AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 111–598

THE STATE OF AVIATION SECURITY: IS OUR CURRENT SYSTEM CAPABLE OF MEETING THE THREAT?

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JANUARY 20, 2010

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

56–411 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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE McCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico
MARK WARNER, Virginia
MARK BEGICH, Alaska

KAY BAILEY HUTCHISON, Texas, *Ranking*
OLYMPIA J. SNOWE, Maine
JOHN ENSIGN, Nevada
JIM DeMINT, South Carolina
JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
GEORGE S. LeMIEUX, Florida
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MIKE JOHANNS, Nebraska

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
ANN BEGEMAN, *Acting Republican Staff Director*
NICK ROSSI, *Republican Chief Counsel*
BRIAN M. HENDRICKS, *Republican General Counsel*

CONTENTS

	Page
Hearing held on January 20, 2010	1
Statement of Senator Rockefeller	1
Statement of Senator Hutchison	5
Prepared statement	6
Statement of Senator Dorgan	8
Statement of Senator DeMint	9
Statement of Senator Lautenberg	11
Statement of Senator Thune	12
Prepared statement	13
Statement of Senator Begich	35
Statement of Senator Snowe	43
Prepared statement	47
Statement of Senator Klobuchar	48
Statement of Senator LeMieux	51
Statement of Senator Ensign	53
Statement of Senator Cantwell	55

WITNESSES

Hon. Janet Napolitano, Secretary, U.S. Department of Homeland Security	14
Prepared statement	16
Hon. Michael E. Leiter, Director, National Counterterrorism Center	21
Prepared statement	24
Hon. Lee Hamilton, Co-Chair, National Security Preparedness Group, Bipartisan Policy Center, and former Vice Chairman, National Commission on Terrorist Attacks upon the United States (9/11 Commission)	25
Prepared statement	27
Hon. Tom Kean, Co-Chair, National Security Preparedness Group, Bipartisan Policy Center, and former Chairman, National Commission on Terrorist Attacks upon the United States (9/11 Commission)	31
Prepared statement	27

APPENDIX

American Civil Liberties Union (Michael W. Macleod-Ball, Acting Director, Washington Legislative Office and Christopher Calabrese, Legislative Counsel), prepared statement	67
Response to written questions submitted to Hon. Michael E. Leiter by:	
Hon. Mark Warner	73
Hon. Mark Begich	73
Hon. Kay Bailey Hutchison	74
Hon. Olympia J. Snowe	75
Response to written questions submitted to Hon. Janet Napolitano by:	
Hon. John D. Rockefeller IV	76
Hon. Bill Nelson	77
Hon. Frank R. Lautenberg	77
Hon. Mark Warner	78
Hon. Mark Begich	80
Hon. Kay Bailey Hutchison	81
Hon. Olympia J. Snowe	83
Hon. Johnny Isakson	85
Hon. David Vitter	86

Page

Response to written questions submitted to Hon. Lee Hamilton and Hon. Tom Kean by:
Hon. Frank R. Lautenberg 90
Hon. Mark Warner 90
Hon. Mark Begich 90
Hon. John Ensign 91

THE STATE OF AVIATION SECURITY: IS OUR CURRENT SYSTEM CAPABLE OF MEETING THE THREAT?

WEDNESDAY, JANUARY 20, 2010

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to the notice, at 2:30 p.m. in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. This hearing will come to order.

I want to thank our witnesses for coming today. There are other hearings on this matter, and I'm really glad of it. Some of you are going to have to do a lot of traveling to a lot of committees, but I'm really glad of that, too. People need to hear from you. And, in fact, you look a long way off.

Secretary Napolitano, I welcome you back to the Committee. I think that you have one of the hardest jobs in America; maybe second or third hardest. The President wins on that. You and Mike can fight out who's second and who's third. I think you are doing a terrific job that—I think your—you personally are underappreciated. I think your department is underfunded. And I think this instant may help us solve that underfunding problem. Your problem doesn't have to be solved. As I told you before, as the hearing, just a few moments ago, started, as far as I'm concerned, you wear four stars on each shoulder.

Director Leiter, this is the first time circumstances have combined to have you testifying before the Commerce Committee. You're a very lucky man. As Chairman of the Intelligence Committee, I had the pleasure of working with you on matters relating to intelligence reform. And, as you know, I expressed my feelings then, how impressed I was at the job that you were doing then and you are doing now.

We've had a very serious problem. There's the question of accountability; that's a hard thing to solve. It's also sometimes not a wise thing to solve in the first few minutes in public. Sometimes it's good to know what you're talking about before you get into that.

And I know my colleagues will recognize your tremendous, profound expertise in understanding what it takes to meet our respon-

sibilities. So, I am very grateful that you are here before our committee, and that you serve as you do.

I know that you've been working around the clock. I've been a Governor, but I don't think even that comes even close to the pressure that both of you—a Cabinet Secretary, NCTC, et cetera—that what—what that amounts to in the way of pressure, sleeplessness, trying to find out how we can do better. That's the purpose of this hearing.

We're going to stay on this subject most of this year. We're going to get it right. This is a very serious thing that happened. The fact that nobody was killed and nobody was particularly injured, except perhaps the perpetrator and one or two others in a minor way, belies the fact that, had things gone according to the way they were meant to, 289 people would have died 20 minutes outside of Detroit. I tend to think of it in terms of what I just said, as opposed to the fact that nothing happened, and I think that's the way you look at it, too.

Lee Hamilton and Tom Kean, you are welcome anywhere, anytime, and you're an asset to the Nation, both of you. Maybe you're just one person; I don't know.

[Laughter.]

The CHAIRMAN. But, you have brought more wisdom and challenged us in more ways. I asked each of you to be tough on us in your questioning—answer to questions, or matters that you want to raise, because this is the time for us to hear clearly from those who have watched wisely from the outside, but really on the inside. Thank you, again, for coming.

OK. So, the Christmas terror attack told us that we need to further harden our defenses and evaluate if we're doing everything we can to meet an evolving al-Qaeda terrorist threat or perhaps non-al-Qaeda terrorist threats. Domestic problems, discontent, all of the instability that rules throughout our country, fear—throughout the world—the fear, the hopelessness, all of this combines to produce exactly the wrong kind of people doing exactly the wrong kinds of things, but they think it's for the right reason. And if they seek martyrdom, it's pretty hard to argue and win them over.

The threat to America is real and we have to get it absolutely right. And our problem, of course, is that we have to get it right 100 percent of the time. Their problem is, they have to get it right once. And it's not fair. But, that's the world we live in, and that's what we need to deal with on this committee, as well as other committees.

A man with a bomb was able to board a plane headed for America. So, it's obvious and clear that our system failed. Cannot be disputed. I know that, every day, countless unsung American heroes are working in your agencies, working 17-hour days, 7 days-a-week, and going through every scrap of information. People have no idea—it's actually—it's classified—people have no idea of the amount of information that comes in each day to the various intelligence agencies. And you get the brunt of it, Director Leiter.

And so, the question is, how do you pick one thing from another? And the answer is that it seems to be impossible, and that can't be the answer; the answer is: We've got to get it right.

How come this guy had—got a visa? How did he get a visa? How come it was his—what he said—what his father told to the American Embassy was not considered a clarion call? Potential answer: All those things come in all the time. Other potential answer is: We should have hearkened to that and responded to that and made sure that he never got on an airplane.

So, I tremendously value—I'm still on the Intelligence Committee, and I still do—the people that work so hard to try to get it right. Seven men and women of the CIA recently killed in Afghanistan. They don't make it home.

So, while we have a responsibility to be frank about where we've fallen short, we must also honor their service. I want that to be very, very clear. We can do that by building on the progress that we've made since the 9/11 attacks, with an eye toward making smart and specific improvements that keep us safe. Easy to say, hard to do.

Nine years ago, our intelligence agencies did not even share information, largely because they could not, by law. First bill that we passed, "Yes, CIA and FBI, you can talk to each other." Stunning. Less than a decade ago. And their information systems weren't interoperable. Part of that's true still today. And because they would not, agencies too often preferred to stovepipe information rather than share it. That was the past. How much is that of the present? We will talk.

Since then, as Mr. Leiter will testify, we have made enormous strides. Today, our systems and practices are far superior to those that were—allowed 19 men to execute the global plan to commit the horrific acts of 9/11. But, we're not fail-safe; we haven't gotten there yet.

And yet, just weeks ago, our system still allowed a terrorist to board flight 5—253 with sophisticated explosives. This was a grave and multilayered failure. The intelligence community did not piece together clues about this man's connections to terrorism; clues that were available, including from his father. It's my general impression it's—it doesn't fall within the habit of Islamic behavior, for a father to go in and, in a sense, give up his son, or even more, for us then to ignore it, that being such a unique and stunning thing for a father to do.

The State Department and the Department of Homeland Security allowed this man to board the airplane with a valid U.S. visa. The Brits hadn't given him one a couple years before. We gave him one that lasts for 2 years. And the international airport screening that we depend on did not detect this man was carrying a potentially devastating explosive device.

One of my questions, Madam Secretary, is going to be about the meeting that you take off for tomorrow, the 21st and the 22nd, with Europeans. How do we—in this tiny, tiny, little world, how can somebody just pass through Amsterdam without any American eyes alighting upon him or her or what their situation might be?

So, we have a responsibility to be brutally honest about where we have fallen short. We have to do better. And the basic fact that will drive much of this committee's work in the year ahead is trying to make it all better. I promise you that. I promise my col-

leagues that. We have to do better protecting our families, safeguarding our communities, and securing our Nation.

Nobody was injured, nobody was killed. Not in my head. Malfunctioned, 252 would have died. So, this is at the top of our agenda for this year, bringing the attention, the resources, and the leadership needed to provide an improvement in our citizens' safety and security. This committee intends to continue asking the tough questions to shape the policies that guide transportation security in all of its modes. And by that I mean our port security, our chemical security, our cybersecurity. And the list goes on. We have oversight of that here. Have we exercised it sufficiently? Perhaps not.

Today's hearing on aviation security represents an opportunity to bring to the table key issues that demand all of our attention. And I want to invite my colleagues to bring their new ideas as we work together to develop concrete solutions that advance our security efforts and make us safer.

Let me end with five suggestions, some key solutions I believe we can and must seriously consider:

Requiring U.S.-bound aircraft and international airports to meet more rigorous security requirements and not letting our cumbersome international negotiating, as a process, slow us down. Is that possible? According to international protocol, it is not. It has to be possible. We cannot talk this thing to death. We are a tiny little globe, interlocked.

Two, engaging a major new effort to develop and deploy advanced imaging technologies, which means more money, more accuracy, and getting serious about stopping any programs that do not work. So, then we have the question of civil liberties versus national security. Forever a problem; forever, rightly, a problem. But, we cannot tread lightly on what we do on national security.

Three, improving and, in some cases, mandating better information-sharing among TSA intelligence agencies and even commercial airlines. I invited an airline to be at this hearing today. They declined. They declined. I was not happy. And I don't know what that tells us, but it tells us that we're all in this together, and everybody has to do their part, and nobody has a safe haven. We need to do more to establish the partnership between government and the private sector when it comes to security.

Four, making the watch list more accurate on the one hand, and more dynamic on the other. Expanding the universe of people who receive secondary screening. I'm a believer in that. Reevaluating our screening criteria. And then doing something called "educating the public" in advance about what may become more stringent scrutiny at airports. Our public understands this very well. They've been through the beginning of TSA. They've been through shoe bomber and taking off the shoes. Have they liked it? No. Have they complied with it? Yes. Because they understand what the stakes are. So, we need partnership with the flying public also.

And finally, number five, requiring coordination between the valuable resources we have at our embassies, especially our regional security offices, and the TSA to identify threats emanating from overseas airports. Believe it or not, this is not always happening today. And it did not happen in this case.

This is not an exhaustive list, but it's something to start with.

All of this obviously is going to require raising new revenues. That's always a problem in the U.S. Senate. But, doing nothing is not an option. I don't know how you improve security. I don't know how you put in better machinery. I don't know how you get to the WBIs—not just 40, but the 900 you want by 2014—without more money, more training for our security people.

So, the need is clear and transparent. The way is hard and difficult. But, it is our obligation.

I look forward to our witnesses' testimony as we work together and make our transportation system as safe as possible.

Just—Madam Vice Chair, if I can just say that I'm sure that our colleagues all know that Erroll Southers withdrew his name for head of TSA today. And our national security system has lost a skilled law enforcement officer who had needed expertise and leadership qualities, because of—I would call it "political games," but, I'm not going to—I'll just scratch that from the record. Anyway, it's a real shame. It's a real shame. So, now we've got to go out and find another one, and vet them in the way that Americans can, which takes a long time. We don't have a long time. I'm confident that the President will very quickly nominate a new candidate to run TSA, and I'm committed to seeing that that person gets through the process.

I thank you, and I thank my colleagues for their patience.

And I turn now to Senator Hutchison, for her opening statement.

STATEMENT OF HON. KAY BAILEY HUTCHISON, U.S. SENATOR FROM TEXAS

Senator HUTCHISON. Thank you, Mr. Chairman.

Mr. Chairman, I would just say that I believe there were legitimate concerns about Mr. Southers, and I think those concerns deserved to be investigated. So, I hope that we can move forward with a new nominee, because we certainly need an experienced person in that position. But, it also needs to be a person who would assure the respect of the people in the agency to have the authority to assure that the agency is doing its job.

I do think that every one of the witnesses have done a lot to try to put America in a place where we can be more secure. I think the members of the 9/11 Commission certainly have given many volunteer hours to give advice, early on, after 9/11. And I think the members of our administration, as well, are working very hard. No one disputes that you are doing everything that you know to do. But, I think now we need to look at what has happened and learn from that. We need to go forward in a constructive way.

The plot that unfolded on Christmas Day just shows that the defense of our homeland from terrorists is dependent on information collection and sharing, intelligence analysis, and the vigilance of our security personnel, and that none of these can be effective without the others. And if there is anything that we have learned from the experience that happened in my home state at Fort Hood, and then this one, on its heels, it's that we're not sharing enough. And what the Chairman said about, after 9/11, saying, "Oh, yes, our intelligence agencies can actually talk to each other," that is a very small first step. And we need to perfect that, and quickly.

The President's own initial review has concluded that, if our intelligence analysts had pieced together the information at their disposal about the attempted bomber, there would have been sufficient grounds to place him on the terrorist watch list, perhaps averting what happened.

Going forward, I think that we need to look at several things:

We need to look at expanding the number of known or suspected terrorists and their associates who are placed on screening lists even though, in the short term, this may result in more mistaken matches.

Number two, I think we need to expedite the adoption of programs that will aid the process, such as the complete implementation of the Secure Flight Program, which will take the ultimate screening responsibility away from air carriers and place it completely within the TSA, which has more access to intelligence than private airlines, making our screening efforts more effective. Progress on that program has been positive of late, but we need to move faster, if we can.

And number three, I think it is very important that we better synthesize intelligence data, especially in relation to associates of known terrorists or those who may be connected to potential terrorist threats.

Since 9/11, we have been in a new era of conflict. However, recently we have seen a series of disturbing changes in our fundamental mission of how we deal with terrorists and terrorist threats—most starkly, in the decision to bring the perpetrators of the 9/11 attacks to New York for civil trials in our courts and the closing of Guantanamo Bay.

Mr. Chairman, this country and its leaders need to remember that we are at war with terrorists and extremists who mean us harm. This is not a war of traditional means, and should not be dealt with through the civil process. We should have an approach that is committed to more vigilance and flexibility and enables our intelligence and security personnel to utilize all the tools at their disposal for the purposes of eliminating the threat to this Nation.

So, this is not a blame game, but it is, I hope, an opportunity for us to talk to you, for you to talk to us, and for all of us to come to the conclusion that we must be more vigilant in pursuing the people who wish to do us harm. And even in today's newspaper, they are talking about recruiting more Americans for these terrorist activities in Yemen, and they are focusing on blond hair and blue eyes so that it is not someone who would raise flags.

So, we've got a problem that we need to confront together, and I hope that we can learn from our hearing, from the hearing you had this morning, and that we can have the confidence that we're all going on the same track.

Thank you, Mr. Chairman.

[The prepared statement of Senator Hutchison follows:]

PREPARED STATEMENT OF HON. KAY BAILEY HUTCHISON, U.S. SENATOR FROM TEXAS

Mr. Chairman, thank you for calling this hearing. The Christmas Day terrorism incident is a bleak reminder of the ever-evolving nature of terrorist threats against the United States.

The plot highlights the fact that the defense of our homeland from terrorists is highly dependent on information collection and sharing, intelligence analysis, and

the vigilance of our security personnel, and that none of these can be fully effective without the others. The Transportation Security Administration (TSA), Department of Homeland Security (DHS) and other critical Federal Agencies have very difficult tasks, but they must do a better job of gathering, identifying and properly utilizing all intelligence information.

The President's own initial review has concluded that, if our intelligence analysts had pieced together the information at their disposal about the attempted bomber, there would have been sufficient grounds to place him on the terrorist watchlist—perhaps averting his attack.

As it stands, we owe a large debt of gratitude to the brave and conscientious passengers and crew members of Flight 253, who subdued the would-be bomber.

But, we should not need to rely on the heroism of airline passengers to keep us safe. We have a complex and multi-layered aviation security system and many of the threats against our transportation system can best be addressed through effective security policies and the use of advanced technology. However, it is just a basic fact that no technology is a silver bullet and all technologies have their limitations. They are simply one of many obstacles a would-be terrorist must account for.

Moving forward, the TSA needs to bolster existing layers of security, and that means fostering effective and innovative technologies and deploying them rapidly. It will also likely mean expanding the number of known or suspected terrorists and their associates who are placed on screening lists, even though—in the short term—this may result in more mistaken matches.

We need to expedite the adoption of programs that will aid the process, such as the complete implementation of the Secure Flight program, which will take the ultimate screening responsibility away from air carriers and place it with the TSA, which has access to more intelligence than private airlines, making our screening efforts more effective. Progress on that program has been very positive as of late, but if we can move faster, we should.

In addition, the Administration needs to be more assertive on an international level with foreign nations that serve as gateways to our country. We need to tighten aviation security rules and procedures without unnecessarily impeding air travel domestically and internationally.

Finally, and most importantly, we need to better synthesize intelligence data, especially in relation to 'associates' of known terrorists or those who may be connected to potential terrorist threats.

I think we all appreciate the difficult job our intelligence community has deciphering meaningful information from the proverbial 'noise,' but I believe we can and should do better. All our security tools and watchlists are only as good as our intelligence collection and our analysis of that intelligence as a whole.

Since 9/11, we have been in a new era of conflict. However, recently, we have seen a series of disturbing changes in our fundamental mission of how we deal with terrorists and terrorist threats—most starkly in the decision to bring the perpetrators of the 9/11 attacks to New York for civil trial.

Mr. Chairman, this country and its leaders need to remember we are at war with terrorists and extremists who mean us harm. We need to be acting like it and responding accordingly through our policies. This is not a war of traditional means and should not be dealt with through civil process and understanding. This war calls for a novel approach that allows us to be more vigilant, flexible, and enables our intelligence and security personnel to utilize all the tools at their disposal for the purposes of eliminating the threat posed to this Nation.

