiciary
March 24, 2010**

Question:

1. Does the State Department view visas as diplomatic tools? Shouldn't they really be seen as possible means of exploitation by potential terrorists and thus their issuance (be) more scrutinized by those trained in terrorism assessment?

Answer:

National security is our paramount diplomatic goal, and 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 securely executing the visa function throughout the world. State Department officers are trained to detect potential exploitation of the visa process, and work closely with host government law enforcement on immigration threats and issues. Our officers collaborate closely with our U.S. government and international partners to share information to strengthen global travel security. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. national interests. National security is paramount.

Every single visa, before it is issued, is run against databases (biographic lookout data, photos, fingerprints) maintained by U.S. intelligence and law enforcement entities and will not be issued if concerns are unearthed.

The issuance and refusal of visas also has a direct impact on foreign relations, the economy, and other key national interests. Visa policy quickly can become a significant bilateral problem that harms U.S. interests if implemented without consideration of its impact on the full range of relevant national interests. The conduct of U.S. visa policy also 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 interests and concerns.

Question:

2. Doesn't the Secretary of Homeland Security have the authority to refuse and revoke visas?

Answer:

Yes, section 428(b)(1) of the Homeland Security Act vests the Secretary of Homeland Security with authority to refuse and/or revoke visas, with such authority to be exercised through the Secretary of State.

Question:

3. At the hearing you stated that you (the State Department) "would not entertain an appeal for revocation of a visa. We would not reinstate. Once a visa is

revoked, it is revoked. The individual is free to apply for a new visa, but after that circumstance..." What is the likelihood of getting a new visa once you have had a visa revoked? Should aliens whose visas are revoked on terror or national security grounds be allowed access to the courts to appeal the revocation?

Answer:

The Secretary has unconditional authority to revoke visas, and revocation by itself does not prejudice any future visa application. In practice, the derogatory information that we have relied on to support prudential revocation of a visa has been sufficient in nearly all cases to sustain a finding of ineligibility, should the alien reapply for a U.S. visa. In every case of an alien whose visa was prudentially revoked because of a potential link to terrorist information, a reapplication would be subject to a Security Advisory Opinion request from the field. In rare cases, the SAO review process could conclude that the information leading to the original revocation was incorrect, unreliable or otherwise deficient. If the Department of State recommends a waiver, it forwards the request to the Department of Homeland Security, which has the waiver authority. In every waiver case, law enforcement concurrence is required and the terms of the visa are carefully considered.

Aliens applying overseas for U.S. visas do not have access to U.S. courts. Aliens whose visas are revoked for any reason may reapply for a visa, and their

visa application will be adjudicated on the basis of the law and the totality of the applicant's circumstances at the time of application. Aliens who have inquiries or seek resolution regarding difficulties experienced during their travel, including watchlist and screening issues, may apply for redress to the DHS Traveler Redress Inquiry Program (TRIP).

Question:

4. Does the Department of State only report possible terror threats in "Visas Viper" cables and then just wait for other government agencies to decide whether State should use their authority to initiate visa revocation? Is the State Department just a pass-through on terror-based revocations?

Answer:

Revocation is an important tool in our border security arsenal. In the wake of the December 25 attack we have reviewed the procedures and criteria used in the field to revoke visas and we have issued and are continuing to issue new instructions to our officers. Revocation recommendations have been added as an element of reporting through the Visas Viper channel, and they are promptly acted upon.

The State Department has broad and flexible authority to revoke visas. Since 2001, we have revoked 57,000 visas for a variety of reasons, including over 2,800 after suspected links to terrorism were reported. We can and do revoke visas in circumstances where an immediate threat is reported, including at the point people

are seeking to board aircraft. In coordination with the National Targeting Center, we revoke visas under these circumstances almost daily.

At the same time, expeditious coordination with our national security partners is not to be underestimated. There have been cases where our unilateral revocation without interagency coordination 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.

When we receive a Visas Viper cable indicating that the subject holds a valid visa, it is our policy to revoke the visa unless a law enforcement or intelligence agency has requested that we not do so.

**Questions For the Record From:
The Honorable Darrell Issa (#1)
House Committee on the Judiciary
Sharing and Analyzing Information to Prevent Terrorism
March 24, 2010**

Questions for Under Secretary Patrick Kennedy, Department of State

Question:

1. Who met with Mr. Abdulmutallab's father in (the) U.S. Embassy in Nigeria? Was it a State Department official? If not, which agency? Did they file a report of the meeting? What agency issued that report to the rest of the intelligence community? If no report was issued, why not?

Answer:

An officer assigned to the embassy met with Mr. Abdulmutallab's father and 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 transmitted widely throughout the USG law enforcement and intelligence community. We would be happy to work with our interagency partners to arrange a classified briefing.

**Questions For the Record From:
The Honorable Steve King (#1 - #8)
House Committee on the Judiciary
Sharing and Analyzing Information to Prevent Terrorism
March 24, 2010**

Questions for Under Secretary Patrick Kennedy, Department of State

- 1. When there is a dispute between the State Department, which is tasked with building diplomatic relations, and DHS, which is tasked with ensuring national security, as to whether or not a visa should be issued, who has the *final say*?**

Answer:

National security is our paramount diplomatic goal, and 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. We do not see a dichotomy between diplomatic relations and national security. Our nation's security depends on our military, economic and diplomatic strength. In rare cases of dispute, Section 428(b)(1) of the Homeland Security Act vests the Secretary of Homeland Security with authority to refuse and/or revoke the visas, with such authority to be exercised through the Secretary of State.

State Department officers are trained to detect potential exploitation of the visa process, and work closely with host government law enforcement on immigration threats and issues. Our officers collaborate closely with our U.S.

government and international partners to share information to strengthen global travel security. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. national interests. National security is paramount.

Every single visa, before it is issued, is run against databases (biographic lookout data, photos, fingerprints) maintained by U.S. intelligence and law enforcement entities and will not be issued if concerns are unearthed.

The issuance and refusal of visas also has a direct impact on foreign relations, the economy, and other key national interests. Visa policy quickly can become a significant bilateral problem that harms U.S. interests if implemented without consideration of its impact on the full range of relevant national interests. The conduct of U.S. visa policy also 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 interests and concerns.

Question:

2. How many visas were revoked in 2001 and in each year since then?

Answer:

FY 2001 (9/11/01 - 9/30/01)	649
FY 2002	13,930
FY 2003	5,751
FY 2004	3,066
FY 2005	2,844
FY 2006	5,379
FY 2007	7,608
FY 2008	7,592
FY 2009	8,368
FY 2010	2,676
Total	57,863

Question:

3. How many visas were revoked in 2001 and in each year since then, *for suspected ties to terrorism?*

Answer:

FY 2001* (9/11/01 - 9/30/01)	
FY 2002*	
FY 2003*	
FY 2004	1,069
FY 2005	491
FY 2006	262
FY 2007	392
FY 2008	257
FY 2009	257
FY 2010	150
Total	2,878

*** Prior to 2004 the Department did not track the specific reason for revocation.**

Question:

4. How many requests – both formal and informal – for Visa Security Units has (the) State Department denied since 2002? (A denial should be counted even if after first denying the request, the request was ultimately approved.)

Answer:

There have been five cases in which initial NSDD-38 requests were turned down. In three of the five cases State and DHS worked together to resolve particular issues, and VSUs subsequently were established.

Question:

5. Under Section 428 of the Homeland Security Act the Secretary of Homeland Security is authorized to establish Visa Security Units at visa-issuing posts overseas “unless the Secretary determines that such an assignment at a particular post would not promote homeland security.” So, where the Secretary of Homeland Security has determined that establishment of a Visa Security Unit at a visa-issuing post would in fact *promote homeland security*, on what possible basis, then, does the Department of State deny a DHS request to open a Visa Security Unit – normally a team of at most three agents – at such an overseas post?