Thank you, I look forward to the testimony.

The CHAIRMAN. Thank you, Madam Vice Chairman.

And I'd just say to our members that I want the following Senators, who I've spoken to, to make statements, each 5 minutes or less. And I hope that others will understand. These are the people who are chairmen and ranking on the relevant subcommittees.

So, I want to start with Senator Dorgan, and then I want Senator DeMint, then I want Senator Lautenberg, and then I want Senator Thune to make statements.

So, we'll start with Senator Dorgan. And I hope others will understand.

STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. Mr. Chairman, thank you. I'll try to be very brief.

You know, this is one of those very important issues in which failure is not an option. And we had, on Christmas Day, something that was near-tragic for a lot of passengers on that airline. And fortunately, the terrorist attack that day failed to achieve the objective.

But, what I want to understand is a couple things. Number one, I think there was a screening failure. The question is, what do we do to—what do we need to do to better screen passengers, balancing it with privacy and so on? And the second is the intelligence failures. What has caused the intelligence failures, especially inasmuch as we put together a DNI to end stovepiping and so on, and clearly that didn't happen here.

Harry Truman, famously, had the sign, "The buck stops here." The question with all of this, for me, is, where does the buck stop with respect to these failures?

And I want to just hypothecate. If we were thinking forward here, and it's today, and we have some information about a couple of weeks from now, and it's a father of a young Nigerian that comes to our intelligence community overseas, and says, "Look, my son is engaged with some bad people. I'm worried about what he might or might not do." He is then put on a watch list, but not on a No Fly List. Nobody checks to see that he has an open visa and cancels the visa. So, here's someone whose father thinks, apparently, he's a potential terrorist or something of that nature, and he's put on a watch list, but, again, not on a No Fly List, and continues an open visa, and there are three intercepts in the next few weeks or so. Two of the—one of them is that a man with the first two names of this person has volunteered for some coming operation; that was an intelligence intercept, I understand. Another intercept would be a Nigerian man being groomed for an operation. And the first intercept actually used the first two names of this young man. The third intercept, in December, mentioned some type of operation on December 25. And then a young man shows up and pays cash for an airline ticket to go from Ghana to—as I understand it—to Amsterdam, to Detroit, and then shows up and boards the plane with no luggage.

So, this isn't looking for a needle in a haystack; this is looking for a big old needle right in the middle of our hand. And the question is, would we see it next time? Because we didn't see it this time. And that is, in my judgment, an unbelievable failure. So, the question is, Where does the buck stop? Who's accountable for that? Because that—it is one thing to say the system failed. But, we're not talking just about systems; we're talking about people who manage and operate the systems, and who have to be accountable for making sure the systems work. Because failure is not an option. And we have constantly, as all of us know, dealt with the last issue—the last issue of the box-cutter, the last issue of the shoe bomb, the last issue of liquid containers, the last issue of sewing plastic explosives in the underwear. It is constantly the last issue. But, much more important than that, in this case, is the question

of, How did we miss so many circumstances, where you actually have a name, and a father describing a son, and a circumstance with three intercepts that talk about a day and the name, and No Fly Lists that aren't coordinated with watch lists, and visa—open visas that aren't coordinated with a watch list? You know, something just doesn't add up at all. So, and I think—my hope is that through this hearing we can understand, What doesn't add up, why doesn't it add up, and where does the buck stop? That's what's important.

So, two issues: How do we better screen? What kind of screening is necessary? What does it cost? How intrusive is it? All of those issues are things we have to talk about. And then, second, what about this unbelievable—to me—issue of intelligence?

I say all of that without denigrating you all. This is a tough job. But, still, I think you and us need to understand what failed and who failed and who's accountable.

The CHAIRMAN. Thank you, Senator Dorgan.

Senator DeMint.

STATEMENT OF HON. JIM DEMINT,
U.S. SENATOR FROM SOUTH CAROLINA

Senator DEMINT. Thank you, Mr. Chairman.

I want to thank Chairman Dorgan for his work in airline safety. You've been a real proponent for many months, long before Christmas, to improve airline safety, and your expertise will be missed.

I want to make a couple of points. I appreciate all the witnesses being here today.

First, I'd like to talk about the Transportation Security Administration. And anytime we implement any change in Homeland Security, TSA, anything related to that, the first question needs to be, how will it improve security? And I've been very concerned, as the Secretary knows, that the Administration has a priority of subjecting our TSA security officers to a collective bargaining regime. No one has yet to give any security reason why collective bargaining should be adopted. Employees are not mistreated. We will not add any flexibility or any benefit. It's clearly a political agenda. And frankly, for me, even though I appreciate what the President has lately been saying, and what has come out of Homeland Security—those things have been encouraging—it's hard for me to take commitments to security seriously as long as forcing TSA into collective bargaining is a priority, because it makes no sense.

Last month, I asked the Secretary how collective bargaining at TSA will improve security. Her answer was that the two weren't mutually exclusive. Her answer was not that it would improve security. And I think anytime when the Secretary of Homeland Security can't tell us how a change in homeland security is going to improve security, it should stop us all in our tracks.

Our security agents now are free to join a union, and the union can advocate on their behalf. But, we all know that collective bargaining is very different; it creates a third-party structure to which our security system has to answer to. Collective bargaining will impose a 19th-century industrial personnel management model to a 21st-century information age threat.

The threat we see in the aviation sector is a creative and nimble threat. These are words the President has used. Our response needs to be nimble and creative. We need to continually improve what we do at TSA. The men and women who protect the aviation sector need to be able to respond quickly to change—to change in the counterterrorism tactics so that we can thwart the tactics of our adversaries and protect passengers. And they need to be able to do it without having to get signoff from the labor unions. The Secret Service, Coast Guard, the military, the FBI—they realized this long ago, and they prohibit collective bargaining.

Let's not be fooled by some of the arguments that we hear, that collective bargaining works in other areas of homeland security. The most immediate past director of Customs and Border Protection is on record saying that collective bargaining made it much more difficult for him to do his job. He had to negotiate staffing policy with labor unions and had to discuss security policy with the unions that was better kept internal.

Quite simply, our security policy needs to be focused on improving security. It can't be subjected to a union middleman. The only concern career professionals at TSA should have when responding to a terrorist threat is, "What best meets the threat?" Not "What best meets the needs of a labor union."

Let me shift focus just a minute to talk about a couple of other things:

One is behavioral targeting. In addition to not going backward with this idea of collective bargaining for TSA, where it has been prohibited, we need a more modern approach to screening. The behavioral screening approach used by the Israelis provides a good model, and it's something that we should take a closer look at. TSA continues to focus on keeping bad things off of airplanes. The Israelis, for example, focus on keeping bad people off of airplanes. Terrorists will always find a weapon, whether it be in a bottle of alcohol purchased at a duty-free store or two strategically placed laptop batteries. If we focus on things instead of terrorists, we're going to lose this war.

To be clear, I'm referring to assessing an individual's behavior, to separate the terrorist from the traveler. Additional random screening will never be as successful as targeting the bad guys. Behavioral profiling is a vital and common sense tool to increase security that we could use more effectively. And I hope we can talk a little bit about that today.

Just one other point, Mr. Chairman, on visas. The Christmas bomber highlighted the need for across-the-board reform of the visa process. We need to make it faster and easier to revoke visas. Traveling to the United States is a privilege; it's not a right. Currently, unless the applicant comes from a country designated as a sponsor of terrorism, the information threshold required for denying a visa may be too high. This issue needs to be addressed quickly for both immigrant and nonimmigrant visas. America can be a safe and welcoming nation at the same time. We do not have to sacrifice security for expediency.

I am also concerned that when security advisory opinions have been requested, some types of visas have actually been issued before all of the relevant intelligence agencies have had a opportunity

to respond. Security has to be a priority, and policies that discourage information-sharing and weaken security must be changed. If we want to enhance security, we have to collect, analyze, and quickly act on that information. The American people deserve to know why this terrorist was not added to the No Fly List and what we intend to do to keep terrorists not only from getting visas, but from gaining access to our country altogether.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

And Senator Lautenberg.

STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Thanks, Mr. Chairman.

If I might just take a moment to say that we have an outstanding group of witnesses at our—at the table, but I am particularly pleased to see former Governor Kean, from New Jersey, and Lee Hamilton, who co-chaired the 9/11 Commission Report. And it was a major piece of work in response to the worst attack ever on our country. We're glad to see them here.

During—the incident over Detroit wasn't the only urgent wake-up call about a major lapse in our national aviation security network that has been recently revealed. During what was supposedly a period of heightened aviation security at an airport—Newark Liberty Airport—that lies within the 2-mile stretch deemed to be the most the most at-risk place for terrorism—that's by the FBI—a man was able to break through security by walking unchallenged into Terminal C of Newark Airport. This breach of security was intentional and shockingly easy. The inexcusable breach occurred when a TSA guard turned his back for a moment and a watching individual took the opportunity to dash under a security tape, into the airport, completely unchecked and unscreened. Without a vigilant traveler's alert to the TSA, we would never have known that the breach occurred.

And even after TSA was alerted, it took 2 hours for them to alert law enforcement people—the police there—to verify the breach on videotape and to take action. Two hours. When a potential terrorist could have been conspiring, with a plan or a weapon, to bring down an airplane. Two hours. When a potential terrorist could have been bird-dogging for a bigger plot.

And while the motives of the man behind the Newark breach may seem benign, this incident was not just as it was portrayed, a playful reunion. The result was a major security breach that shut down an entire terminal of a major airport for more than 6 hours and delaying more than 16,000 people from getting to their families, friends, or final destination. It caused over 100 flight delays and 27 flight cancellations.

And since 2002, DHS has spent $1 billion on technology to screen passengers coming into an airport terminal. But, all of that screening technology is useless if someone can just walk in through an exit without being noticed. This exit at Newark Airport had security cameras operated by TSA. But, the principal camera had been broken for almost a week. TSA knew about the broken camera and failed to report it.

The cameras weren't the only things that broke down; there was a complete communications breakdown between TSA and its partners on the ground, the Port Authority and Continental Airlines. Fortunately, the Continental Airlines camera nearby was effectively recording during this time. TSA still failed to notify the Port Authority police of this breach.

And we can be sure that terrorists are—observe actively the kind—this kind of a free passage for plans that they may have.

A security breach of this nature is a matter of national security and needs to be treated that way. And that's why I'm taking action today to introduce legislation to close the dangerously—the dangerous security gaps exposed by the breach at Newark Airport.

My legislation mandates that all airport terminal checkpoints and exits have working security cameras. It will require sufficient personnel at secure area exits. If someone purposely breaches airport security, under my bill they will face serious consequence; not, as is suggested, a $500 fine, which is nothing more than a tap on the wrist that makes a joke out of the security structure. I'm going to be working with DOJ and DHS to make sure the Federal Government gets involved in enforcing the law and handling major aviation security breaches instead of ceding this responsibility to State or local authorities.

The incidents at Newark and Detroit exposed fundamental weaknesses in our aviation security system. And if we learn from these events and treat them with the seriousness they deserve, I'm confident that we can say to all Americans who want to fly, "You're safe as safe can be made."

And with that, I thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Lautenberg.

Senator Thune.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you Mr. Chairman. I want to thank you and Senator Hutchison for holding this very important hearing.

And I also thank our panelists for being here today, and would echo what's been said about Congressman Hamilton and Governor Kean, and your good work, and we appreciate the many contributions that you have made in looking carefully at this in great detail, making recommendations about how to do a better job.

I do have to say that I think the initial reaction to this, that the system worked, could not have been more wrong. And it seems, to me at least, that there were significant breakdowns and failures in the system, and those need to be corrected or this is going to happen again. And I think the people on Flight 253, and the crew, can be very thankful that the explosive failed to detonate. But, that doesn't, for a minute, suggest that there aren't going to be other efforts made, by those who would want to kill Americans, to somehow get into our system and have access to Americans and airplanes and other forms of transportation that they can use to try and kill and disrupt and damage America and our interests.

So, we need to get this fixed. One of the things that I appreciate both Congressman Hamilton and Governor Kean have had to say is that we do have to recognize that one of the greatest threats that

we face in this country, when it comes to air travel, is public complacency, particularly following the stepped-up security protocols following 9/11. I appreciate that you recognize that in your testimony.

I think we all have to figure out where the intelligence and other human errors occur that failed to stop Mr. Abdulmutallab from entering the United States. It's pretty clear that there was a failure when it comes to sharing intelligence, a failure when it comes to analyzing intelligence.

I share the observation of the Senator from South Carolina, that the focus of this effort really needs to be on terrorists.

I'm interested in hearing, Secretary Napolitano, from you, and from Mr. Leiter, about what's being done to adjust the process by which names are added to the No Fly and Selectee Lists, and what, if any, technological barriers exist when it comes to subjecting airline flights to the larger subset of the TIDE database, the 550,000 names, because clearly there has got to be a better job when it comes to screening and identifying people who are already on these lists, and making sure that they're not getting this kind of access.

The other issue I'd be interested in hearing about is how often there have been suspended flights into the United States due to insufficient security standards that are employed by foreign countries. I know we have TSA people that are looking at those, but, it seems, to me at least, that is another area where there were serious breakdowns in the process this time around.

So, I appreciate the hearing, Mr. Chairman. I'm anxious to hear from our witnesses.

This is a critically important issue, and we need to do everything we can to double down our efforts to make sure that these types of incidents don't happen again in the future.

Thank you.

[The prepared statement of Senator Thune follows:]

PREPARED STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Mr. Chairman and Ranking Member Hutchison, I appreciate you calling today's hearing and I appreciate the panel of witnesses that have joined us today to talk about a very serious matter.

Without question, the 289 passengers and crew of Flight 253 have much to be thankful for as a result of the failed detonation of explosives on Christmas Day. However, the events that resulted in Mr. Abdulmutallab being permitted to fly into the U.S. have sparked a very serious discussion both here in the United States and across the globe when it comes to passenger safety and security.

As I noted last fall when this committee held a hearing regarding the TSA, *the greatest threat that we face as a country when it comes to air travel, is public complacency following the stepped up security protocols following 9/11,* I was pleased to see that both Congressman Hamilton and Governor Kean noted such in their testimony.

While it is clear that intelligence and other human errors failed to stop Mr. Abdulmutallab from entering the United States, I will keep my remarks brief in the interest of hearing from our witnesses and asking questions following their remarks. Thank you Mr. Chairman.

The CHAIRMAN. Thank you, Senator Thune.

I want to both explain and apologize to our witnesses. We do this—and there are a number of people, in addition to those who spoke here on the dais, who want to say things. We can't. What we would traditionally do is, we have the relevant Subcommittee Chair

and Ranking Members say a word. You, in turn, have to listen to that. But, on the other hand, they made some pretty good points.

So, I would now call on Secretary Napolitano. We welcome your statement.

STATEMENT OF HON. JANET NAPOLITANO, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Well, thank you, Chairman Rockefeller, Senator Hutchison, members of the Committee, for the opportunity to testify on the terrorist attack aboard Northwest Flight 253 on Christmas.

I am pleased to be here today with Director Leiter, with Governor Kean, and with Representative Hamilton.

Now, as President Obama has made clear, this Administration is determined to find and to fix the vulnerabilities in our systems that allowed this attack to occur on Christmas Day.

Our country's efforts against terrorism include the actions of the Department of Homeland Security and many other agencies, as well as those of our international allies. So, I'd like to focus my statement, Mr. Chairman, on the DHS role within these larger efforts.

First, by and large, DHS is a consumer of the United States Government's Consolidated Terrorist Watch List which we use to help keep potential terrorists from boarding flights and to identify travelers who should undergo additional screening. Within the United States, DHS performs physical screening at airport checkpoints and provides further in-flight security measures. Outside of the United States, we must work with foreign governments and airlines to advise them on which passengers may prove a threat and require security measures for flights bound for the United States. As you know, TSA does not screen people or baggage at international airports.

Now, regarding the Christmas Day attack, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with explosives on his person. The interagency process to fix these vulnerabilities, highlighted by this attack, is well underway. And as a consumer of terrorist watch list information, DHS welcomes the opportunity offered by this process to contribute to improving our Federal Government's ability to connect and assimilate intelligence. And we are working with the NCTC, with the OD&I, and others to do that.

We're also focused on improving aviation screening and expanding international partnerships to guard against a similar type of attack. I believe several of the members have made inquiry about that.

So, I have submitted a longer written statement describing these various programs that work to keep terrorists from boarding planes, and ask that it be put in the record.

In terms of the DHS role in this case, the bottom line is this: He was not on the No Fly List, which would have flagged him to be prevented from boarding; nor was he on the Selectee List, which would have flagged him for secondary screening in Amsterdam by the Dutch. Furthermore, the physical screening performed by for-

eign authorities at airports in Nigeria and in the Netherlands failed to detect the explosives on his body.

Now, immediately after the attack, DHS responded quickly. And let me pause here a moment.

Senator Thune, I think you have quoted my words back to me exactly, "The situation worked," an unfortunate phrase that was inaccurate, and for which I apologize. But, I'd like for your understanding in context, because, while it was a failure that he was allowed to get on this plane, it was a failure that we did not know that he had these intentions. Once this incident occurred, the following operational activities took place, conducted through the leadership of the TSA:

First, we directed the FAA to alert all 128 flights from Europe bound for the United States of the situation. We increased security measures at domestic airports. We implemented enhanced screening for all international flights coming to the United States. And we reached out to state and local law enforcement, air carriers, international partners, and relevant agencies, to provide them with the information they needed on the ground.

Now, we have outlined, in our report to the President, five areas of action that correspond very well with what the members have commented on in their statements:

First, as this incident underscores, aviation security is increasingly an international responsibility. That's why I dispatched Deputy Secretary Lute and other top DHS officials on a multicontinent tour, to meet with our international counterparts on these measures. Tonight, I will travel to Spain to meet with my European counterparts tomorrow to work on strengthening international security and standards for aviation, including information-sharing between countries, technology, and other issues.

Second, DHS has created a partnership with the Department of Energy and its national labs to use their scientific expertise to improve screening technology at domestic airports. And it goes to a point you were making, Senator Dorgan.

Third, DHS will move forward in deploying enhanced screening technologies, like advanced imaging technology and explosive trace detection machines, to improve our ability to detect the kind of explosives used in the Christmas Day attack. We currently have 40 of these machines deployed in the United States. We intend to deploy at least 450 more this year.

Fourth, we will strengthen the capacity of aviation law enforcement, including the Federal Air Marshal Service. I would include here, as well, that we intend to increase other law enforcement techniques, as well, including behavior detection officers at our airports.

And finally, DHS will work with our interagency partners to reevaluate and modify the way the terrorist watch list is created, including how names are added to the No Fly and Selectee Lists.

I'm very glad to be working with my colleague Director Leiter, Admiral Blair, with whom I was with this morning, in addition to the members of this committee who have done so much to improve our national intelligence and commerce apparatus as we deal with these issues.