Answer:

The process for evaluating an agency’s request for locating a position in a mission overseas is the National Security Decision Directive 38 (NSDD-38) process. Under NSDD-38 procedures, a Chief of Mission must determine whether it is possible and safe to accommodate additions to mission personnel. Embassies and consulates overseas have finite space and limited resources. When making a

determination on an NSDD-38 request, the Chief of Mission will consider how each additional position would contribute to mission priorities, and the impact of each position on available space, other resources, and support capabilities, while also considering the threat level and existing presence at post of the agency requesting new positions. VSU expansion has faced challenges common to agencies that have expanded their overseas presence in recent years. Secure workspace, safe housing and appropriate support resources are at a premium in all of our embassies and consulates. The ability to add physical resources within short time frames is severely constrained by the requirements that must be met to build or expand embassies and consulates.

Question:

6. Has Department of State headquarters established specific reasons, which it has communicated to all embassies and consulates, for which an NSDD-38 request for establishment of a VSU at a visa-issuing post overseas may be refused? If so, what are those criteria? If not, why not? Why would (the) State Department ever deny a request that would enhance national security?

Answer:

There are no NSDD-38 criteria specific to VSUs. The Department of State provides guidance to Chiefs of Mission when reviewing any NSDD- 38 proposal. Chiefs of Mission consider these five issues before making their decision:

- Whether the need for the proposed position is addressed in the Mission Strategic Plan.

- Whether other resources at post might perform the proposed function.
- If the request is for one or more U.S. direct hire positions (i.e. full-time U.S. government employees), whether the function could be performed by TDY or local hire staff.
- The administrative support, space, and funding arrangements that would be required for the proposed position(s).
- Whether the benefits of increasing the Post's staff size outweigh the heightened security risk relating to such an increase.

Question:

7. I understand that the Department recently first refused, then approved a couple days later, an NSDD-38 request for establishment of a Visa Security Unit at a visa issuing post. One of the reasons for the refusal stated in the original refusal cable was that a State Department Assistant Regional Security Officer (ARSO) was expected at the post and that a VSU would thus be unnecessary. Is it the position of the Department of State that the presence of an ARSO at a post makes a VSU unnecessary?

Answer:

No, in fact, the presence of a VSU focusing on counterterrorism-related issues complements our Assistant Regional Security Officer-Investigator (ARSO-I) program. "ARSO-I" is a title given to the Department of State's Diplomatic Security Service Special Agents, who, as federal law enforcement officers, investigate U.S. visa and passport fraud. VSU officers collaborate with consular officers and ARSO-Is at various points during the visa adjudication process,

including pre-issuance reviews, to enhance the overall visa process by providing law enforcement expertise earlier in the process.

Question:

8. The Department of State has ultimately approved every NSDD-38 request for establishment at a post that DHS has sent since the Christmas bombing incident, including one post where State has long resisted a VSU. Will the State Department go back to denying or ignoring VSU requests once it believes that Congressional attention is no longer focused on the issue?

Answer:

The Department will continue to work collaboratively with DHS within the processes prescribed by an October 2004 Memorandum of Understanding between the Department of State and the U.S. Immigration and Customs Enforcement, Visa Security Unit (ICE/VSU) on the Administrative Aspects of Assigning Personnel Overseas, and NSDD-38, to determine where the establishment of a VSU is appropriate based on a number of factors, including the effectiveness of alternative arrangements for DHS staff, available space at the embassy, support capabilities, and security concerns at the post. Department officers are assigned to work with ICE on site selection, the establishment of VSUs overseas, and to help ICE navigate the interagency process for establishing new positions overseas. Over the years, the Department has gone to extraordinary lengths to support ICE/VSU expansion, including sending senior consular and diplomatic security officers on visits to posts to help ICE explain their mission to Chiefs of Mission.



**Responses to Questions for the Record from Patricia Cogswell
Submitted by Ranking Member Lamar Smith**

Question: Doesn't the Secretary of Homeland Security have the authority to refuse and revoke visas?