And I'm also very grateful to the men and women of the Department of Homeland Security. They work hard every day, every week, to keep this country safe against terrorist attacks. And that is work that is ongoing and that, while I cannot ever guarantee—and I will not to this committee or any committee—that we will never have another attack by someone like an Umar Farouk Abdulmutallab, I can tell you this, that our department is working every day, in every way we can think of, to keep the American people safe.

[The prepared statement of Secretary Napolitano follows:]

PREPARED STATEMENT OF HON. JANET NAPOLITANO, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Chairman Rockefeller, Senator Hutchison, and members of the Committee: Thank you for this opportunity to testify on the attempted terrorist attack on Northwest Flight 253.

The attempted attack on December 25 was a powerful illustration that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. This Administration is determined to thwart those plans and disrupt, dismantle and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just DHS, but many other Federal agencies and the international community as well.

As our part in this effort, DHS is a consumer of the U.S. Government's consolidated terrorist watchlist, which we use to help keep potential terrorists off flights within, over or bound for the United States and to identify travelers that require additional screening. We work with foreign governments, Interpol, and air carriers to strengthen global air travel security by advising them on security measures and on which passengers may prove a threat. We also work with air carriers and airport authorities to perform physical screening at TSA checkpoints and to provide security measures in flight.

Immediately following the December 25 attack, DHS took swift action at airports across the country and around the world. These steps included enhancing screening for individuals flying to the United States; increasing the presence of law enforcement and explosives detection canine teams at air ports, and of air marshals in flight; and directing the FAA to notify the 128 flights already inbound from Europe about the situation. Nonetheless, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with the explosive PETN on his person. As President Obama has made clear, this Administration is determined to find and fix the vulnerabilities in our systems that allowed this breach to occur.

Agencies across the Federal Government have worked quickly to address what went wrong in the Abdulmutallab case. The effort to solve these problems is well underway, with cooperation among DHS, the Department of State, the Department of Justice, the Intelligence Community, and our international allies, among others. As a consumer of terrorist watchlist information, the Department of Homeland Security welcomes the opportunity to contribute to the dialogue on improving the Federal Government's ability to connect and assimilate intelligence. We are also focused on improving aviation screening and expanding our international partnerships to guard against a similar type of attack occurring again. To those ends, today I want to describe the role that DHS currently performs in aviation security, how DHS responded in the immediate aftermath of the attempted Christmas Day attack, and how we are moving forward to further bolster aviation security.

DHS' Role in Multiple Layers of Defense

Since 9/11, the U.S. Government has employed multiple layers of defense across several departments to secure the aviation sector and ensure the safety of the traveling public. Different Federal agencies bear different responsibilities, while other countries and the private sector—especially the air carriers themselves—also have important roles to play.

DHS oversees several programs to prevent individuals with terrorist ties from boarding flights that are headed to, within, or traveling over the United States or, in appropriate cases, to identify them for additional screening. Specifically, DHS uses information held in the Terrorist Screening Data base (TSDB), a resource managed by the Terrorist Screening Center (TSC), as well as other information provided

through the Intelligence Community to screen individuals; operates the travel authorization program for people who are traveling to the United States under the Visa Waiver Program (VWP);[1] and works with foreign governments, international and regional organizations, and airlines to design and implement improved security standards worldwide. This includes routine checks against Interpol databases on wanted persons and lost or stolen passports on all international travelers arriving in the United States. The Department also performs checkpoint screenings at airports in the United States.

To provide a sense of the scale of our operations, every day, U.S. Customs and Border Protection (CBP) processes 1.2 million travelers seeking to enter the United States by land, air or sea; the Transportation Security Administration (TSA) screens 1.8 million travelers at domestic airports; and DHS receives advanced passenger information from carriers operating in 245 international airports that are the last point of departure for flights to the United States, accounting for about 1,600 to 1,800 flights per day. Ensuring that DHS employees and all relevant Federal officials are armed with intelligence and information is critical to the success of these efforts.

Safeguards for Visas and Travel

One of the first layers of defense in securing air travel consists of safeguards to prevent dangerous people from obtaining visas, travel authorizations and boarding passes. To apply for entry to the United States prior to boarding flights bound for the U.S. or arriving at a U.S. port of entry, most foreign nationals need visas—issued by a U.S. embassy or consulate—or, if traveling under a Visa Waiver Program country, travel authorizations issued through the Electronic System for Travel Authorization (ESTA).[2]

Issuing visas is the responsibility of the Department of State. At embassies and consulates where it is operational, the Visa Security Program positions personnel of U.S. Immigration and Customs Enforcement (ICE) to assist State Department personnel in identifying visa applicants who may present a security threat. For individuals traveling under the VWP, DHS operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. These systems examine an individual's information to assess whether he or she could pose a risk to the United States or its citizens, including possible links to terrorism. Without presenting a valid authorization to travel to the United States at the airport of departure, a foreign national is not able to board a U.S.-bound flight.

The Department also works with other Federal agencies and our foreign partners to try to prevent possible terrorists from obtaining boarding passes. These include the application of the No-Fly List and the implementation of Secure Flight program, which I explain below.

Pre-departure Screening

As another layer of defense, DHS conducts pre-departure passenger screening in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. DHS uses TSDB data, managed by the Terrorist Screening Center that is administered by the FBI, to determine who may board, who requires further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

Specifically, to help make these determinations, DHS uses the No-Fly List and the Selectee List, two important subsets within the TSDB. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, over, or within the United States. Individuals on the Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

---

[1] The 35 countries in the Visa Waiver Program are: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, and the United Kingdom (for the U.K., only citizens with an unrestricted right of permanent abode in the U.K. are eligible for VWP travel authorizations).

[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.

Through the Secure Flight Program, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List, and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, DHS began to transfer this responsibility to TSA in 2009, and the transition is targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination.

As an additional layer of security, DHS also uses the Passenger Name Record (PNR), the Advanced Passenger Information System (APIS), and the Immigration Advisory Program (IAP) to assess a passenger's level of risk and, when necessary, flag them for further inspection. PNR data, obtained from the airline reservations systems, contains various elements, which may include optional information on itinerary, co-travelers, changes to the reservation, and payment information. PNR data is evaluated against "targeting rules" that are based on law enforcement data, intelligence and past case experience. A PIS data, which carriers are required to provide to DHS at least 30 minutes before a flight, contains important identifying information that may not be included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. DHS screens APIS information on international flights to or from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations. APIS is also connected to Interpol's lost and stolen passport database for routine queries on all inbound international travelers.

Another layer in the screening process is the Immigration Advisory Program (IAP). The CBP officers stationed overseas under the IAP program at nine airports in seven countries receive referrals from CBP screening against the TSDB, of which the No Fly list is a subset. IAP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

Checkpoint Screenings and In-flight Security

The third layer of defense for air travel in which DHS plays a role is the screening of passengers and their baggage. TSA screens passengers and baggage at airports in the United States, but not in other countries. When a traveler at a foreign airport is physically screened, that screening is conducted by the foreign government, air carriers, or the respective airport authority.

Domestically, TSA employs a layered approach to security, which includes measures both seen and unseen by travelers. The 48,000 Transportation Security Officers at hundreds of airports across the country screen passengers and their baggage using advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines, vapor trace machines that detect liquid explosives, Advanced Imaging Technology, full-body pat-downs, explosives detection systems, Bomb Appraisal Officers, and Behavior Detection Officers—both at the checkpoint and throughout the airport. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security throughout the airport perimeter and in limited access areas of airports. The $1 billion in Recovery Act funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

In an effort to enhance international screening standards, TSA conducts security assessments in accordance with security standards established by the International Civil Aviation Organization (ICAO) at more than 300 foreign airports, which include foreign airports from which flights operate directly to the United States and all airports from which U.S. air carriers operate. If an airport does not meet these standards, TSA works with the host government to rectify the deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. In long-term circumstances of non-compliance with international standards, TSA may recommend suspension of flight service from these airports to the United States. In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level. If an airport is located within one of the 35 VWP countries, DHS conducts

additional audits and inspections as part of the statutorily mandated VWP designation and review process.

In terms of in-flight security, Federal Air Marshals (FAM) are deployed on high-risk domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more volunteer pilots serve as armed, deputized Federal Flight Deck Officers. Additionally, armed law enforcement officers from Federal, state, local, and tribal law enforcement agencies that have a need to fly armed provide a force multiplier on many flights.

DHS Response to the Christmas Day Attack

The facts of the Christmas Day attempted bombing are well established and were relayed in the report on the incident that the President released on January 7, 2010. On December 16, 2009, Umar Farouk Abdulmutallab, a Nigerian national, purchased a round-trip ticket from Lagos, Nigeria to Detroit. Abdulmutallab went through physical security screening conducted by foreign airport personnel at Murtala Muhammed International Airport in Lagos on December 24 prior to boarding a flight to Amsterdam Airport Schiphol. This physical screening included an x-ray of his carry-on luggage and his passing through a walk-through metal detector. Abdulmutallab went through additional physical screening, conducted by Dutch authorities, when transiting through Amsterdam to Northwest Flight 253 to Detroit, and presented a valid U.S. visa. Abdulmutallab was not on the No Fly or Selectee Lists. Accordingly, the carrier was not alerted to prevent him from boarding the flight or additional physical screening, nor did the IAP officer advise Dutch authorities of any concerns. As with all passengers traveling on that flight, and similar to all other international flights arriving in the United States, CBP evaluated Abdulmutallab's information while the flight was en route to conduct a preliminary assessment of his admissibility and to determine whether there were requirements for additional inspection. During this assessment, CBP noted that there was a record that had been received from the Department of State, which indicated possible extremist ties. It did not indicate that he had been found to be a threat, or that his visa had been revoked. CBP officers in Detroit were prepared to meet Abdulmutallab upon his arrival for further interview and inspection. The attack on board the flight failed in no small part due to the brave actions of the crew and passengers aboard the plane.

Immediate DHS Response

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. TSA directed the Federal Aviation Administration to apprise 128 U.S.-bound international flights from Europe of the attempted attack and to ask them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosive detection canine teams, state and local law enforcement, expanded presence of Behavior Detection Officers, and enhanced screening. That evening, DHS issued a security directive for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

From the first hours following the attempted attack, I worked closely with the President, Assistant to the President for Homeland Security and Counterterrorism John Brennan, senior Department leadership, and agencies across the Federal Government. I communicated with international partners, Members of Congress, state and local leadership and the aviation industry and met with national security experts on counterterrorism and aviation security. The results of these communications culminated in two reports to the President: one on New Year's Eve and the second on January 2, 2010.

One of our most important conclusions was that it is now clearer than ever that air travel security is an international responsibility. Indeed, passengers from 17 countries were aboard Flight 253. Accordingly, DHS has embarked upon an aggressive international program designed to raise international standards for airports and air safety. On January 3, 2010, I dispatched Deputy Secretary Jane Holl Lute and Assistant Secretary for Policy David Heyman to Africa, Asia, Europe, the Middle East, Australia, and South America to meet with international leadership on aviation security. In these meetings, they reviewed security procedures and technology being used to screen passengers on U.S.-bound flights and worked on ways to bolster our collective tactics for defeating terrorists. This afternoon, I am traveling to Spain to meet with my European Union counterparts in the first of a series of global meetings intended to bring about broad consensus on new, stronger, and more consistent international aviation security standards and procedures.

In addition to these efforts, the Department has been in close contact with Congress, our international partners, the aviation industry and state and local officials across the country since the afternoon of the attempted attack. On December 25, the Department issued a joint bulletin with the FBI to state and local law enforcement throughout the nation; conducted calls with major airlines and the Air Transport Association; distributed the FBI-DHS joint bulletin to all Homeland Security Advisors, regional fusion center directors and Major City Homeland Security Points of Contact in the country; and notified foreign air carriers with flights to and from the United States of the additional security requirements. DHS has maintained close contact with all of these partners since the attempted attack, and will continue to do so.

On January 3, TSA issued a new Security Directive, effective on January 4, which includes long-term, sustainable security measures developed in consultation with law enforcement officials and our domestic and international partners. Because effective aviation security must begin beyond our borders, this Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism[3] or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners.

Steps Forward to Improve Aviation Security

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. On January 7, I joined Assistant to the President for Counterterrorism and Homeland Security John Brennan to announce five recommendations DHS made to the President as a result of the security reviews ordered by President Obama. At the President's direction, DHS will pursue these five objectives to enhance the protection of air travel from acts of terrorism.

First, DHS will work with our interagency partners to re-evaluate and modify the criteria and process used to create terrorist watchlist, including adjusting the process by which names are added to the No-Fly and Selectee Lists. The Department's ability to prevent terrorists from boarding flights to the United States depends upon these lists and the criteria used to create them. As an entity that is primarily a consumer of this intelligence and the operator of programs that rely on these lists, the Department will work closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watchlist system.

Second, DHS will establish a partnership on aviation security with the Department of Energy and its National Laboratories in order to use their expertise to bolster our security. This new partnership will work to develop new and more effective technologies that deter and disrupt known threats, as well as anticipate and protect against new ways that terrorists could seek to board an aircraft with dangerous materials.

Third, DHS will accelerate deployment of Advanced Imaging Technology to provide capabilities to identify materials such as those used in the attempted December 25 attack, and we will encourage foreign aviation security authorities to do the same. TSA currently has 40 machines deployed at nineteen airports throughout the United States, and plans to deploy at least 450 additional units in 2010. DHS will also seek to increase our assets in the area of explosives-trained canines, explosives detection equipment, and other security personnel.

Fourth, DHS will strengthen the presence and capacity of aviation law enforcement. As an interim measure, we will deploy law enforcement officers from across DHS to serve as Federal Air Marshals to increase security aboard U.S.-flag carriers' international flights. At the same time, we will maintain the current tempo of operations to support high-risk domestic flights, as we look to longer-term solutions to enhance the training and workforce of the Federal Air Marshal Service.

Fifth, as mentioned earlier, DHS will work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in foreign airports and the commitments of our foreign partners to enhance security—not just for Americans, but also for their nationals traveling to this country.

[3] The State Department currently lists Cuba, Iran, Sudan, and Syria as state sponsors of terrorism.

In all of these action areas to bolster aviation security, we are moving forward with a dedication to safeguard the privacy and rights of travelers.

Conclusion

The attempted attack on Christmas Day serves as a stark reminder that terrorists motivated by violent extremist beliefs are determined to attack the United States. President Obama has made clear that we will be unrelenting in using every element of our national power in our efforts around the world to disrupt, dismantle, and defeat al-Qaeda and other violent extremists.

While we address the circumstances behind this specific incident, we must also recognize the evolving threats posed by terrorists, and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities in all sectors. President Obama has clearly communicated the urgency of this task, and the American people rightfully expect swift action. DHS and our Federal partners are moving quickly to provide just that.

I wish I could close by giving you a 100 percent guarantee that no terrorist, ever, will try to take down a plane or attack us in some other fashion. I cannot give you such a guarantee; that is not the nature of the world we live in, nor of the threats that we face. What I can give you, however, is the 100 percent commitment of myself, DHS leadership, and the entire DHS enterprise to do everything we can to minimize the risk of terrorist attacks.

Chairman Rockefeller, Senator Hutchison and members of the Committee: Thank you for this opportunity to testify. I can now answer your questions.

The CHAIRMAN. Thank you, Madam Secretary.

And now Director Leiter.

STATEMENT OF HON. MICHAEL E. LEITER, DIRECTOR, NATIONAL COUNTERTERRORISM CENTER

Mr. LEITER. Mr. Chairman, Senator Hutchison, members of the Committee, thank you.

Needless to say, I wish that my introduction to this committee were under a very different set of circumstances than they are today.

I'm honored to appear also with Secretary Napolitano, Governor Kean, Congressman Hamilton.

But, I also want to say that I am honored to appear—I know, in our audience today, in the gallery, are members of the families of the victims of 9/11. And I want to make a personal pledge to them, on behalf of myself and also the members of NCTC and the counterterrorism community, to continue to do all that we can to honor their family members' memory by trying to keep the scourge of terrorism from touching others.

I want to start with an assertion which I hope is as crystal clear as Secretary Napolitano's was. Umar Farouk Abdulmutallab should not have stepped on a plane on Christmas Day. The system failed—the counterterrorism system failed. And I, along with other leaders, have told the President that. I'm here to tell you that. And I'm here to tell the American people that. And I think, most importantly, that we are determined to do better.

The Director of National Intelligence and I have both been tasked by the President to look at how we can improve those elements of analysis, of collection, of information-sharing, and watchlisting, that obviously need to be repaired.

I'd like to quickly run down some of the events that led to the Christmas Day attack. And although I can't go into great depth in an open session, I think it's important to make some points, be-

cause, frankly, there are no shortage of inaccuracies in the media that have been reported.

But, I want to start, first, by debunking what has become conventional wisdom among some, that this is the same failure that occurred on 9/11. It is not. And that is not to suggest that it is not potentially tragic, but it is to highlight, because, unlike 9/11, where there was a failure to share information the U.S. Government had, that is not what occurred in this case. And, obviously, any prescription for repairing the failings has to know what caused the failings in the first place.

I would open also by saying this is all the more frustrating to me because the intelligence community and NCTC did identify many of the things that led up to this attack, but we very much failed in the last tactical mile of associating some of the plotting that we saw with this individual, Umar Farouk.

Throughout 2009, in the fall, in front of other Members of Congress, we spoke to the growing danger posed by al-Qaeda in the Arabian Peninsula, and, in particular, the danger posed by European and Western recruits that they might have for plotting against the homeland. And although we didn't know it at the time, we were concerned about operations on Christmas. But, again, we did not connect that with Abdulmutallab. And we also warned about the type of explosive that Abdulmutallab used, and the ways in which it might prove a challenge to screening, which, of course, manifested itself on Christmas Day.

But, again, despite these pieces that we did connect, we simply did not make the final connections, and we failed in doing so, the last tactical mile linking this individual to this plot.

We did, in fact, have the information from his father about his concern he expressed, with his son going to Yemen, and that he had come under the influence of religious extremists, and that he was not returning home. And we had other streams of information from other intelligence channels. So, we ended up with a partial name, an indication of a Nigerian. But, no piece of intelligence brought that together, nor did my analysts or my organization or I bring that together.

As a result, although Mr. Abdulmutallab was, in fact, entered as a known and suspected terrorist, into what is known as the Terrorist Identities Datamart Environment—that list of 550,000 I believe Senator Thune referred to—he was not watch-listed, because this information was not connected to him. And hence, he also was not placed on the No Fly or Selectee Lists.

Had all of the information that was available to the U.S. been linked together to this one individual, he would have undoubtedly been watch-listed, and therefore, he would have been on the visa screening list and the border inspection list.

And I want to read this verbatim, because it's a—it's an important point. "Whether he would have been placed on either the No Fly or Selectee List, again, based on the existing standards of 2008 and 2009, would have been determined by the strength of the analytic judgment about exactly who he was and what he was doing." And, as I'd like to note quite clearly, one of the lessons that we have learned, and the President has tasked us to do, is to review

these watch-listing standards in a way that they are as flexible and as nimble as the enemy we face.

Finally—and I hope I have made clear that I do not wish to make excuses for what we didn't do right. We didn't do things right, and we didn't do things well. I do want to note the context for some of these failings.