Response: Yes, the Secretary does have the authority to refuse or revoke visas. This authority is codified in two locations:

- (1) The Homeland Security Act of 2002 (HSA), the Secretary of Homeland Security may "refuse visas in accordance with law." 6 U.S.C. § 236(b)(1); and
- (2) DHS and the Department of State entered into a Memorandum of Understanding (MOU) that articulates the processes to be used in exercising the authority to refuse or revoke visas. *Memorandum of Understanding Between Secretaries of State and Homeland Security Concerning Implementation of Section 428 of the Homeland Security Act of 2002* (Sept. 30, 2003).

Question: I understand that Visa Security Units (VSUs) at posts overseas review visa applications for possible criminal or terrorist-related threats to ensure that visas are not issued to applicants posing those types of threats.

But what, if anything, do VSUs do to review previously issued visas for possible revocation?

I know that VSUs will follow tips or leads about possible criminals or terrorists and recommend revocation about visas such individual suspects may have, but what if any affirmative steps do VSUs take to regularly review visas that have been issued at post for possible revocation?

Response: U.S. Immigration and Customs Enforcement (ICE) special agents stationed at posts overseas under the VSU program routinely interact with foreign law enforcement officials and public contacts. VSU agents actively pursue information that may lead to the refusal of a visa application or revocation of an existing visa. VSU agents at post routinely assist DOS by conducting investigations and using DHS resources to identify current visa holders who may be associated with an application that is denied for terrorism or fraud. The Visa Security Program at ICE Headquarters has placed staff at the National Counter Terrorism Center and at the U.S. Customs and Border Protection National Targeting Center to better coordinate cases and facilitate information sharing. A routine part of the duties of VSU agents assigned to both locations is to identify current visa holders whose visas may be subject to revocation, and to refer these cases to DOS directly or through the Terrorist Screening Center for revocation. VSU agents also participate in Visas Viper committees at each post. These committees allow participating agencies to report on possible terrorists for watchlist inclusion. If an individual applying for or holding a U.S. visa is identified as a possible watchlist candidate, then the VSU provides appropriate input to inform the visa adjudication process and any decision on possible revocation of a previously issued visa. In

the wake of the December 25 attack the Department of State has instituted changes to its Visas Viper and visa revocation procedures to more accurately match Visas Viper subjects with visa records, and to revoke any visas more expeditiously.

Question: How, exactly, do you understand that mandate for DHS established by Section 428 of the Homeland Security Act?

Do you see the DHS role in the visa process as limited to just running visa applicants names through security check databases or a much broader one to control visa policy generally?

Response: Both the Departments of State and Homeland Security both see DHS's role as broader than just "running names through security check databases." DHS plays a strong role in the overall visa policy.

Specifically, section 6(e) of the MOU between the Secretaries of State and Homeland Security, which concerns the implementation of section 428 of the Homeland Security, provides that DHS employees assigned to overseas posts under section 428(e) perform the following duties:

(1) Provide expert advice to consular officers regarding specific country threats relating to the adjudication of individual visa applications or classes of applications. Actions may include but are not limited to:

- (1) Gathering and reviewing intelligence reports and coordinating with other agencies at posts to consolidate up-to-date information (with respect to terrorist groups or other entities or individuals in the host country who pose a threat to homeland security and their connections with individuals and groups in other countries), and making this information available to consular officers in a timely and useful manner;
- (2) Briefing consular officers and providing training sessions concerning terrorist groups or other entities that pose a threat to homeland security and interview techniques useful in detecting persons who may be a threat or whose applications may be fraudulent; and
- (3) Consulting with consular officers on particular visa applicants who raise homeland security concerns.

(2) Review any such applications, either on the initiative of the DHS employee in accordance with procedures prescribed by DHS or upon the request of a consular officer or other person charged with adjudicating such applications. The actions may include, but are not limited to, providing input to or recommending security advisory opinion requests based on their expertise.

(3) Conduct investigations with respect to consular matters under the jurisdiction of the Secretary of Homeland Security.