Each day, NCTC receives and reviews literally thousands of pieces of counterterrorism intelligence. Although the exact number is classified, it is well over 5,000 pieces of terrorism data, with more than 5,000 names each day. We put on the watch list more than 350 individuals a day. And we look at more than 30 or 40 specific plots every day. So, although I undoubtedly admit we must do better, the multidimensional and varied nature of this threat means that even intelligence is not a silver bullet; it is one part of a multilayer set of defenses, including technology, international cooperation, and screening, that we must combine.

Briefly—and, of course, I'll—I'm happy to take more questions on this—we are trying to improve this situation as quickly as we can, pursuant to the President's directive of January 7. In line with the President's conclusions and his direction, we're moving in, really, five broad areas:

First, as a number of you have noted, we're examining the "No Fly List" standards. Frankly, the pressure over the past 8 years has never been to put more people on the "No Fly List," it has been just the opposite. We have to look at what those standards are and ensure that we are, again, flexible enough to have individuals, either "Selectees" or "No Flys," regardless of whether or not we have specific intelligence about their involvement in operations.

Second, although we saw the growing threat in Yemen, we—and I include myself in that "we"—and the DNI, did not adequately move resources to address that threat. We were simply more focused on the threats that we saw within Yemen, and the threat outside was not addressed quickly enough with additional resources. We need to do that, and that has already been done, to some extent.

Third, we have to move away a bit from a names-based system of tracking threats. It's fairly easy—and I think we're quite good, as proved in many cases in 2009—to tracking threats when we know a name and we know what the plot is. But, it's much, much harder, and we have to do a better job of pursuing small, discrete pieces of data that don't automatically add up to a threat. That is our challenge, and we are trying to do that now.

Fourth, we are making sure that we assign priority for tracking of threats as they come in. And we have done that quite well, again, when the threat is of a high profile and something we understand fully. We have to assign that same level of responsibility when we also are not sure what the threat is.

And finally, we have to make sure, again, that the records within our watch lists are enhanced, to the extent they can. This is certainly a matter of technology, and technology applies to all of the areas I've already discussed. But, it is also simply a matter of having enough people to put their eyes on these records and make the connections that will help keep the Nation safe.

Although I would strongly echo what Secretary Napolitano noted, that none of this will guarantee security. But, it must be used to perfect the system to the greatest extent possible.

Thank you. And I look forward to working with the Committee.

[The prepared statement of Mr. Leiter follows:]

PREPARED STATEMENT HON. MICHAEL E. LEITER, DIRECTOR, NATIONAL COUNTERTERRORISM CENTER

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee on Commerce, Science and Transportation: Thank you for your invitation to appear before the Committee to discuss the events leading up to the attempted terrorist attack on Christmas Day and the improvements the National Counterterrorism Center and the Intelligence Community have underway to fix deficiencies.

It is my privilege to be accompanied by Janet Napolitano, Secretary of Homeland Security.

The attempted terrorist attack on Christmas Day did not succeed, but, as one of several recent attacks against the United States inspired by jihadist ideology or directed by al Qa'ida and its affiliates, it reminds us that our mission to protect Americans is unending.

Let's start with this clear assertion: Umar Farouk Abdulmutallab should not have stepped on that plane. The counterterrorism system failed and we told the President we are determined to do better.

Within the Intelligence Community we had strategic intelligence that al Qa'ida in the Arabian Peninsula (AQAP) had the intention of taking action against the United States prior to the failed attack on December 25, but, we did not direct more resources against AQAP, nor insist that the watchlisting criteria be adjusted prior to the event. In addition, the Intelligence Community analysts who were working hard on immediate threats to Americans in Yemen did not understand the fragments of intelligence on what turned out later to be Mr. Abdulmutallab, so they did not push him onto the terrorist watchlist.

We are taking a fresh and penetrating look at strengthening both human and technical performance and do what we have to do in all areas. Director of National Intelligence Blair and I have specifically been tasked by the President to improve and manage work in four areas:

Immediately reaffirm and clarify roles and responsibilities of the counterterrorism analytic components of the IC in synchronizing, correlating, and analyzing all sources of intelligence related to terrorism.

Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.

Take further steps to enhance the rigor and raise the standard of tradecraft of intelligence analysis, especially analysis designed to uncover and prevent terrorist plots.

Ensure resources are properly aligned with issues highlighted in strategic warning analysis.

Additionally, NCTC has been tasked by the President to do the following:

Establish and resource appropriately a process to prioritize and to pursue thoroughly and exhaustively terrorism threat threads, to include the identification of appropriate follow-up action by the intelligence, law enforcement, and homeland security communities.

Establish a dedicated capability responsible for enhancing record information on possible terrorists in the Terrorist Identities Datamart Environment for watchlisting purposes.

The Events Leading Up to the Christmas Day Attack

I will now briefly discuss some of the details of the bombing attempt and what we missed. As the President has said, this was *not*—like in 2001—a failure to collect or share intelligence; rather it was a failure to connect, integrate, and understand the intelligence we had.

Although NCTC and the Intelligence Community had long warned of the threat posed by al Qa'ida in the Arabian Peninsula, we did not correlate the specific information that would have been required to help keep Abdulmutallab off that Northwest Airlines flight.

More specifically, the Intelligence Community highlighted the growing threat to U.S. and Western interests in the region posed by AQAP, whose precursor elements attacked our embassy in Sana'a in 2008. Our analysis focused on AQAP's plans to strike U.S. targets in Yemen, but it also noted—increasingly in the Fall of 2009—the possibility of targeting the United States. We had analyzed the information that this group was working with an individual who we now know was the individual involved in the Christmas attack.

In addition, the Intelligence Community warned repeatedly of the type of explosive device used by Abdulmutallab and the ways in which it might prove a challenge to screening. Of course, at the Amsterdam airport, Abdulmutallab was subjected to the same screening as other passengers—he passed through a metal detector, which didn't detect the explosives that were sewn into his clothes.

As I have noted, despite our successes in identifying the overall themes that described the plot we failed to make the final connections—the "last tactical mile"—linking Abdulmutallab's identity to the plot. We had the information that came from his father that he was concerned about his son going to Yemen, coming under the influence of unknown religious extremists, and that he was not going to return home. We also had other streams of information coming from intelligence channels that provided pieces of the story. We had a partial name, an indication of a Nigerian, but there was nothing that brought it all together—nor did we do so in our analysis.

As a result, although Mr. Abdulmutallab was identified as a known or suspected terrorist and entered into the Terrorist Identities Datamart Environment (TIDE)—and this information was in turn widely available throughout the Intelligence Community—the derogatory information associated with him did not meet the existing policy standards—those first adopted in the summer of 2008 and ultimately promulgated in February 2009—for him to be "watchlisted," let alone placed on the No Fly List or Selectee lists.

Had all of the information the U.S. had available, fragmentary and otherwise, been linked together, his name would have undoubtedly been entered on the Terrorist Screening Data base which is exported to the Department of State and the Department of Homeland Security. Whether he would have been placed on either the No Fly or Selectee list—again based on the existing standards—would have been determined by the strength of the analytic judgment. One of the clear lessons the U.S. Government has learned and which the Intelligence Community will support is the need to modify the standards for inclusion on such lists.

In hindsight, the intelligence we had can be assessed with a high degree of confidence to describe Mr. Abdulmutallab as a likely operative of AQAP. But without making excuses for what we did not do, I think it critical that we at least note the context in which this failure occurred: Each day NCTC receives literally thousands of pieces of intelligence information from around the world, reviews literally thousands of different names, and places more than 350 people a day on the watchlist—virtually all based on far more damning information than that associated with Mr. Abdulmutallab prior to Christmas Day. Although we must and will do better, we must also recognize that not all of the pieces rise above the noise level.

The men and women of the National Counterterrorism Center and the Intelligence Community are committed to fighting terrorism at home and abroad and will seek every opportunity to better our analytical tradecraft, more aggressively pursue those that plan and perpetrate acts of terrorism, and effectively enhance the criteria used to keep known or suspected terrorists out of the United States.

The CHAIRMAN. Thank you, Director Leiter.

Now the Honorable Lee Hamilton.

STATEMENT OF HON. LEE HAMILTON, CO-CHAIR, NATIONAL SECURITY PREPAREDNESS GROUP, BIPARTISAN POLICY CENTER, AND FORMER VICE CHAIRMAN, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (9/11 COMMISSION)

Mr. HAMILTON. Chairman Rockefeller, Senator Hutchison, members of the Committee, Secretary Napolitano, and Director Leiter, Tom and I, of course, are delighted to be with you.

And I think we are eternally grateful to the Members of the U.S. Senate for the way in which they have followed up the implementa-

tion of the recommendations of the 9/11 Commission. The actions of the Senate, over a period of several years now, have just been exceedingly good, from our standpoint.

My remarks will be, I hope, very brief and on target. They will be directed principally to the questions of intelligence and not so much to commerce.

I was gratified to hear from a number of you, as you spoke, about the necessity of the—recognizing that the threat is real and we have to reject complacency and recognize that that threat is genuine. I think many of you emphasized that in your remarks.

Tom and I appear here today as members of the National Security Preparedness Group, which is a successor to the 9/11 Commission. It's made up of a number of people, evenly divided between Republicans and Democrats. I think their names are familiar to you; they're in the written testimony.

In the years since the passage of the Intelligence Reform and Terrorism Prevention Act which created the Director of National Intelligence and the National Counterterrorism Center, it is our view that the U.S. Government has made significant positive strides to correct the shortfalls that were obvious on September 11. But, obviously we've seen, from the incidents at Fort Hood and the skies above Detroit, there is a lot of work to be done.

The DNI has been hobbled by disputes over its size, its mission, and its authority. Nonetheless, the determination of the terrorists to attack the homeland remains unabated, demonstrated by these events, and, from our point of view, understands the critical importance for creating and supporting the DNI and the NCTC. It is imperative that the DNI and the NCTC be successful in their vital and very complex missions that they have been asked to undertake for the country.

We note with approval, as Director Leiter said a moment ago, while other failures did occur, apparently the Christmas attack was not a repeat of the failures to share information that were evident on 9/11. That suggests to us that progress has certainly been made and that agencies and analysts are sharing critical information.

In an age when we are collecting more information than ever before, the real challenge, it seems to us, is, how do you understand, manage, and integrate vast amounts of information? It's really a problem of data management. We need better management of the data. And, of course, we have to look to the state-of-the-art technology to help us better sort through massive amounts of information to ensure the right people are seeing it time to make a difference.

The greatest single challenge that arises from this incident, in our view, is the urgent need to strengthen the analytic process. We are pleased that the President has asked the DNI to look at this issue, and he is certainly properly situated in the community to assume a leadership role in that respect.

Another lesson that emerged from the Christmas attack reminded us of 9/11. We repeatedly said that one of the problems there that—was, no one was in charge. Well, in a sense, that's what's happened here. The intelligence community is designated as "in charge" of running down all the leads associated with a particular threat. We welcome redoubled efforts to assure that respon-

sibility for investigating leads on potential threats are assigned, pursued, and acted upon immediately and aggressively.

We need to do a better job of judging the sources of potential attacks. We are seriously behind the curve when, as the Director said a moment ago, we were not sufficiently aware of a possible attack on the United States from Yemen.

The final point I want to make is that one of the things that has always concerned me about intelligence is that, though I think the intelligence community does a very good job, I don't think they do as good a job as they should on longer-term threats. It's quite understandable that they should concentrate on the near-term. But, I think this is—this incident is an example of it, so heavily concentrated on Iraq and Afghanistan and Pakistan, for reasons that are obvious to all of us, that we kind of did not see, or at least did not see sufficiently, the kind of attack that could come to us from Yemen; a longer-term perspective. And I think the intelligence community must learn not only to focus on the immediate threats, but also threats that are developing, as they were in Yemen.

I'd turn to Governor Kean.

[The prepared statement of Congressman Hamilton and Governor Tom Kean follows:]

PREPARED STATEMENT OF CONGRESSMAN LEE HAMILTON AND GOVERNOR TOM KEAN, BIPARTISAN POLICY CENTER

I. Introduction

We are very happy to appear before you today. As Chairman of the Intelligence Committee Senator Rockefeller made numerous contributions to our national security and we are glad to be back with you again.

Today, we are appearing in our capacity as Co-Chairmen of the Bipartisan Policy Center's National Security Preparedness Group (NSPG), a successor to the 9/11 Commission. Drawing on a strong roster of national security professionals, the NSPG works as an independent, bipartisan group to monitor the implementation of the 9/11 Commission's recommendations and address other emerging national security issues.

NSPG includes the following membership:

- Mr. Peter Bergen, CNN National Security Analyst and Author, Schwartz Senior Fellow at the New America Foundation.
- Dr. Bruce Hoffman, Georgetown University terrorism specialist.
- The Honorable Dave McCurdy, former Congressman from Oklahoma and Chairman of the U.S. House Intelligence Committee, President of the Alliance of Automobile Manufacturers.
- The Honorable Edwin Meese III, former U.S. Attorney General, Ronald Reagan Distinguished Fellow in Public Policy and Chairman of the Center for Legal and Judicial Studies at The Heritage Foundation.
- The Honorable Tom Ridge, former Governor of Pennsylvania and U.S. Secretary of Homeland Security, Senior Advisor at Deloitte Global LLP, Ridge Global.
- The Honorable Frances Townsend, former Homeland Security Advisor and former Deputy National Security Advisor for Combating Terrorism.
- Dr. Stephen Flynn, President, Center for National Policy.
- Dr. John Gannon, BAE Systems, former CIA Deputy Director for Intelligence, Chairman of the National Intelligence Council, and U.S. House Homeland Security Staff Director.
- The Honorable Richard L. Thornburgh, former U.S. Attorney General, of Counsel at K&L Gates.
- The Honorable Jim Turner, former Congressman from Texas and Ranking Member of the U.S. House Homeland Security Committee, Arnold and Porter, LLP.

- Mr. Lawrence Wright, New Yorker Columnist and Pulitzer Prize winning author of *The Looming Tower: Al Qaeda and the Road to 9/11.*
- The Honorable E. Spencer Abraham, former U.S. Secretary of Energy and U.S. Senator from Michigan, The Abraham Group.

Over the course of 2009, our group met with Obama Administration and former senior officials from the Bush Administration, including:

- Director of National Intelligence, Admiral Dennis Blair (July 2009).
- CIA Director Leon Panetta (July 2009).
- Secretary of Homeland Security Janet Napolitano (July 2009).
- FBI Director Bob Mueller (September 2009).
- Former CIA Director Mike Hayden (September 2009).
- Former DNI Mike McConnell (September 2009).

We will also meet with Deputy National Security Adviser John Brennan next week.

We believe the strength of our group will allow us to be a voice on national security issues and a resource to you and the executive branch. First and foremost, we are here to help play a constructive role in support of your work.

* * * * * * *

Since the 9/11 attacks 8 years ago and the release of our Commission report 5 years ago, the Federal Government has implemented many changes in America's homeland security and intelligence apparatus.

As demonstrated by the recent attempted terrorist attack in the skies over Detroit, the threat remains strong. We must reject complacency and recognize we still face a serious threat from organizations like Al-Qaeda. Al-Qaeda's core is still active, individuals are still being radicalized in Western countries and motivated to commit violence, and homegrown lone actors are still a risk. As our colleague Bruce Hoffman observed, "*al Qaeda is on the march, not on the run*." This is not a reason for panic but for a concerted, comprehensive effort.

Recently the 5 year anniversary of the Intelligence Reform and Terrorism Prevention Act passed and in recent months our group has been studying the implementation of the 9/11 Commission's recommendations, especially the state of intelligence reform, and new threats to our national security. Many of the findings in that report hold true today and can help guide our response to the attacks at Fort Hood and on Christmas Day.

Intelligence Coordination and Management

At their core, the problems evident on September 11, 2001, were about the failures and obstacles to sharing information among the Federal partners charged with protecting the country. And even if that information had been made available, there was no one in the Federal Government charged with fusing together intelligence derived from multiple foreign and domestic sources.

To facilitate information-sharing and to create an entity whose job it would be to connect the dots, the bipartisan 9/11 Commission recommended, and the Congress and the President established, a Director of National Intelligence (DNI) and a National Counterterrorism Center (NCTC).

The DNI would be charged with breaking down bureaucratic, cultural, technological, and policy barriers to the sharing of information among Federal agencies and the NCTC would be the hub, the "primary organization in the U.S. Government for analyzing and integrating all intelligence." The idea was for the DNI to ensure information-sharing so the NCTC could access and assess all available relevant information and then connect disparate pieces of threat information to aid in preventing future attacks.

In the 5-years since the passage of the Intelligence Reform and Terrorism Prevention Act, the U.S. Government has made significant strides to correct the shortfalls and mistakes evident on September 11, 2001. *But as we've seen from the recent terrorist incidents at Fort Hood and in the skies above Detroit, there is still work to be done*.

The DNI has been hobbled by endless disputes over its size, mission, and authority. Nonetheless, the determination of the terrorist to attack the homeland remains unabated as demonstrated by these events and underscores the critical need for creating the DNI and the NCTC. It is imperative that the DNI and the NCTC to be successful in the vital missions they have been asked to undertake for the country.