In addition, DHS, as chair of the Security Advisory Opinion Review Board, has policy oversight over the Security Advisory Opinion (SAO) process and the Secretary of Homeland Security exercises final authority to deny an individual's visa application. SAO's are the mechanism used by the Department of State (DOS) to provide consular officers advice and background information to adjudicate visa applications abroad in cases of security or foreign policy interest. Checks may be triggered by a variety of criteria deemed to be significant for reasons of national security, including positive results from visa name check results, or upon a consular officer's request. SAO namechecks are referred to FBI, CIA, and the Terrorist Screening Center for processing through their databases.

Question: Does DHS see no role in its overseas-posted VSUs in other aspects of the visa adjudication process?

Response: DHS does see a role for the VSU overseas in other aspects of the visa adjudication process. VSU officers provide advice and training to consular officers, participate in terrorist lookout committees, conduct criminal investigations, and provide liaison to other law enforcement, intelligence agencies, and host nation officials. They may recommend applicants to the Security Advisory Opinion process for further in-depth security checks. VSU officers conduct in-depth law enforcement interviews of individual visa applicants if warranted. Where VSU officers encounter information in the visa process that may be of interest for intelligence or law enforcement purposes, it communicates that information to U.S. Customs and Border Protection for use at the border, as well as disseminating information to domestic ICE offices and other agencies for law enforcement and intelligence use. As outlined in the section 428 MOU with the Department of State, VSU officers routinely exercise DHS authority to recommend denial or revocation of visas when it is determined to be warranted.

Question: Of the 2,800 individuals with suspected ties to terrorism whose visas have been revoked since 2001, how many of these individuals are still in the country?

How many were removed?

What is being done to find the remainder that are still in the United States and remove them?

Response: The Department of Homeland Security works closely with the Department of State to ensure that individuals whose visas were revoked because of suspected ties to terrorism cannot travel to or enter the United States. With respect to those individuals whose visas were revoked for suspected ties to terrorism since 2001, it is important to note that most of these visas were revoked prior to the individual attempting to travel to the United States. Information for all individuals whose visas have been revoked are included on "lookouts" in the relevant systems used by the Department of State and DHS to screen travelers to the United States. (i.e., DHS's TECS (biographic), DHS's IDENT (biometric), and State's

Consolidated Consular Database (CCD)). Those who attempt to enter with an invalid visa are now stopped before they board an aircraft departing for the United States, under our new procedures implemented since the December 25th attempted bombing. Prior to December 25th, when a person applies for entry at the U.S. land border, they would be stopped at the border.

In addition, in response to the Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack, the U.S. government has taken additional steps to identify all current visa holders who also had records in the Terrorist Identities Datamart Environment (TIDE) and assess their current status. The U.S. government identified that there were 1,287 individuals who had a valid visa and who also had a record in TIDE. This total includes individuals for whom the information in TIDE was previously determined insufficient for the individual to be added to the Terrorist Screening Database (TSDB), the official U.S. known or suspected terrorist watchlist, the individual was previously granted a waiver, or the individual had been previously determined not to present a threat.

DHS determined that only 641 of the 1,287 individuals had traveled to the United States. Of those 641 individuals, DHS believes only eight of these individuals may have violated immigration laws by staying in the United States past their term of admission. These individuals are currently under investigation by U.S. Immigration and Customs Enforcement.

Question: What is the earliest that an airline passenger is screened or “vetted?”

Is it when they are already on or about to get on the plane?

TSA has talked about a program called “Secure Flight,” that would start the vetting process 72 hours in advance. Is this operational?

Do you have any suggestions that would allow the vetting process to start earlier?

Response: DHS has implemented a layered approach to screening advance passenger information to ensure the timely, thorough, and appropriate level of information-based screening specific to CBP’s and TSA’s respective missions. DHS currently begins its vetting for all international travelers 72 hours in advance of the flight to the U.S., and is in the process of implementing vetting of all domestic travelers 72 hours in advance of the flight under the Secure Flight program.

TSA is implementing the Secure Flight program, which requires covered air carriers to provide Secure Flight Passenger Data (full name, date of birth, gender, and redress number if available) beginning 72 hours prior to the departure of a flight (domestic or international). As of April 28, 2010, 73 U.S. aircraft operators and foreign air carriers have totally or partially implemented Secure Flight, representing approximately 60 percent of the total daily enplanement volume. The Secure Flight program normally screens against the No Fly and Selectee subsets of the Terrorist Screening Database (TSDB) and the Centers for Disease

Control's Do Not Board list. TSA anticipates that Secure Flight deployments for U.S. aircraft operators will be completed in spring 2010. TSA expects Secure Flight deployments for all foreign air carriers with watchlist matching for all covered flights, international and domestic, by the end of calendar year 2010.

CBP receives passenger name record (PNR) data for international flights to and from the U.S. beginning 72 hours prior to departure. CBP screens PNR data against various law enforcement databases and TSDB, including the No Fly and Selectee subsets. Additionally, carriers are required to transmit their complete and final passenger manifests through the Advance Passenger Information System (APIS) to CBP no later than 30 minutes prior to securing the aircraft doors (for batch transmissions) or up to the time of securing the aircraft doors through the interactive APIS Quick Query (AQQ) transmission process. APIS data includes passenger information that is found on the biographic page of passports or other travel documents, such as full name, date of birth, gender, document number, and country of document issuance. CBP screens APIS data against the TSDB and other law enforcement databases, including but not limited to TECS, the State Department's Consular Lookout and Support System (CLASS), which includes visa revocation records, the National Crime Information Center for active wants and warrants and INTERPOL records, including the Stolen and Lost Travel Documents database.

In addition to the Secure Flight, PNR, and APIS screening, most foreign nationals who travel to the United States are screened through the State Department's visa application process or CBP's Electronic System for Travel Authorization for Visa Waiver Program travelers. In most cases, these screening efforts take place long before the 72-hour pre-departure window and the results are incorporated into CBP's APIS and PNR screening.

Once all carriers have transitioned to Secure Flight, TSA screening will begin 72 hours prior to departure. TSA will assume responsibility for screening air passengers against the No Fly and Selectee subsets of TSDB and the Centers for Disease Control's Do Not Board list. Concurrently, CBP will continue to screen PNR and APIS data as part of their border security and immigration admissibility determinations.

Question: From a security standpoint, wouldn't the best scenario be to have Visa Security Unit personnel screen 100% of visa applications?

Response: ICE special agents screen all visa applicants at posts where Visa Security Unit personnel are stationed by running applicant names against Department of Homeland Security indices. If derogatory information is discovered during basic screening, ICE agents will conduct in-depth vetting on those applicants. This type of vetting serves two objectives: 1) to confirm the identity and ineligibility of mala fide applicants and 2) to "clear" eligible applicants incorrectly associated with derogatory information. ICE special agents then select additional visa applicants for in-depth vetting based on additional, site-specific factors.

The Department of State conducts vigorous screening on all visa applicants. Every visa application is run against databases (biographic lookout data, photos, fingerprints) maintained by U.S. intelligence and law enforcement entities. If these checks, and/or the consular officer's interview unearth any concerns of a security, criminal or eligibility nature, adjudication of the application is suspended pending the appropriate inter-agency review and adjudicative procedure.

Those posts where VSU personnel are stationed were selected based on risk-based analysis. It is DHS's view that requiring 100% screening by VSU of all visa applications would tremendously increase the burden on VSUs without a corresponding increase in results. As new threats and risks associated with the visa process emerge, DHS will act appropriately to assist the Department of State in screening applicants.

Question: Do you support delegating visa refusal/revocation authority to DHS Visa Security Officers assigned to visa-issuing posts overseas?

Response: As a general matter, the Secretary supports delegation of appropriate authority under section 428(b)(1) of the Homeland Security Act (HSA) to those within DHS best positioned to assess the security and operational interests and make determinations on revoking or refusing a visa application. DHS is currently in the process of determining the appropriate DHS official or officials to receive such a delegation and to carry out that function and will timely inform the Department of State of any delegation consistent with the MOU.