We welcome the President's recent review of the Christmas attack and *we should continue to study this incident and the attack at Fort Hood so we can apply their lessons to making the country safer. Here are some of our preliminary observations:*

- *Information sharing and Connecting the Dots.* The 9/11 Commission found that the biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is human or systemic resistance to sharing information whether collected outside the U.S. or inside the U.S. bearing on threats pertaining to international terrorists. We recommended providing incentives for sharing information within the Intelligence Community. *We note with approval that, while other failures did occur, apparently the Christmas attack was not a repeat of the failures to share information that were evident on 9/11. That suggests to us that progress has been made and that agencies and analysts are sharing critical information.* However, it is not clear whether the NSA intercepted conversations referenced in news reports were widely shared. The incident points out two additional challenges that need to be addressed:
  - *Rather than a failure to share information, the Intelligence Community is awash with data. In an age when we are collecting more information than ever before, the real challenge is how do you understand, manage, and integrate vast amount of information.* The DNI needs to develop ways of dealing with intelligence information overload. At the same time, we need to do a better job of pushing information to the right people within the Intelligence Community. We welcome President Obama's order to distribute intelligence reports more quickly and widely. We need better management of the data and to look to technology to help us better sort through massive amounts of information to ensure the right people are seeing it in time to make a difference. The technology we use must be state-of-the-art, constantly upgraded to quickly put information together and it must be properly placed instantaneously so better analysis can occur.
  - *As President Obama said, there was a failure to connect the dots. With more rigorous analysis, we might have been able to connect disparate pieces of information that might have foretold of the Christmas plot.* The greatest single challenge that arises from this incident in our view is the urgent need to strengthen the analytic process. We are pleased the President asked the DNI to look at this issue. The DNI was charged by the Congress in the Intelligence Reform Act to ensure the highest analytical standards within the Intelligence Community. The DNI is properly situated within that Community to assume a leadership role in applying more rigorous standards to analytical tradecraft. Congress should also support these entities by giving the DNI and the NCTC the resources they need and the ability to recruit and keep the best people.
- *Designating Someone in Charge.* Another lesson from the Christmas attack is that we need to do a better job of ensuring that someone within the Intelligence Community is designated as "in charge" of running down all leads associated with a particular threat stream. As John Brennan indicated, we did not follow up and prioritize the intelligence indicating that al Qaeda in the Arabian peninsula sought to strike the homeland because no one intelligence entity or team or task force was assigned responsibility for doing that follow up investigation. In our investigation of the 9/11 attacks, we frequently saw confusion about roles, responsibilities, and missions and we welcome redoubled efforts to assure that responsibility for investigating leads on potential threats are assigned, pursued, and acted upon immediately and aggressively.
- *We need to do a better job of judging sources of potential attacks properly.* As the President's review has shown, we had a "strategic sense" that Al Qaeda in the Arabian Peninsula was becoming a threat, but "we didn't know they had progressed to the point of actually launching individuals here." *This at once shows the need for improved collection and better analysis*. We collect a tremendous amount of intelligence and we need the very best people not only sorting through it for tactical details, but in a strategic sense asking where the next attack will come from.
- *No Sanctuaries.* Finding that our attackers on 9/11 benefited from the time, space, and command structure afforded in Afghanistan, the 9/11 Commission placed great emphasis on identifying and prioritizing *actual or potential* terrorist sanctuaries. We recommended strategies employing all elements of national power to keep terrorists insecure and on the run. We're fortunate that the attack on Christmas emanating from Yemen did not succeed and this episode reminds us of the need to identify other potential sanctuaries. As our colleague Bruce Hoffman observed: "Al Qaeda is aggressively seeking out, desta-

bilizing and exploiting failed states and other areas of lawlessness . . . and over the past year has increased its activities in places such as Pakistan, Algeria, the Sahel, Somalia, and of course Yemen." *The U.S. should take a fresh look at these areas and deepen our commitment to ensuring al Qaeda cannot exploit those territories.*

The Effectiveness of the Director of National Intelligence

We would like to say a word on the state of intelligence reform and the effectiveness of the DNI. After 5 years of experience with the new intelligence system, we are frequently asked, is it working? Our NSPG has been conducting a review of the Intelligence Reform and Terrorism Prevention Act and the effectiveness of the DNI and has begun work intended to help answer this question.

We have more work to do but our preliminary answer is that the DNI has achieved a meaningful measure of success in its first years—that has made it worth the inevitable turmoil—but is a work in progress closer to the beginning of reform than the end.

Some of the successes in the last 5 years include progress on information-sharing, a joint-duty program, and despite the failures evident in the Christmas attack, the National Counter Terrorism Center. Since September 11, 2001, the NCTC and other government agencies have repeatedly connected the dots and shared information necessary to defeat terrorist attacks. Improvements have clearly been made although that sharing is not as prompt and seamless as it should be.

But the DNI and the NCTC need most of all is the unyielding support of the President and the Congress if those organizations are going to achieve their role in integrating the Intelligence Community.

We as a country gave the DNI a hard job and a gargantuan to do-list, including:

- Solving systemic and longstanding information-sharing issues among Intelligence Community entities, especially to break down the "wall" between foreign and "domestic" intelligence, and to create an architecture to enable such sharing;
- Serving as the President's Principal Intelligence Advisor;
- Developing a national intelligence budget across all intelligence agencies;
- Overseeing billions of dollars of intelligence community acquisitions;
- Improving the quality of intelligence analysis, especially to guard against "group-think," and to manage an intelligence process that is inclusive of a variety of view points;
- Facilitating a "culture change" within the Community by establishing a joint duty system, modeled on DoD's Goldwater-Nichols, to enable personnel to rotate assignments within the intelligence community;
- Bringing a mission focus to the IC by creating a group of Mission Managers "responsible for all aspects of the intelligence process to those issues" and leading centers like National Counter Terrorism Center and National Counterproliferation Center.

The DNI was given substantial authorities to accomplish these missions. The DNI must be the person who drives inter-agency coordination and integration. We are concerned about the expanding growth and bureaucracy of the DNI and we urge vigorous reevaluation of all its functions to assure its leanness. The DNI's authorities must be exercised with discretion and consideration of the priorities and sensitivities of other intelligence agencies.

However, to be sure, there are ambiguities in the law. These ambiguities can contribute to mission confusion and lack of clarity about lanes in the road. *But the burden is on the President to be clear on who is in charge of the Intelligence Community and where final authority lies on budget and personnel matters. The President's leadership is crucial and must be continuing or we run the risk of mission confusion and decrease the prospect of long and lasting reform that was recommended after September 11, 2001.*

Privacy and Civil Liberties

The balance between security and liberty will always be a part of the struggle against terrorism. America must not sacrifice one for the other and must be in the business of protecting freedom and liberty as well as fighting terrorism. Following the 9/11 Commission recommendations, the Bush Administration created a Privacy and Civil Liberties Oversight Board to advise the Executive Branch and oversee government efforts to defend civil liberties. The board was staffed and became operational in 2006. In 2007, Congress restructured the Board as an independent agency outside the White House. Despite early accusations of undue delay and inadequate

funding, the Board held numerous sessions with national security and homeland security advisers, the attorney general, and the FBI director, among others, on terrorist surveillance and other issues arising from intelligence collection.

However, the Board has been dormant since that time. With massive capacity to develop data on individuals, the Board has to be the champion of seeing that collection capabilities do not intrude into privacy and civil liberties. *We continue to believe that the Board provides critical functions and we urge President Obama to reconstitute it, quickly appoint its Members, and allow them full access to the information and the authority to perform to perform this essential function.*

Congressional Oversight

The 9/11 Commission also placed great importance on rigorous Congressional oversight. This recommendation helped precipitate the creation of a House Homeland Security Committee and a Senate Homeland Security and Governmental Affairs Committee. However, enduring fractured and overlapping committee jurisdictions on both sides of the hill have left Congressional oversight in a unsatisfactory state. DHS entities still report to dozens of separate committees hundreds of times per year, which constitutes a serious drain of time and resources for senior DHS officials. Further, the jurisdictional melee among the scores of Congressional committees has led to conflicting and contradictory tasks and mandates for DHS. Without taking serious action, we fear this unworkable system could make the country less safe.

The 9/11 Commission also called Congressional oversight over intelligence dysfunctional. We made recommendations to strengthen the oversight committees which were not accepted by the Congress though some progress has been made. Today we want to emphasize the enormous importance we attach to rigorous oversight of the intelligence community. Congressional oversight can help ensure the intelligence community is operating effectively and help resolve disputes about conflicting roles and missions. We urge the Congress to take action to strengthen the oversight capabilities of the intelligence committees.

STATEMENT OF HON. TOM KEAN, CO-CHAIR, NATIONAL SECURITY PREPAREDNESS GROUP, BIPARTISAN POLICY CENTER, AND FORMER CHAIRMAN, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (9/11 COMMISSION)

Mr. KEAN. Thank you, Lee. And thank you, Chairman Rockefeller, and—I'm sorry—Vice Chair—there. It's on now? Thank you.

The CHAIRMAN. Thank you for being here.

Mr. KEAN. Thank you, Mr. Chairman, and I thank you——

The CHAIRMAN. I tend to think of you two as founding fathers. [Laughter.]

Mr. KEAN. Thank you.

But, the—I would mention to the Committee, by the way, something that Mr. Leiter also said, that it seems remarkable to me—we have here in the room with us today, again, members of the people representing the families of 9/11—it is remarkable to me that all these years after they suffered that tragedy, that they're here, hearing after hearing, that I talk to them on the phone all the time, that they have never flagged one minute in their efforts to make sure that that never, ever happens to families again. They're a remarkable group of people, and I just want to commend them to you today.

Senator HUTCHISON. That's very impressive. That is.

Mr. KEAN. Yes.

The—I'd like to say just a word about the effectiveness of—again, of the DNI. We're frequently asked, Lee and I, both of us, "How is it working?" You know, "How is it working?" And so, we've been trying, in our new group, to conduct a review of the Intelligence

Reform and Terrorism Prevention Act, and see just how effective the DNI is. And we began our work to try and answer that question.

We have a lot more work to do, obviously, but what we can see already is that the DNI has achieved a meaningful measure of success in its first years, has made it, probably, hopefully, worthwhile—the inevitable turmoil. But, it's a work in progress, and it's probably closer to beginning of reform than the end.

Some of the success of the last 5 years include progress on information-sharing, a joint-duty program, and, despite the failures evident in this attack we've been talking about on Christmas, the National Counterterrorism Center.

Since September 11, 2001, the NCTC and other government agencies have repeatedly connected the dots. And they have, in the past, shared the information necessary to prevent terrorist attacks. Improvements have clearly been made, although that sharing is not as prompt nor as seamless as we would like it to be.

But, what the DNI and the NCTC need most of all, in our opinion, is the unyielding support of the President and the Congress, if those organizations are going to achieve their role in integrating the intelligence community in preventing these attacks.

You know, we all gave the DNI a very, very difficult job and a gargantuan to-do list, and the DNI was given the substantial authorities to accomplish those missions.

We are concerned about the expanding growth of bureaucracy of the DNI, and we urge vigorous reevaluations of all its functions, to assure that it's lean and efficient. The DNI's authorities must be exercised with discretion and consideration of the priorities and sensitivities of the other intelligence agencies that it works with.

However, to be sure, there are still ambiguities—excuse me—in the law that you passed. These ambiguities can contribute to mission confusion and sometimes a lack of clarity, perhaps, in the lanes in the road. But, the burden is on the President to be clear on who is in charge of the intelligence community, and where final authority lies on budget and on personnel matters. Absolutely crucial here is the President's leadership, or we run the risk of mission confusion and a decrease in the prospect of long and lasting reform that was recommended after September 11, 2001.

Let me say just a couple of other matters here before I close:

The Chairman mentioned, in his opening remarks, the problems and the balance that always has to occur between civil liberties and the need to keep ourselves safe. This will always be part of the struggle against terrorism; we'll face these decisions all the time. And we can't sacrifice one for the other. We have to keep both. We are in the business of protecting freedom and liberty as well as fighting terrorism.

Now, we have recommended a board. This board has been dominant for a couple of years, and the Congress passed that legislation. With a massive capacity to develop data on individuals, this board—civil liberties board—has to be the champion of seeing that collection capabilities do not include—do not intrude unnecessarily into privacy and civil liberties. We continue to believe that that board, that we recommended and the Congress put into being, has critical functions and should be established. It doesn't now exist.

The President has not yet appointed the members. So, we urge President Obama to reconstitute it, quickly appoint its members, and to allow them full access to the information and the authority to perform and do this essential function.

Now, you are doing exactly what is required, here in this room today. Nothing, probably, is as important in this whole intelligence area than your oversight, Congressional oversight. And we placed a tremendous amount of importance to that in our report. I know our recommendations helped make the creation of a House Homeland Security Committee and a Senate Homeland Security Committee and Governmental Affairs Committee. However, there is enduring, fractured, and overlapping committee jurisdictions. And that's true on both sides of the Hill. And this has left Congressional oversight, in our opinion, not yet in a satisfactory place.

DHS entities still report to dozens of separate committees hundreds of times per year, and that takes, as every Secretary has told us, a tremendous drain on their time and resources for their most senior officials.

Furthermore, the additional melee among scores of Congressional committees has led to conflicting and contradictory tasks and mandates for DHS.

Now, we worry that unless we work to fix this system, it's unworkable and it could make this country less safe.

We also called Congressional oversight over intelligence dysfunctional, at the time of our report. We made recommendations to strengthen the oversight committees, which were not accepted by the Congress, although undoubtedly some progress has been made.

Today, we'd just like to emphasize the tremendous, enormous importance we attach to rigorous oversight of the intelligence community. Congressional oversight can help ensure the intelligence community is operating effectively and help resolve disputes about conflicting roles and missions when they occur.

So, we urge you all—the Congress—to take action to strengthen the oversight capabilities of the intelligence committees, because we think if you don't oversee intelligence, nobody does. And we would commend you—commend that task to you.

Thank you.

The CHAIRMAN. Thank you, Governor, very much.

There's no way that I can agree with you more about the need for oversight. It's really the only instrument that the legislative branch has. And it—because of its classified nature, it's reserved, really, to two—for the most part, to two committees, one in each house. And I do know that over the last number of years, what—the basic changes that have been made are, in fact, to take the Intelligence Committee, which was a so-called "B committee," to make it an "A committee"—more budget. And second, it was term-limited. It was term-limited to 6 years or 8 years, I forget which it was. But, we got rid of that. So, now members are on permanently, at the discretion of their respective leaders in their respective parties in both houses.

A great deal of the experience of the Iraq and Afghan war were, in fact, trying to bludgeon—you know, I—there are all kinds of words I could use for it—to try and pry out from the administrations—both administrations, Republican and Democrat—who hold

on—people think that the Intelligence Committees own the intelligence, they have the intelligence. They don't. They only get what the Administration is willing to give them. And so, sometimes you have to use strong-arm tactics. Somebody says, "I need a deputy." I said, "I need full information." I used that tactic once, and it worked. A DNI got a deputy director because he agreed that he would brief not just the gang of six, the gang of four, the gang of eight, and all of that nonsense of earlier years, but the entire committee. And so, that's the—that doesn't say that we're getting what we should be or that we're doing what we should be with what we get, but it does mean, at least, the process is headed in the right direction. And all of the folks involved—and I feel very strongly about that.

Let me just—I've already used a lot of time. I'm just fascinated, Secretary Napolitano, with this concept of screening watch lists. We've got the TIDE database. We've got the terrorist screening database. We've got the Selectee—that's—the first is 550, the second is 430 individuals. And then we go to the Selectee, 14,000; and the No Fly, 3,400.

My question and my frustration is—and, Director Leiter, I think that you said that there was movement to restrict even further the No Fly List. I think you said that.

Mr. LEITER. Prior to December 25——

The CHAIRMAN. Yes.

Mr. LEITER.—we experienced——

The CHAIRMAN. But, see, that's so wrong. I don't understand why, for example—with this Farouk, Abdulmutallab, why is it that he can get on a list, which comes back from the State Department and goes to—it's classified, but I know where it is. And so, it's not possible to say that there is not some cause for doubt about him as a person, but he doesn't end up on any list that means anything. So, he just cruises right on through, gets his 2-year visa, Lagos, Amsterdam, Detroit, no problem; 2-year visa. I don't understand—well, the question I want to ask is, Do you think that there is—Secretary Napolitano, particularly—both of you—that there is—that there's a false sort of division of databases and groups that you move from one to another?

You know, my instinct, just as an individual citizen, is that the "No Fly List" ought to be a whole lot larger. Why do we make the assumption that, because somebody's on the—you know, the terrorist screening database list, et cetera, that that doesn't—that's, you know—and they're determined—NCTC and the—conjunction with the FBI—they determine they're known or reasonably suspected terrorists, but they can still fly. And they're not even on the "Selectee List," much less the "No Fly List." I don't understand those divisions. Should they be rethought, in view of what happened on Christmas, or do you think I'm overreacting?

Secretary NAPOLITANO. Mr. Chairman, first of all, that is an integral part of the review and the actions that the President has directed, that that entire set of processes and protocols that were set up to move from the larger to the more specific, in terms of the databases, be relooked at, in light of what happened on December 25, and in light of what could happen in the future. So, it shouldn't just be reactive, but also proactive.

As I said before, you know, the CBP looks at the—and these are protocols that have been in existence for a number of years—but they look at the——

The CHAIRMAN. You'd better explain——

Secretary NAPOLITANO.—No Fly List.

The CHAIRMAN.—"CBP" to us.

Secretary NAPOLITANO. Customs and Border Protection.

They look at the "No Fly List" and the "Selectee List," in terms of what happens internationally. That, too, is something that may need to be reexamined. But, I think the real heart of your question goes to the watch list, their systems, their creation overall. And let me defer to Director Leiter on that.

Mr. LEITER. Mr. Chairman, the basic question, should the distinctions and differences be reevaluated? The simple answer is, "Absolutely. Yes." And that's what the President has directed, and we want to.

I will say, there is an enormous variation between different people on those watch lists. It ranges from the person who's associated with the financier to the operative. Now, the standards that have evolved since 9/11—and again, were promulgated in 2008 and 2009—made us make distinctions which are readily apparent after 12/25—are distinctions that, I believe, the Congress and the American people are very uncomfortable with. And I believe that it would make much more sense, in light of the reaction we have seen, to have many more people on the No Fly List or the Selectee List than we do today.

My only point about the pressure was, I will tell you, prior to December 25 of this year, the pressure had been, in fact, in the exact opposite direction. The pressure was to remove and scrub those No Fly and Selectee Lists and the watch lists, to inconvenience as few people as possible, and reduce the number of false positives. That was the pressure under which we existed, and I am more than happy—and, as the President has directed us to do, we are going to reevaluate that, based on the events.

The CHAIRMAN. Good.

I'm going to call on, obviously, Senator Kay Bailey Hutchison. After that will be Senator Dorgan, followed by Senator Begich, who appears to be missing an opportunity to ask a question.

STATEMENT OF HON. MARK BEGICH,
U.S. SENATOR FROM ALASKA

Senator BEGICH. Mr. Chairman, I have to co-chair a hearing at 4 o'clock.

The CHAIRMAN. OK.

Just preside over the Senate?

Senator BEGICH. No. An actual——

The CHAIRMAN. Oh, OK.

Senator BEGICH.—a real work meeting.

The CHAIRMAN. Oh, a real—OK, OK.

[Laughter.]

The CHAIRMAN. OK.

The CHAIRMAN. Anyway—Senator Hutchison.

Senator HUTCHISON. Thank you, Mr. Chairman.

I just want to ask one more question along the same lines as the Chairman's, and that is about the association with the Yemeni cleric who used to operate out of Maryland. After the Fort Hood incident, it would seem that there would be a deep look into everything that might be associated or connected with that particular cleric. And so, my question is, Why wouldn't Mr. Abdulmutallab's association with that same cleric have been enough to get him on the database, to at least have a big yellow flag, if not a red one?

Mr. LEITER. Absolutely, Senator.

To begin, immediately after Fort Hood—and this is continuing—we have, in fact, engaged an interagency—CIA, FBI, National Security Agency, NCTC—scrub of all of Anwar al-Awlaki, looking at his various contacts, to determine who poses a threat. What——

Senator HUTCHISON. And then, would those people that he has tentacles to, now be put on watch lists? I mean, can we be assured of that?

Mr. LEITER. Those individuals—it depends. It depends on the nature of those communications. In some cases, under the existing standards, were someone to send—you know, communicate in a way which was completely innocent, it might not put that person on the No Fly List; it might put that person on a different layer of the list. And, of course, the list itself, and being placed on that list cannot be based purely on protected First Amendment activity. So, there may be some issues there.

With respect to Mr. Abdulmutallab——

Senator HUTCHISON. Let me just ask you one——

Mr. LEITER. Of course.

Senator HUTCHISON.—one thing more, though.

OK, you had the Yemeni connection. And then you had the man's father, who raised a flag of some kind. Do you have the capability to merge that kind of information and raise the level on someone like that?