**Responses to Questions for the Record from Patricia Cogswell
Submitted by Representative Bob Goodlatte**

Question: According to testimony from CIA Director Leon Panetta before the House Intelligence Committee, Al Qaeda is adapting its methods and making its members more difficult to detect. Specifically, he mentioned that Al Qaeda is pursuing efforts to strike the U.S. by deploying individuals to the U.S. and using terrorists with “clean credentials,” i.e. terrorists who do not have a history of terrorism. This very committee has heard testimony on multiple occasions from the State Department’s Inspector General that the visa lottery program, which allows 50,000 foreign nationals to enter the country each year at random, “contains significant risks to national security from hostile intelligence officers, criminals, and terrorists attempting to use the program for entry into the United States as permanent residents.” If Al Qaeda is trying to send terrorists with no prior record into the U.S., as Director Panetta testified, then I am fearful of how many terrorists have entered the U.S. through the visa lottery program already and are operating here now as permanent residents. I am also concerned about terrorists sending recruits with no prior records to apply for the program.

In light of Director Panetta’s prior testimony about Al Qaeda’s tactics, do you share my and the State Department Inspector General’s concerns that the visa lottery program can be used, and possibly is being used, by terrorists to enter the U.S.?

Response: The State Department can answer specific questions about the visa lottery program, but it is important to note that individuals, once they are notified about their eligibility to apply for a visa through the visa lottery, are subject to the same requirements, standards, and security checks as other individuals applying for visas. DHS believes that the visa lottery program is no more likely to be used by terrorists to enter the U.S. than any other visa program.

As part of the visa application process, the State Department collects fingerprints and photographs from the individual. The applicant’s biographical information (name, date of birth, etc.), and biometrics (facial image, fingerprints) are run against various data sets within the U.S. Federal government (including DHS’s IDENT and FBI’s IAFIS biometric systems) as well as INTERPOL to identify information that would indicate that the person is ineligible, or has previously used another identity. State also interviews each applicant.

The visa applicant is checked again at the time of travel – first using the biographic information provided by the carrier, then again by U.S. Customs and Border Protection (CBP) when the individual arrives at the U.S. border and applies for admission. As part of this process, CBP collects the visa holder’s fingerprints and confirms that the person before them is the same person to whom the visa was issued by the State Department.

In addition to the visa issuance process, DHS has multiple layers of security in place to help identify individuals who are not a known threat, but who wish to harm the United States, including behavioral detection and the in-person interview conducted by CBP officers before an individual is allowed to enter the United States. DHS recognizes the risks posed by individuals who may be previously unknown, and has implemented layers of security for all travelers to the United States, including those who obtain visas through the visa lottery, to minimize the potential for those who wish to harm the United States from exploiting any individual program.

**Responses to Questions for the Record from Patricia Cogswell
Submitted by Representative Daniel Lungren**

Question: What role did DHS play in deciding or approving the “reasonable suspicion” standard for watchlisting? Why was a standard that has its roots in 4th amendment law chosen as criteria for deciding whether someone should be put on a list for being suspected of involvement in terrorist activities?

Response: In July 2008, the TSC’s Policy Board met and established an interagency working group to develop and articulate substantive derogatory criteria regarding acceptance of terrorist nominations into the TSDB. The working group’s goal was to articulate nomination acceptance criteria to assist analysts in providing sufficient supporting information when submitting terrorist nominations. The Department of Homeland Security is a member of the TSC Policy Board.

To describe a known or suspected terrorist, the relevant terrorist screening Presidential Directives alternatively use the phrases “appropriately suspected” (Homeland Security Presidential Directive (HSPD)-6, “Integration and Use of Screening Information to Protect Against Terrorism”, issued September 16, 2003), “reasonably suspected” (HSPD-11, “Comprehensive Terrorist-Related Screening Procedures,” issued August 27, 2004), and “articulable and reasonable basis for suspicion” (HSPD-24, “Biometrics for Identification and Screening to Enhance National Security”, issued June 5, 2008). HSPD-24 expressly builds upon HSPD-6 and HSPD-11 and represents the most recent explanation concerning the policy of the United States regarding the types of individuals who pose a threat to national security that should be identified and screened to better protect the American people. Consequently, the TSC Policy Board Working Group believed that “reasonable suspicion” best articulated the standard of review as set forth in the relevant terrorist screening presidential directives.