Mr. LEITER. Absolutely, Senator. And, in fact, the failure here, and the failure on our part and elsewhere, was not making that connection. It was not making that connection between what the father came in and said and other sources of intelligence. Now, some of those sources of intelligence weren't flagged in a way that made it more likely that that intelligence would be connected. So, there were some failings there. But, also, the basic act of seeing all that intelligence and piecing it together is what we did not do.

Senator HUTCHISON. But, let me——

Mr. LEITER. But, undoubtedly, had it been, he could have been at a higher level of watch list.

Senator HUTCHISON. OK, let me ask you this, because it goes back to the first thing that the Chairman said in his opening statement. Do we have the tools now to communicate, completely and effectively, without bureaucratic mumbo-jumbo, between intelligence sources and security forces on the ground, so that you can put those kinds of different levels of an awareness together to raise it to a substantial awareness level?

Mr. LEITER. Senator, this is going to be hard to believe, but probably the single best example, where we go from the most classified sense of intelligence down to the operator in the field—and this is true even after 12/25—is, in fact, the watch list. The problem here

was not that that information did not flow, because it can flow quite easily to the police officer in the street, to the visa officer, to the Customs and Border Protection officer. The problem is, we didn't have the right derogatory information associated with that record. So, we hadn't connected the intelligence to raise the flag, but the information could have flowed quite easily.

But, a second piece of your question is, do we have the systems in place that make it easy to connect those pieces of data in the first instance? And the answer is, yes, in some places, and not nearly enough so in others. Some agencies are far ahead of others, and we still have, clearly, some systems which are so rudimentary and basic that they're not doing a good job of that. For example——

Senator HUTCHISON. OK.

Mr. LEITER.—the State Department's visa system, where, when they mistype one letter in the name, his visa does not come up. I consider that a significant weakness in the technological system that enables effective information-sharing.

Senator HUTCHISON. OK. I guess my final question, to try to just get to the nugget, is, Do you have all of the authority to do what needs to be done? And I'm not even saying this is easy, because I know if a father comes in and says, "I think my son is someone you should watch," maybe that, in itself, by itself, isn't enough. But, then you have the Yemeni cleric, and maybe that wasn't quite enough to also matter. But, together, you've got to be able to say——

Mr. LEITER. Absolutely.

Senator HUTCHISON.—"OK, put this together, and it's really big." So, do you have the authority—and, Madam Secretary—do you all have the authority to get to the heart of this and not have all these constraints and different bureaucracies and different rules and all of the confusion that seems to maybe exist sometimes?

Mr. LEITER. Senator, I'll try to be very brief.

I think the basic system structure works. But, there are four areas which, undoubtedly, we need to focus:

One is technology. The technology is not as advanced as it needs to be to connect all of these pieces.

Second, in terms of authorities, to make sure that people are following up in the way they need to follow up. Those authorities, frankly, to the National Counterterrorism Center, were purposefully vague, and we are now working with the White House, through the President's direction, to make sure there is accountability.

Third, we simply need the people to do it, because you can have the best Google-like tool in the world; you need the people to work that watch list and look at that information.

And fourth, I think——

Senator HUTCHISON. Are you saying we don't have enough people on the job? Is that——

Mr. LEITER. I think—absolutely. As I tried to make clear, we did not have enough people to put on this Yemen problem, and we did not shift people away from other problems quickly enough. And now, what we've been directed by the President to do, I think there will be a resource tail to make sure you can pursue these minute leads in a way that you can have greater confidence that they will

be tracked down and will be connected exactly the way you and the American people expect and deserve.

Secretary NAPOLITANO. Senator, I—what I would add to that is—again, the international dimension of this is so very important. You know, he traversed two international airports, Lagos and Amsterdam. Every airport—not every airport in the world operates at the same level of security standards. We also need, I think, quite frankly, to work more closely on the international scale, in terms of sharing information about individuals—who's had a visa revoked, and why, for example. And so, that is part and parcel of the corrective action that we are taking.

Senator HUTCHISON. Thank you.

The CHAIRMAN. Thank you very much.

This is—this list, which changes as people come in and go out, which is what always happens, which is fine—is done in order of original appearance so that it's fair, although some may like it more than others.

Senator Dorgan.

Senator DORGAN. Senator Rockefeller, thank you very much.

I am not exactly clear on all of this, so—and I know it's complicated. I wasn't sure, back in 2002, whether creating the Department of Homeland Security was the right thing to do. We put 22 agencies together, in the biggest merger of Federal agencies since the second world war. Maybe that's the right thing, but it—we put a lot of different cultures together.

And then the question of DNI; it wasn't clear to me whether it was very smart to do that. I—although I understood, we had all these stovepipes sticking up and nobody trying to coordinate them. So, I understood that wasn't working very well.

But, as I understand it now, we have—we now have 16 different agencies involved in the intelligence system; eight agencies involved in the watch-listing process—those eight agencies in the Terrorist Identities Datamart Environment. Then we have, I believe, three different agencies involved in placing individuals on the terrorist screening database. And only then would Homeland Security come in and make decisions about placing individuals on either a No Fly List or a Selectee List. And maybe that's a—maybe that's not exactly correct, but it seems to me you've got a lot of agencies doing a lot of different things.

What I don't understand is this. When we created DNI, we were going to try to deal with these stovepipes. So, what happens—if you can tell me in an unclassified situation—what happens when a father comes and says to our intelligence community, "Look, I've got a kid out there"—and I've seen some rumors about what the conversation was, but, "I've got a kid out there that's gone wrong. It appears to me there are some—you ought to have some concerns about some links to terrorism." What happens to that information? Where did it go? And where was the failure?

Secretary NAPOLITANO. If I might, before—I'm going to——

Senator DORGAN. All right.

Secretary NAPOLITANO.—defer to Mike again, but, there was something in your question that was not correct, and——

Senator DORGAN. All right.

Secretary NAPOLITANO.—it's that DHS does not create the Selectee or the No Fly List. We receive the Selectee or the No Fly List, and that is then used by CBP officials at foreign airports to advise foreign governments or foreign air carriers, as the case may be, about particular individuals.

Senator DORGAN. All right.

Secretary NAPOLITANO. I just want to be——

Senator DORGAN. Thank you.

Secretary NAPOLITANO.—clear about that.

Senator DORGAN. Thank you.

Mr. Leiter?

Mr. LEITER. Two things should have happened when that father came in. One thing happened, one thing did not.

The first thing is, the agency that received that sent a message back to headquarters, and that message was also available to NCTC. That's the good. Not so good, it was not disseminated in a way that it was widely available to the rest of the intelligence community. Now, I do want to stress, that's still different from what happened on 9/11; that was simply——

Senator DORGAN. Why was it not disseminated?

Mr. LEITER. It was, fundamentally, the oversight and mistake of an individual office, and I believe the director—Director Panetta—Leon Panetta—has already taken steps to solve that problem.

Senator DORGAN. Was there a process or procedure that was ignored? Or was it a person that made a mistake? Tell me——

Mr. LEITER. Senator, I'd actually prefer—happy to take it up with you in some sort of closed session. But, also, I would, frankly, like to defer to Director Panetta, who can speak more specifically to the procedures of that agency.

But, the information was somewhat available.

The second thing that should have happened, and did happen, was, after that meeting, the State Department and the embassy had a—the country team had a meeting to say, Was this person someone that they had to be worried about? And they in turn nominated him to the Terrorist Identities Datamart Environment at NCTC as a possible terrorist, based on this interview. That occurred; he was nominated; he was placed on the watch list. The one thing that did not occur there was, again, when they checked to see if he had a visa, they misspelled his name, and hence, did not discover he had a visa.

Senator DORGAN. Yes, they misspelled the last name, apparently?

Mr. LEITER. Correct.

Senator DORGAN. And so, one of the intercepts—I'm—understand one of the earlier intercepts actually had his two first names.

Mr. LEITER. Umar Farouk——

Senator DORGAN. Yes.

Mr. LEITER.—that's correct.

Senator DORGAN. And so, there's a—there's his father; there's an intercept with two first names that were spelled correctly; there's an intercept about maybe something December 25; there's an intercept with somebody from Nigeria and a possible action. And so, we have all these things. I guess I'm wondering, with all these agencies—sixteen and eight and three, or whatever—is there somebody

that's sitting around, that—as a result of DNI, that gets rid of stovepipes, and you bring it in to a desk or a room or some situation room, and somebody gathers all that and says, "Aha. I see. This is a puzzle, and I just got the five pieces. I've put the five pieces together. And we got a guy out there that's trouble, and we're going to make damn sure he's not on an airplane"?

Mr. LEITER. Senator, the primary responsibility for doing that was mine, as the Director of National Counterterrorism Center, NCTC. Also with responsibility, pursuant to the President's conclusions, and consistent with past practice, was the CIA. We both had responsibility to do that, and we didn't do that. Now——

Senator DORGAN. Well, I understand—from an organization, and from heading an organization, I understand what you're saying, and I admire that. But, I'm asking, In the organization, do you have a group of people who are sitting there, pulling all that—those pieces together, to say, "Aha. Now we see something that's about to happen, and we're going to take action"?

Mr. LEITER. Senator, two pieces of that. One, I will tell you that, although I can't speak to it fully in an open session, part of what you cited in the press reports was, in fact, discussed in analytic products that we provided to policymakers concerned with operations. What we did not know, and what we did not connect, is exactly who and where. So, we were in fact concerned of an operation, but we hadn't pieced those pieces together.

But, second, if I may, Senator.

Senator DORGAN. Yes, of course.

Mr. LEITER. One of the reforms that we've already started to initiate, and which I think is critical and does have some repercussions in terms of the need for people, is to put together exactly the teams that I think you imagine. And their sole job is not to write intelligence for policymakers, but their sole job is to dig into, in an interagency way, with all the information, these bits of data, and piece them together and uncover the plots.

Senator DORGAN. Mr. Chairman, my time is expired.

Let me thank—I have other questions I'm going to submit, if I might.

And let me also say to you that I see there are other relatives of the—the victims of the Colgan crash. I want to mention that they are here, too. And they are at every hearing that we hold dealing with the issue of safety. And I admire the passion with which they now serve their country, coming to these hearings.

The CHAIRMAN. Thank you, Senator Dorgan.

And now Senator Lautenberg.

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

Because we have so many questions that we'd like to ask, and the time not permitting that, can we be assured, Mr. Chairman, the record will be kept open and that the witnesses are instructed to——

The CHAIRMAN. Absolutely.

Senator LAUTENBERG.—respond——

The CHAIRMAN. Absolutely.

Senator LAUTENBERG.—to that?

And I would ask our wonderful witnesses at the table—that includes all of you, by the way—that the answers be as brief as possible, rather than questions taking all the time.

But, I want to—the mystery about whether or not someone on one list doesn't match up with another—I mean, I come out of the computer business, and so does my colleague here, and, you know, there are lots of things that we do in the commercial world that get names identified immediately. If you ever walk in with a credit card and you're in Paris or Lisbon or wherever, put your American Express through the slot, and the answer is—the answer comes back immediately. Now, why, therefore, isn't the technology available that talks about those people who are on the No Fly or the terror watch list? I think it's outrageous to suggest that, you know, multiple departments are required to check on one another and create an organization that gets rather cumbersome at its roots.

Mr. LEITER. Senator, if I may, because I must have misspoke. The lists are coordinated with one another. There is no disconnect between the lists, except if there has been a choice that the lists should not match. And what I mean by that is, if you're in TIDE, we know, if you're in TIDE, whether or not you're in the next list and whether or not you're No Fly. And there has been a decision that one does not qualify for the other. The lists speak to each other and are fully coordinated with one another.

Senator LAUTENBERG. Thank you.

Governor Kean, the Detroit bombing attempt raised questions about who should be on the terror watch list—much of what we're talking about here—including the No Fly List. But, even people who pose such a serious threat that they're not allowed to fly are still able to buy guns in this country. And there's discouragement of excessive interference or followup—you have to destroy lists in 36 hours, and you have to respond in 3 hours and all. And here we're talking about something that—talking about, Worried about a gun? You got an airplane full of people. There is—in my view—there is no comparison to the two threats that pose.

Do you support closing the terror gap by giving the Attorney General the authority to deny gun purchases to people who are on this list? Just to deny them outright. We've heard the plea on the other side, said, "Well, someone could be on there incorrectly or unfairly." Too bad. I don't want to break the law, and I don't want to invade privacy, but the fact of the matter is, we ought to be able to access these things, and err on the side of the safety of the American people. What do you think?

Mr. KEAN. Senator, the Attorney General has asked for that authority, and I would certainly back him up. But, he should be given it. I think to allow people on the terrorist watch list to go in and purchase weapons of any kind is just not very wise. And as far as the other law goes, the FBI, as we know, had the Fort Hood shooter under observation, they were looking at him. What they didn't see was the fact he'd walked into someplace called "Guns Galore," and bought weapons, because the law now says the records have to be destroyed within 24 hours; used to be longer than that. I suspect if it were there longer than that, the FBI might have had that information; might have connected the dots, and who knows whether or not it would have been prevented or not. So, I would rec-

ommend that you might look at both those things. And particularly as the—this Attorney General has asked for—and the previous Administration also asked for—terrorists should not be allowed to get weapons.

Senator LAUTENBERG. Secretary Napolitano, what's the—what does your department think about closing this loophole, this—that permits gun purchase? I am leaving the Detroit situation to the review by my colleagues. I want to focus more on this relatively narrow area.

Secretary NAPOLITANO. You know, Senator, I'm not sure that right now I'm prepared to give you an answer on that. I am—what I am prepared to say is that, look, there are a lot of things that have to happen to prevent somebody like an Umar Farouk Mutallab from getting on an airplane. It's a very layered system. It begins with intel and all of the ways that Mike has described how the intel works, up to when somebody shows up at an airport, then all the layers within the airport itself—some seen, some not seen. It's all of those things combining together that, done right, and done in a coordinated fashion, minimize the risk that there will be an attack on Americans.

Senator LAUTENBERG. Mr. Chairman, are you going to permit——

The CHAIRMAN. Yes, we'll continue——

Senator LAUTENBERG.—a second——

I just want to close by saying there are some 600 million American—Visa cards around the world. You can go anyplace in the world and try to buy something, and they know immediately whether you're eligible.

The CHAIRMAN. Yes. And another question that comes from that is, what is it that airlines can do if they're paid in cash? I'm convinced there has to be something they can do to follow up. I don't want an answer to that now.

You have to leave in 10 minutes for Spain—leave here for Spain. That's what I call——

Secretary NAPOLITANO. Sir, I'll be happy to hang around for a few more minutes, if I can answer some more questions.

The CHAIRMAN. Well, then now you've made a liar out of me to Senator Snowe.

Mr. LEITER. I'm happy to leave in 10 minutes for Spain, Mr. Chairman.

[Laughter.]

The CHAIRMAN. Oh, you do. OK. All right.

Secretary NAPOLITANO. Mr. Chairman, if I could leave by 4:30, that would be——

The CHAIRMAN. That's what I'm talking about. That's called 10 minutes.

Secretary NAPOLITANO. OK.

[Laughter.]

The CHAIRMAN. Thirteen.

[Laughter.]

The CHAIRMAN. Will you please give me some idea of why, when you go over there and meet with the Europeans, why—what hope is there for bringing some sense of rationality between the practices that we pursue at home, in terms of screening, machinery,

you know, whole-body imaging, which is considered a civil liberties problem. On the other hand, that's the only thing which probably would have discovered what this guy had in his underpants.

What do you sit down and talk with them about? There has got to be a common system that works around the world, but you're dealing with separate societies. Some of them are so pro-civil liberties that they are very lax. On the other hand, I don't know how any of them could be in Europe, because they're the ones who've taken most of the pounding.

So, what do you do? I mean, what about the folks at Lagos? What about the folks at Amsterdam? What about the folks in less- or well-traveled countries? How do you rationalize the system? What are you going to do for the next few days?

Secretary NAPOLITANO. First, we're using the December 25 attack as a catalyst. There were passengers from 17 countries on this plane. This illustrates the international nature of this problem. And the initial meetings that the Deputy Secretary held, in the immediate wake of December 25, were fruitful in a way that some meetings that I'd had over the course of last year were not. So, we're going to use this attack as an opportunity to see if we can get agreements made that we have not been able to get before.

Second——

The CHAIRMAN. Like what?

Secretary NAPOLITANO. Like better exchange of information about passengers. Like standardization of the kinds of equipment and procedures that will be used in airports on randomized bases, so the terrorists can't predict what's going to happen at—one at one time or one at another. Like training and increase of capacity of law enforcement on the ground in countries, particularly in airports that may not have the capacity right now. Like a real outreach and focus on airports that have the larger percentage of throughput of last points of departure to the United States. All of that underway.

We'll be meeting with individual countries. We'll be meeting with groups; *i.e.,* those from the EU. I will be meeting with ICATA, which is one of the international air travel associations, on Friday. And we've already been meeting with ICAO, which is the U.N. air safety, air security branch, which is located in Canada. We've already been meeting with them.

And our goal, Mr. Chairman, is to say, this is not just a United States problem. In this century, everybody from around the world needs the ability to travel and to know that the air environment is a safe one. So, it's designed to get more uniform standards, higher standards, increased training capacity, increased both physical law enforcement and technology available around the globe.

The CHAIRMAN. OK. I thank you.

And I call upon Senator Snowe.

And I thank you for yielding.

STATEMENT OF HON. OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman.

And I thank all of you for being here today.

These are obviously, very key forums for eliciting exactly what went wrong and what we must do to prevent it in the future, without question.

As one who has been involved in these issues for many years, going back into the 1980s, when we were dealing with aviation security, international airports, and the list goes on—information-sharing and so on—this all still has a familiar ring, in terms of rigid stovepipes. And it seems, a cascading series of failures required passengers on a plane to stand between a terrorist and a disaster. So, we could have had a profound consequential event in this country. And I think we all understand that. But, I certainly hope that somehow the sense of urgency in our institutions is not sublimated into bureaucratic quagmires. It's something that we have to be focused on each and every day. I know there are extraordinary men and women who serve this country, so I understand that, and I understand your service and contribution, and I thank you.

And to the tireless efforts of Congressman Hamilton and Governor Kean, thank you. You've been tenacious and tireless, as watchdogs and in conducting oversight over this major, mighty endeavor for this Nation. You have unparalleled insights and expertise, which I deeply appreciate, and thank you for the continuity of your service.

And to all the families who are here today, and who have lost loved ones, they continue to provide extraordinary public service, even in light of the profound personal grief that they have had to endure. And that's a tribute to them, and that's why we're here today, continuing to ask these tough questions, because this is what it's all about. We've got to get to the heart of the matter.

Secretary Napolitano, I want to ask you several questions regarding Umar Farouk so that I'm clear on the relationship that DHS has, in terms of the information that is gleaned from such individuals. Now, you said that you're a consumer of information; DHS is a consumer of information. But, you also have an analytic branch within the Department of Homeland Security. Now, was Umar Farouk ever debriefed by the Department of Homeland Security when he visited the United States and after he had traveled to Yemen?

Secretary NAPOLITANO. Senator, I think that, in an unclassified setting, that's probably not a question that I should answer.

Senator SNOWE. OK. So, when Customs and Border Protection receives a manifest 72 hours before departure, at which point was it clear that they needed to question him further?

Secretary NAPOLITANO. They receive, 72 hours in advance of departure, passenger name data, which is different than the manifest, which has a much more complete set of information. What they push forward to a foreign airport, where there—where CBP has personnel—and we don't have personnel at all foreign airports—but, where we do, they push forward the No Fly and the Selectee List.

The No Fly List means you advise the carrier, "That person should not board a plane." Selectee, you advise the foreign government, "That person needs to get a secondary screening."

And the key difference you're getting at, and your question is getting at, is, Well, what happens—Why was it, when he was going to get to Detroit, he was going to be in secondary? He was going to be in secondary when he got to Detroit because he had been identified as someone, although not on No Fly or Selectee, but, he was in the larger database that should be looked at for secondary screening before admission into the United States.

So, you have one set of things that say, "Well, should he be allowed on a plane?" And the other is, "Should he be admitted into the United States?"

Senator SNOWE. See, I don't understand that distinction. I have a really hard time with that.

Secretary NAPOLITANO. Yes, I——

Senator SNOWE. I mean, I'm just——

Secretary NAPOLITANO. Yes.

Senator SNOWE.—I'm stunned by it, to be honest with you. If somebody's a threat, they're a threat. I don't know how you make a distinction between a threat and an aviation threat. I just don't understand that. And second——

Secretary NAPOLITANO. It——

Senator SNOWE.—how was he ever allowed on the plane? You know, I think that it's a fair presumption—then once that information has been disseminated—that it has to be evaluated before anybody gets on the plane. And that's what I don't understand. And they have that manifest and that information 72 hours prior. And so, to—all of a sudden, they decided that they needed to question him further and are going to wait——

Secretary NAPOLITANO. No——

Senator SNOWE.—til he gets to Detroit?

Secretary NAPOLITANO. Senator, I'll be happy to provide you with a more detailed briefing, and your staff. But, if I might—again, 72 hours in advance, they have a passenger name record. It can be 30 minutes in advance that they get who actually is boarding a plane, with more information that can be matched against a variety of databases.

Now, in terms of why he was allowed to get on the plane—if he had been on the right database,—if he had been on the right list—forget databases; just take databases out of this equation—if he had been on the right list, he would not have been allowed to get on that plane in Amsterdam. The mistake made here was that he was not on the right list.

Now, what are we doing to fix that? Part of it is improving the quality and extensiveness of the lists. Part of what we are doing is looking at how we use the lists themselves.

But, again, since he was coming in from an international airport, we're not a solo actor, even in that regard, because, even in that regard, we need cooperation; in this case, from the Dutch, but it could be from another country, as well.

Senator SNOWE. But, what information did you have—that Customs and Border Protection had—to warrant further questioning, between the time he boarded the plane in Nigeria and the time he landed in Detroit?

Secretary NAPOLITANO. By that——

Senator SNOWE. Because, that—it's——

Secretary NAPOLITANO. Yes. By that time——

Senator SNOWE. I'll make certain assumptions that he was somehow—we've had more information on him——

Secretary NAPOLITANO. By that——

Senator SNOWE.—and he should have been in the database, and that should have been pulled up.

Secretary NAPOLITANO. I'm sorry. I didn't mean to interrupt.

Senator SNOWE. Yes.

Secretary NAPOLITANO. Apologize.

By that time, he had been matched with the note that had been issued by the State Department of some concern that he was associated with an extremist organization. That note, which was the State Department note, had never been matched up appropriately with the watch lists and the No Fly List.

Senator SNOWE. But, your department can nominate individuals for the watch list. Is that correct?

Secretary NAPOLITANO. Yes——

Senator SNOWE. And for the No Fly List.

Secretary NAPOLITANO. Yes.

Senator SNOWE. You have that authority.

Secretary NAPOLITANO. Yes.

Senator SNOWE. I mean, you don't create it, but you can nominate individuals, based on your acquisition information. And you have a number of analysts. So, clearly, it's a sizable organization, to also analyze individuals that you may have debriefed along the way. I think that's important to understand.

Secretary NAPOLITANO. And, Senator, I think, in terms of that, we should go into classified. But, let me say this. And this is an important question for this committee and for the Senate. Because, as has already been mentioned, there has been, in the creation of the Department and the creation of the NCTC and the creation of the DNI, all sorts of overlapping jurisdictions and authorities and what have you. A question is, Does the intel and analysis part of DHS do the same thing as NCTC? Does NCTC do the same thing as others? Are we supposed to be a redundancy? What is our contribution in the I&A field? And the fundamental contribution of this I&A, this department's I&A, is to take information—intel—that has been gathered and analyzed, and to push that out; push that out operationally where it needs to go, or push that out, most importantly, or as importantly, to State and local law enforcement.

So, yes, we have an intel function. Yes, we can nominate. But, we are not a redundancy. And I don't think we should be a redundancy with NCTC or DNI. The redundancy here, on the intel side—and this was explained by John Brennan, in the aftermath, in the immediate report—the redundancy that was designed in the system, with respect to this information, was between the NCTC and CIA.

Senator SNOWE. OK. Thank you.

The CHAIRMAN. Thank you, Senator Snowe.

Senator SNOWE. I'd like to submit my statement.

[The prepared statement of Senator Snowe follows:]

PREPARED STATEMENT OF HON. OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Thank you, Mr. Chairman. We are here this afternoon with our distinguished panelists, including Secretary Napolitano—who is appearing before us for the second time in 2 months—as well as Director Leiter, Governor Kean, and Congressman Hamilton to determine how this egregious breakdown of the security network instituted in the aftermath of 9/11 occurred, and how such colossal and eminently preventable failures are avoided in the future. This is nothing less than the security of our homeland, our people, and our Nation and our efforts must rise to a level commensurate with both the challenges and the potentially catastrophic consequences.

Regrettably, it is all too evident that with respect to our aviation security, we've returned to square one. Despite our best efforts, inexcusable and systemic breakdowns continue to endanger the lives of our citizens and those visiting our country. And on Christmas Day of 2009, after a succession of collapses in security, only a handful of heroic passengers stood between a terrorist . . . and disaster.

It is simply *unacceptable* that the same gaping holes that have persisted since the tragedy of September 11, 2001, continue to plague our efforts to mitigate the threat against commercial aviation. Rigid stovepipes within the various intelligence agencies and the law enforcement community disturbingly have reappeared and inhibit the sharing of information. And the requisite and required sense of urgency in our governmental institutions seems to have been sublimated by bureaucratic quagmires that preclude proactive steps from being taken. Indeed, how else can we explain the myriad red flags that were either missed or ignored?

The passenger, Abdulmutallab, purchased a ticket with cash . . . did not check any luggage for an international flight . . . had recently visited Yemen . . . and the Department of Homeland Security (DHS) knew he was a threat inbound for the U.S. He did not even choose to bring a coat when traveling to Detroit in December. Each of these facts should have raised a red flag.

This information, taken together, would have certainly resulted in a passenger at Dulles or Logan Airport or anywhere else in the country being taken aside for additional screening at the minimum. Yet, this individual who was already identified by our intelligence agencies as a "threat" was not only allowed to board an aircraft bound for Amsterdam, but was then permitted to board another aircraft bound for the United States! Why? Because, according to National Security Adviser John Brennan, he was not classified as an 'aviation threat.' *Let me repeat,* he was known as a *threat*—but not, apparently, classified as an "*aviation threat*" *Moreover,* DHS knew of this individual's presence on the flight, but reportedly intended to question him AFTER he landed in Detroit!

These are astonishing lapses, and they *should not have occurred.* Did the intelligence community fail to provide the requisite information to the Department of Homeland Security in order to place Abdulmutallab on the "No-Fly" List? Yes. And there are *zero excuses* for the ongoing problems this country is having with the various intelligence agencies' systemic breakdowns. At the same time, when does DHS step forward based on the information they already have and act independently? Abdulmutallab was denied access when attempting entry into Britain—the British Home Secretary, Alan Johnson, said "if you are on our Watch List, you do not come into our country."

So why did someone at DHS decide to wait until the "threat" arrived in the U.S., rather than provide additional screening in Amsterdam, or better yet, Nigeria? There are so many lapses, so many intrinsic failures—that I cannot help but feel after all the billions we've spent in the last decade erecting this vast security network, it is remarkable we are still asking the same questions this committee asked after the tragedy of 9/11. And that is a telling indictment of the current state of the system that's been created.

Who and what is responsible? As I stated before the Senate in 2004, I saw firsthand the consequences of a lack of accountability during my 12 years as a member of the House Foreign Affairs International Operations Subcommittee and as Chair of the International Operations Subcommittee of the Senate Foreign Relations Committee

Among other issues, it was a lack of accountability that permitted the radical Egyptian Sheik Rahman, the mastermind of the first World Trade Center bombing in 1993, to enter and exit the U.S. unimpeded five times, even after he was put on the State Department's Lookout List in 1987. In 1995 and again after the terrorist attacks of 9/11, I introduced legislation establishing Terrorist Lookout Committees in our embassies and consulates abroad—all in an effort to create greater accountability in the protection of our homeland.

As a senior member of the Select Committee on Intelligence, I am well aware of our enemies' adaptability—which is all the more reason our security and intelligence networks cannot afford to be bogged down in bureaucratic wrangling. We too must be able to *adapt* rather than simply *react* to each threat as it appears. The 9/11 Commission warned that terrorists constantly analyze our defenses, look for areas where security is weak, and plan accordingly. We absolutely must look forward, to prepare for these new threats, while continuing to guard against current dangers.

Unfortunately, there remain other vulnerabilities that have gone unaddressed. Unscreened cargo is still loaded onto commercial aircraft, yet no one can be certain how much is actually screened, and to what standard—contradicting the Homeland Security's claims that they have already reached 50 percent screening and will achieve 100 percent by this August. The uncertainty surrounding air cargo screening is particularly galling given my work with Senator Hutchison on air cargo security legislation as far back as 2002.

Additionally, on December 7 of last year, TSA mistakenly published its security screening manual and protocols on-line, a classified document that revealed—on the Internet, no less—how to circumvent security. This incredible gaffe could have provided information to the Christmas Day bomber and his handlers, information used during his trip from Nigeria to Detroit.

Another issue of great significance to this committee is the relationship we have with our international partners with respect to screening flights bound for the United States from other countries. According to TSA Director of Global Security Programs Cindy Farkus, there are fewer than two dozen TSA inspectors around the world responsible for ensuring that 245 foreign airports are complying with international security standards. That is an unacceptable deficiency, considering the Federal Aviation Administration's (FAA) forecast of more than 150 million passengers flying to or from the United States this year. Even *more* troubling is the Government Accountability Office's conclusion that without frequent visits to each of these airports on a regular basis, "security deficiencies . . . may arise and go undetected and unaddressed."

In sum, Mr. Chairman, our work begins anew—I am certain Governor Kean and Congressman Hamilton would agree that, particularly given their yeoman efforts on the 9/11 Commission and in the intervening years—we must redouble our efforts to tear down the walls of bureaucracy that unnecessarily restrict our ability to successfully protect America. Our constituents, and the nation, deserve nothing less. Thank you, Mr. Chairman.

The CHAIRMAN. I—now Senator Klobuchar, to be followed by Senator LeMieux and Senator Ensign and Senator Cantwell and Senator Udall.

VOICE. Mr. Chairman?

The CHAIRMAN. I want to get one thing straight. Who has to leave at 4:30?

[Laughter.]

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Could I ask my question, and Senator——

Mr. HAMILTON. Mr. Chairman, Governor Kean has a 5 o'clock train he has to be on, so he has to leave promptly, as well.

VOICE. Right.

The CHAIRMAN. OK. But, you do not, Mr. Director?

Mr. LEITER. I'm here at your pleasure, Mr. Chairman.

The CHAIRMAN. OK. That's good. I thought you'd said you had to leave. OK.

Senator Klobuchar.

Senator KLOBUCHAR. Thank you.

Secretary Napolitano, just to shift, for 1 minute, here, we have 17 families in Minnesota that are awaiting children. They've been to Haiti, they've seen these kids. And I do appreciate the front-line work that you and Secretary Clinton have done, and also your

granting of humanitarian parole, that I requested last week. I spent the weekend with some of these families, as they clutched these photos, and I promised them I would ask about, not their specific situations, but just what is happening, in terms of a safe haven? Just the details of how these kids are going to get to the United States, or get somewhere safe in Haiti, as they hear reports that the orphanages, you know, don't have enough water, don't have enough food, and just—the sooner we can get them over, the better.

Secretary NAPOLITANO. Yes, Senator Klobuchar, we are working very closely to get orphans out who need to get out, who are already qualified for adoption in the United States. And we will work closely with your office.

But, let me just pause a moment, and say, we have already removed a number of orphans, already, to the United States, and some more are coming. That being said—and our heart goes out to those families, families in other States, and, most importantly, the orphans themselves.

In a catastrophe the size of Haiti, the number—we have to now set up a process, beyond that for orphans already identified with adoptive parents, before other children are removed, because we are there, really, at the acquiescence of the Government of Haiti; they have to agree that this——

Senator KLOBUCHAR. I understand.

Secretary NAPOLITANO.—child can be removed, and should be, to another country for care. So, the State Department is working with Haiti on that. Secretary Clinton is on that. We met about this late last night. The Secretary of Health and Human Services is involved, because when a child is brought here from Haiti, normally there's a lot of medical and health attention that needs to be carried out before they can be——

Senator KLOBUCHAR. I understand.

Secretary NAPOLITANO.—delivered. And so——

Senator KLOBUCHAR. Just if—if I could just impress on you that—I realize some of this is in the hands of the Haitian government.

Secretary NAPOLITANO. Right.

Senator KLOBUCHAR. I want to say that your staff has been very helpful today. We've been——

Secretary NAPOLITANO. Good.

Senator KLOBUCHAR.—directly talking to them.

Secretary NAPOLITANO. Right.

Senator KLOBUCHAR. We feel that this—the adoptions we have are pretty far along in the process, and so we will continue to get the details. But, I just wanted to impress on you, one, to thank you for what you're doing, but, two, how important it is for these families.

I wanted to ask, as I look for solutions to all of this—as a former prosecutor, I know you this—I know you know this—it's very easy to, like, look at every detail, and you always think, later, "What could we have done differently?" And you can always find, when a crime occurs, the changes that need to be made. But, going forward, the full-body scanners; would that have prevented this, if he

had gone through a full-body scanner in Amsterdam or one of the other airports?

Secretary NAPOLITANO. There is no doubt, in my view, that the whole-body imaging, particularly in the current iteration of the technologies and the technologies we're now working on with DOE, would be a very clear improvement over any technology that was used in Schiphol on Christmas.

Senator KLOBUCHAR. OK.

And the timetable here, we're—I think, 450 new ones. We've got 2,100 airport lanes, I think I read, in our country; 2,500 international flights, that I'm sure you'll be dealing with tonight, coming in. The timetable of getting these out?

Secretary NAPOLITANO. At least 450, domestically, this year. We're obviously looking at how to accelerate that. And then, working internationally to see that they will employ that kind of technology—which, by itself, by the way—and I can't emphasize this enough—in and of itself, no one technology, no one process, no one intel agency is the silver bullet here. It's——

Senator KLOBUCHAR. Right.

Secretary NAPOLITANO.—layer, layer, layer, layer. It's good technology with behavior detection officers, with canines, with explosives detection equipment, with the right watch list, with the right names on it, and the right intel——

Senator KLOBUCHAR. Got it.

Secretary NAPOLITANO.—behind it. So, as you can see, even from this hearing, all of these things have a role to play. It's very layered, and needs to be a layered, process.

Senator KLOBUCHAR. OK. And one last question. On the watch list, something that I've been looking at, as a member of this committee for a while, it's my feeling that there are people that shouldn't be on it, that waste resources; the kid going to Disneyland, in Minnesota, and who got—continually got questioned, for years, from the time he was a baby—to people that should be on it, that aren't. Just how do we go about this, not only adding people that clearly—I know that's been a lot of the focus of the questions today—but also looking at Secure Flight, what's happening with that, what the implementation date is on that. And finally, working with our airlines. As you know, this was a Northwest Airlines flight, now owned by Delta. Northwest Airlines, originally based in Minnesota. I've talked to their—Richard Anderson, the CEO, at length. It was their employees and that brave—those brave passengers that were on the front line that stopped this from happening. So, they have a big interest in making this work in the future.

And I'd just encourage you to work with the industry, because in so many international airports, there is no TSA, so the airlines are still on the front line.

Secretary NAPOLITANO. Well—right. And the private carriers are part of the process, too. In fact, I've already met with them individually, at least U.S.-flag carriers—had several long conversations with CEO Anderson, among others. They are going to be part of this solution. Trust me. Secure Flight—should be basically implemented, domestically, by March of this year. There are two airlines

that may lag by another 30 to 60 days. But, basically, domestically, that's where we are.

Internationally, it will take longer, but we're looking, basically, at having it implemented—Secure Flight, internationally—by the end of 2010.

Senator KLOBUCHAR. Thank you very much.

The CHAIRMAN. Thank you Senator.

Senator LeMieux.

STATEMENT OF HON. GEORGE S. LEMIEUX, U.S. SENATOR FROM FLORIDA

Senator LEMIEUX. Thank you, Mr. Chairman.

I've not had the opportunity to interact and interface with you folks yet, so I appreciate that opportunity today.

And I know, Madam Secretary, you have to go.

So, let me just ask you a quick question before you have to take your leave for Spain.

I think it's the belief of the American people that 99.99 percent of the folks who are going through security in this country pose no threat. And a lot of folks come to me and say, "We really feel like we're being harassed when we go through TSA," whether it's the child that's getting patted down or the 85-year-old grandmother, who's being patted down. At the same time, we have these folks, like the Christmas Day bomber, who made it through security. Do we use—and if this isn't the right setting for it, I understand—are we using any kind of predictive modeling, to follow up on what Senator Lautenberg was talking about, such as what credit card companies do in their antifraud measures? Do we score people? I mean, we're not just taking data based upon information. I assume that we use the good intelligence, the people who are working in Homeland Security and other agencies, to look for potential threats, and use computer modeling to say, "This person is a threat."

Secretary NAPOLITANO. Senator, we do that. We also employ, as I've said, a number of things in domestic airports, such as behavior detection officers. So, that is underway, as well. But, we also employ random selection. And random selection is truly random, so that when the 85-year-old grandmother who—there must be an 85-year-old grandmother who has been pulled aside in every State in the Union, because I always hear about the 85-year-old——

Senator LEMIEUX. There are a lot——

Secretary NAPOLITANO.—grandmother——

Senator LEMIEUX.—in Florida.

[Laughter.]

Secretary NAPOLITANO. I'm from Arizona. I can appreciate that.

[Laughter.]

Secretary NAPOLITANO. But, in any event—but, truly random must mean truly random. And it's also random and differentiated between airports. So, we will not have the same process in place in every airport in the United States on any given day.

Senator LEMIEUX. Well, that makes sense to me. But, I hope—and you were talking about the travel for international folks in the future, this kind of clear travel concept—I would hope that, in the future, there is a way, through biometrics or other ways, for the

average American to be able to—not go through without any type of screening; that doesn't make any sense—but for us to focus on the people that we're concerned with the most, and put most of our energy toward them. That seems to make more sense to me.