The U.S. Government did not choose to invoke a Fourth Amendment standard and does not consider watchlisting to be a search or seizure under the Fourth Amendment.

The Homeland Security Deputies Committee reviewed and approved the reasonable suspicion standard and its accompanying guidance in January 2009. TSC then finalized the Updated Protocol which it issued in February 2009.

**Responses to Questions for the Record from Patricia Cogswell
Submitted by Representative Steve King**

Question: When there is a dispute between the State Department, which is tasked with building diplomatic relations, and DHS which is tasked with ensuring national security, as to whether or not a visa should be issued, who has the final say?

Response: The Departments of State and Homeland Security share the goals of ensuring the safety of our country. We work together to try and help determine who may pose a threat to our nation and ensuring that those individuals are not able to obtain a visa or enter the United States.

During the creation of DHS, Congress gave DHS certain responsibilities with respect to visa policy and the issuance process. Specifically, section 428 of the Homeland Security Act (HSA) of 2002 authorized the Secretary of Homeland Security to: administer and enforce the Immigration and Nationality Act (INA) and other laws relating to visas; to refuse a visa for individual applicants in accordance with law; assign DHS officers to diplomatic posts to perform visa security activities; initiate investigations of visa security-related matters; and provide advice and training to consular officers.

DHS's Visa Security Program (VSP) plays a significant role when there are concerns raised about granting a visa to a particular individual. VSP places ICE special agents (DHS law enforcement officers) in U.S. embassies and consulates to work collaboratively with Department of State (DOS) consular officers and Diplomatic Security Agents to administer the visa adjudication process.

ICE now has VSUs at 14 high-risk visa adjudication posts in 12 countries. At these 14 posts, in fiscal year 2009, ICE agents working with their DOS counterparts screened nearly 905,000 visa applicants and, determined that more than 300,000 applicants required further review. Following subsequent inquiry and investigation, ICE and DOS jointly recommended refusal of over 1,000 applicants. In every instance, DOS followed the VSU recommendation and ultimately refused to issue the visa. VSP recommendations have also resulted in visa revocations by DOS.

Question: How many individuals who have been screened by the DHS Visa Security Units have been given U.S. visas and then committed or attempted to commit terrorist attacks in the United States?

Response: DHS has no information suggesting that this has ever occurred.

Question: ICE's Visa Security Program (VSP) has identified 57 visa adjudicating posts as

high-risk. I also understand it costs approximately \$1.7 million to set up a Visa Security Unit at a visa-issuing post overseas.

Why then does the Administration's proposed budget only request \$7.3 million for the VSP in FY 2011?

That amount would only cover 4 additional Visa Security Units not even a dent in the 57 posts where VSUs are needed.

In the wake of the Christmas bombing incident does DHS now support increasing the amount requested in the budget for the VSP?

Response: In fiscal year (FY) 2010, ICE received two-year money that will be used to deploy four additional posts and expand positions in two existing posts.

For FY 2011, the President has requested the same level of funding and resources as FY 2010, which will cover existing VSUs, (including the planned locations and positions from the FY 2010 expansion), and will establish a new office in Saudi Arabia.

ICE is continuing Visa Security Program (VSP) deployment in accordance with the 5-year VSP Expansion Plan, which received approval and support across ICE, DHS, the Department of State and the White House Homeland Security Council, and supports the *National Implementation Plan* on the War on Terrorism. The expansion process requires close coordination with the host country and the Department of State, through the NSDD-38 process, based on the reality of limited space in embassies for which many agencies compete. While continuing this modest expansion, ICE is coordinating with the Department of State to collectively advance visa security more broadly.