Secretary NAPOLITANO. Senator, if I might, Secure Flight, which Senator Klobuchar was just referring—that will help a lot, because that will exchange data that will—that allows us to remove the false positives——

Senator LEMIEUX. Right.

Secretary NAPOLITANO.—from the system. Those sorts of things, as they get implemented—we're not talking about the needle in a haystack, in a way; it's about the needle among the needles. And it is not the easiest thing to do in advance. So, what we want to be able to do is, yes, get the false positives out of the system so we can focus where we need to focus. These sorts of things that are underway will help us with that.

Mr. LEITER. And, Senator, if I might add, and I can't go into depth in an open session, but we do use biometrics for a number of the levels of screening, both the visa process and entry into the country. That is a costly endeavor, to integrate that into all of the screening, and it also poses significant policy issues regarding the protections of privacy data and U.S. persons data. So, it's an area that I think will probably be coming back to committees like this, seeking assistance, either in terms of resources or legislation, to ensure that we can, in fact, use this biometric data effectively.

Senator LEMIEUX. And, Director, you said, a moment ago, that you are now putting these teams together who will be able to be responsible for trying to see different issues, and put the pieces together. I think the American people assume that that's happening now. I'm new to the Senate, and so I think I have fresh eyes to look at this. I think the American people assume that there are rooms of people around this country, working for the Federal Government in any one of these agencies, who are looking at all this data, analyzing it, and making reports and decisions to not let people on planes or come across borders or get visas. Is that correct?

Mr. LEITER. Senator, it is, except, at the same time that they were doing that, they also had to write intelligence and sort of analyze these things and send them up to policymakers. The purpose of this is to free them from those requirements so they can focus all of their time with sufficient numbers on these small bits of data, which, again, in combination, paint a very damning picture. But, when they come in individually, surrounded by thousands of other pieces of data, really don't stand up to the analyst.

Senator LEMIEUX. For both of you, is there one thing that we could do which would—and I know nothing would solve the problem completely; you're never going to be able to ensure safety 100 percent—but, is there one thing—is it just a full-body scan? Is there one thing that you think, "Boy, that would really make a large difference in making our country safe?" What's the first thing we should do?

Secretary NAPOLITANO. Senator, I think that one of the first, if not the first, things we should do is push out the advanced technology that we know exists, even as we recognize the next generation of technology is still on its way.

Mr. LEITER. Senator, my real answer is, there isn't one thing. There really is not one thing that would make a huge difference here. It is a combination of many little things.

I will say, if I could only have one thing to pick, it would be to ensure that we do get the international cooperation we need, especially with our European partners, of providing the data and doing the screening that we want them to provide and do. That, otherwise, leaves us with a significant gap, because we can't cover the entire world. We need their assistance to protect the country.

Senator LEMIEUX. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Senator Ensign, before I call on you—Secretary Napolitano, can you still get to Europe?

Secretary NAPOLITANO. I think Senator Ensign——

The CHAIRMAN. I wanted to test you——

Secretary NAPOLITANO.—is the last one here who hasn't had a chance to ask a question.

STATEMENT OF HON. JOHN ENSIGN, U.S. SENATOR FROM NEVADA

Senator ENSIGN. I have one——

Secretary NAPOLITANO. I'd be happy to stay.

Senator ENSIGN. I have one——

Secretary NAPOLITANO. Yes.

Senator ENSIGN. OK. Quick question that I'm going to ask all of you. You can start. This gets to ideology. Do you believe that there's an ideology of radical Islam that has anything to do—or that underlies the USS Cole attack, Hasan, the Christmas Day bomber, 9/11—do you think that this radical Islam that's out there in the world, that that underlies what's going on?

Secretary NAPOLITANO. Senator, there is no doubt that there is a terrorist ideology in this world that is operating, both internationally and some of it now homegrown, that is underlying the attacks we're seeing now——

Senator ENSIGN. That's associated——

Secretary NAPOLITANO.—some of the ones we've seen in the past.

Senator ENSIGN.—with radical Islam?

Secretary NAPOLITANO. That is associated—if you want to call it that, yes.

Senator ENSIGN. Well, I mean——

Secretary NAPOLITANO. Yes.

Senator ENSIGN. It is.

Mr. LEITER. Yes. And I don't think I should have my job if I said anything else.

Secretary NAPOLITANO. Yes. I mean, I think—absolutely.

Mr. HAMILTON. Yes.

Senator ENSIGN. Thank you. The reason I asked that is, there was actually a report out today on the Fort Hood incident. And in the 86 pages is—actually, John Lehman—a member of the 9/11 Commission—former Navy Secretary—talks about this. I'll quote him, and he says that there's a reluctance—not a single place, in the 86 pages talking about Hasan, does it mention anything to do with radical Islam. And what he says, and I'll quote him, he says,

"It shows you how deeply entrenched the values of political correctness have become. It's definitely getting worse, and is now so ingrained that people no longer smirk when it happens."

The reason I asked that—we had a hearing in the Homeland Security Committee, before the Christmas break, about the Fort Hood incident. And this question was asked about political correctness. Is it clouding our judgment? Are we afraid to ask the wrong questions?

This gets back to not religious profiling, not racial profiling, but terrorist profiling. If there is an ideology that is underlying what is happening here, we'd better recognize that, and we'd better call it what it is. We certainly didn't back away from Nazism as a political ideology. Well, if radical Islam is what is—they've called for this jihad against the West—against us, against American values—we'd better recognize that.

The reason I say that, even, you know, that every young military officer is required to read "The Art of War." Well, a big part of the art of war is knowing your enemy. Well, a big part of the enemy is their ideology; it's their motivation. And one of the reasons I ask that is because it seems to me that the Christmas Day bomber, which we know had ties, through this cleric, to Hasan, and the Fort Hood tragedy that went on, that it would have seemed to me that, after the Fort Hood incident—because that took place initially—that if the ideology was the thing that was driving it, we would focus a lot of our intel on the ideology with this guy's disseminating information to some of the people that he's communicating with.

And, Director Leiter, you mentioned something about First Amendment rights, and I wanted to give you the chance to clarify it. Abdulmutallab and the cleric, their communications—is that protected by First Amendment rights, as far as not getting on a No Fly List, when those conversations happened overseas?

Mr. LEITER. No, Senator. And I want to make clear that, prior to 12/25, we weren't—we didn't intercept any communications between Abdulmutallab and Anwar al-Awlaki, the cleric to which you're referring.

And my only point on the communication was, certainly people—you can imagine some conversations people could have which would be First Amendment and wouldn't justify watch-listing——

Senator ENSIGN. But——

Mr. LEITER.—or No Fly.

Senator ENSIGN.—I just wanted to make sure that if we had intercepted a conversation between the two of them overseas, even if it——

Mr. LEITER. Oh, absolutely.

Senator ENSIGN.—it would never be protected by First Amendment.

Mr. LEITER. Absolutely not, Senator.

Senator ENSIGN. OK. I just wanted to ask, because the way that you said it, it could have been misleading, and——

Mr. LEITER. I apologize.

Senator ENSIGN.—I wanted to give you——

Mr. LEITER. Senator, can I just add? There is no doubt in my mind—and we have done everything we can at NCTC to make

quite clear to the American people and to Members of Congress—that, undoubtedly, underlying the reign of violence that al-Qaeda has brought, it is inspired by a violent extremist Islamic ideology, period. That does not mean that Islam is violent. It does mean——

Senator ENSIGN. I agree.

Mr. LEITER.—that Islam is extremist.

Senator ENSIGN. I don't—no, I—listen, I totally agree; that's why I said, a radical form of Islam that exists in the world.

Mr. LEITER. OK. As Director of NCTC, I want to be as clear as possible that——

Senator ENSIGN. Yes, I agree with you. I agree with you and, you know, don't want to see discrimination against people just because they follow the Islamic faith.

The CHAIRMAN. Senator Ensign?

Senator ENSIGN. Yes.

The CHAIRMAN. In the—your time is up. It's just barely up, but Senator Cantwell has a question for Secretary Napolitano, who should have left 15 minutes ago, but is being generous. I want to give Senator Cantwell a chance, with your forbearance, to ask a question.

Senator ENSIGN. Absolutely.

Could I have 1 minute, right after she just asks this one quick——

The CHAIRMAN. You got it.

Senator ENSIGN.—question, just because I want to ask each one of them a——

The CHAIRMAN. You got it.

Senator ENSIGN.—just a yes-or-no question.

The CHAIRMAN. You got it.

Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman.

Do I have 5 minutes now? Or——

The CHAIRMAN. Yes.

Senator CANTWELL. Oh, OK. Thank you. Thank you, Mr. Chairman.

Secretary Napolitano or Director Leiter, did the U.S. counterterrorism agencies have any specific negative information about Mr. Abdulmutallab, prior to his father alerting the U.S. Embassy in Nigeria?

Secretary NAPOLITANO. Let me ask Director Leiter. I don't know whether we should answer all of that in open session.

Mr. LEITER. Senator, the—I would be happy to give you an answer to that in closed session.

Senator CANTWELL. Great. Hopefully, I'll see you later and I'll get that.

My understanding is, from news reports, that his name was placed on a British version of a watch list. Was that information shared with the U.S. Government or any—you know, if so, which agencies received that information and when was it received?

Mr. LEITER. It was not as—I believe it was not shared and he was denied a visa for nonterrorist reasons. In my conversations

with my British colleagues, they had no information involving his association with terrorism prior to the events of 12/25, or, I should say, no information different from what we had.

Senator CANTWELL. But, he was subsequently put on their equivalent watch list there, and so, if their—if you didn't hear from them, isn't there a—some sort of one-to-one correspondence between the British government and the United States——

Mr. LEITER. Senator, it is my understanding——

Senator CANTWELL.—watch lists?

Mr. LEITER. Senator, it is my understanding that he was denied a visa. He was not placed on their terrorist watch list. They—we do exchange information regarding terrorist watch lists; he was not on that watch list.

Senator CANTWELL. You do not believe that he—if an individual was placed on a watch list in Britain, they should be placed—that would be sufficient grounds to be on a watch list—the TIDE list?

Mr. LEITER. Oh, I think there's very good reason, if an individual is on the British's terrorist watch list, that he should also be placed on the American terrorist watch list. He was not on the British terrorist watch list.

Senator CANTWELL. OK.

And second, if we had—Secretary Napolitano, you mentioned cooperation. And I've been very active in the Visa Waiver Program, saying we should have more conditions on that program. And so, I know that the current State Department website says, "To be admitted to the Visa Waiver Program, a country must meet various security and other measurements required, such as enhanced law enforcement, security-related data-sharing, and members are also required to maintain high counterterrorism law enforcement, border control, and document security standards." So, that's the current level by which those 35 countries have to cooperate with us.

Now, do you think that we need to enhance that? Or do you think that is the power now to say to those individuals?

Secretary NAPOLITANO. I think what we need to do is make sure that the standards that have been set forth for Visa Waiver are enforced on a continuous and continual basis, and, like all of the standards that have been referred to throughout this afternoon's session, that we continually refresh them and make sure they match what we need to match to make sure that terrorists aren't allowed to travel around the globe.

Senator CANTWELL. So, you think that their—I mean, you mention going there and having this dialogue. My question is, Do we have enough, with that State Department language there, to require the cooperation on data-sharing that we need, or do we need to do more?

Secretary NAPOLITANO. Right now, using the U.K. as an example, we have very good cooperation on data-sharing. Whether there are new or additional types of data, or new or additional types of things that need to be done in this ever-changing environment, is something that we continually need to challenge ourselves with.

Senator CANTWELL. OK.

And then, the—I'm reading a *New York Times* article, which says that after Mr. Abdulmutallab's application to renew his student

visa was rejected, the Secretary said the suspect was then placed on a watch list.

Secretary NAPOLITANO. I don't know what article you're referring to.

Senator CANTWELL. I'm referring to *The New York Times,* December 29, 2009. So, maybe you could——

Secretary NAPOLITANO. You're going to have to help me out. I don't know what—the context—if you could——

Senator CANTWELL. It's about——

Secretary NAPOLITANO.—help me, please.

Senator CANTWELL.—Britain's rejected visa renewal for the suspect, and the fact that he was on it.

So, maybe we can find out what watch list he was on in the U.K. and whether that information could have been shared with the United States, or should have been shared with the United States. My question today was more about the policy ramifications of—if it wasn't, why shouldn't it be? Why shouldn't somebody on Britain's list be shared with this?

And I guess, my overall, you know, concern, having been a member of the Judiciary Committee in 2002, when we had a great discussion with the FBI after 9/11, and a lot of the questions and data-sharing information about why FBI agents in Arizona didn't share information with FBI agents in Minnesota, that the question is, How far have we come in 8 years on this data-gathering analytical analysis. I mean, we're spending billions of dollars in Iraq and Afghanistan. We should not be at a hearing today, saying we don't have enough analysts or that we don't know about cloud computing and that information across various databases can't be shared, that just because you misspelled somebody's name, information can't come up. All those are technology solutions that are in the market today, and so, that shouldn't be our barrier to this issue. And so, I hope that we will realize that the war on terrorism is an asymmetrical threat, and that asymmetrical threat means we have to be a very flat organization with sharing information, and that that needs to be very robust.

So, I hope we can resolve this question about the British watch list and whether that information will be shared.

Mr. LEITER. And, Senator, of I may, I fully agree with your underlying point about sharing with the British. In fact, I know Secretary Napolitano and I have both engaged with our British colleagues since to review those very issues, to ensure that this information is being shared fully, especially because we see so many links back through the U.K. through so many of our plots.

Senator CANTWELL. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cantwell.

Secretary Napolitano, I'm sort of embarrassed, because you need to go, and I don't know whether you're being polite——

Secretary NAPOLITANO. I think Senator Ensign wanted——

The CHAIRMAN.—and I——

Secretary NAPOLITANO.—to have one more question, and then I'm going to ask permission please, to leave.

The CHAIRMAN. Permission is granted. I mean, you know——

Secretary NAPOLITANO. Yes.

The CHAIRMAN. OK. So——

Senator Ensign.

Senator ENSIGN. Thank you.

You mentioned, before, about when Abdulmutallab came into this country, that it's a different policy, whether or not he's allowed into the country versus getting on an airplane. This is a question, going forward. Is that policy going to be changed? In other words, it doesn't make any sense to me that somebody would have to go through secondary screening to get into the country, but they didn't have to go through secondary screening to get on an airplane.

Secretary NAPOLITANO. Well, it's the difference between secondary screened—if there's information about being a threat to aviation, versus secondary screening because they may have had some other criminal indicator or some other bad behavior or what have you. So, it's the difference between, you know, those two things.

But—to your question, this isn't about labels. It's not about which list or what list; it's looking at the entirety of the problem and saying, "All right. Now, this guy—this individual was able to get on a plane. He was able to get on a plane bound for the United States, and get on a plane bound for the United States with PETN. That should not happen. What actions do we need to take to make sure that that doesn't happen again?" And that's how we're looking at it. Not——

Senator ENSIGN. Right. The only reason——

Secretary NAPOLITANO. I can go into all the complexities——

Senator ENSIGN. The only reason I——

Secretary NAPOLITANO.—it doesn't really——

Senator ENSIGN.—bring that up is, he probably wasn't suspected of some other kind of criminal activity, the reason he was going through secondary screening—it would be my guess—the reason he was going through secondary screening in Detroit, before he got into the country, after he got off the airplane. That type of a list, you would think, would—should keep him from getting on the airplane in the first place. In other words——

Secretary NAPOLITANO. Indeed. Indeed. And——

Senator ENSIGN. And that's——

Secretary NAPOLITANO.—we have——

Senator ENSIGN.—all I'm saying. I'm suggesting to you that you look at that as a policy change.

Secretary NAPOLITANO. Indeed. And, Senator, we have already made that change. If you are in a State Department database, and those words are associated with a name, we are now already pushing that forward in the international environment. I have a feeling that there will be other changes made as part of this review, as well.

Senator ENSIGN. Good.

Thank you for your indulgence, Mr. Chairman.

Secretary NAPOLITANO. Thank you.

Senator ENSIGN. Thank you for staying, very, very much.

And I have other questions for the panel that I'll submit for the record.

The CHAIRMAN. Thank you, Senator Ensign.

I might say, to all members—and this isn't the end of the hearing—thank you very much, Madam Secretary—that there's a 7-day period to submit any further questions.

VOICE. [Off-mike.]

The CHAIRMAN. Yes—oh, absolutely. But, I just wanted to make that plain now.

And so, Frank, you'd be up.

Senator LAUTENBERG. Yes, if I might, Mr. Chairman——

The CHAIRMAN. I mean, Senator Lautenberg.

Senator LAUTENBERG.—ask of—since Governor Kean and—called you "Lee." I can't call you "Mr. Hamilton." Lee, I have a question that I'd like your view on.

Security cameras are—seem to be an important—not "seem"—are an important part of the surveillance that's required to keep people from getting access to secure areas. And I wonder whether a—you might know, or if anyone knows, whether all airports have security checks.

Mr. Leiter, do you—would you know that?

Mr. LEITER. Senator, I apologize. I simply don't know if every——

Senator LAUTENBERG. OK. No—Lee, would you recommend that every airport that has commercial traffic have security cameras at critical access points?

Mr. HAMILTON. Yes, I think I would. But, security cameras raise a lot of questions about privacy. And how you do that, how you set those security cameras up, and who sees the images, makes a lot of difference. I think you have to be very alert to that.

So, I favor security cameras. I think they can be very careful. But, their use can certainly be abused.

Senator LAUTENBERG. Yes. I'm just talking about—with security checkpoints.

Mr. HAMILTON. Right.

Senator LAUTENBERG. That's so—you agree that——

Mr. HAMILTON. Yes.

Senator LAUTENBERG.—it's a valuable tool and we should have them.

Thanks, Mr. Chairman, you've been very indulgent, and I appreciate it.

Thanks, to both of you, for your endurance, as well as your answers.

The CHAIRMAN. Well, they're not finished yet.

Senator LAUTENBERG. Oh, I'm sorry. I didn't mean to preempt exit.

[Laughter.]

The CHAIRMAN. Senator LeMieux, was there any question you had?

Senator LEMIEUX. Just a couple of questions.

Director Leiter, after Abdulmutallab was taken off the plane at some point, he was Mirandized. Do you agree that he should be Mirandized and treated in that fashion?

Mr. LEITER. Senator, I—this is really a question that I have to defer to the Department of Justice. Although trained as a lawyer, exactly when——

Senator LEMIEUX. You're more than trained as a lawyer. I think you were the president of the Harvard Law Review and a clerk for

a Supreme Court Justice. And you're about as accomplished as a lawyer as there is.

Mr. LEITER. I'm starting to feel like maybe I should go back to that line of work, Senator.

[Laughter.]

Mr. LEITER. But, in all honesty, ultimately, the decision of when that should be done, or has to be done, clearly has to be within the ambit of the Department of Justice and the FBI.

I think what is equally clear is the utility of having interagency discussions prior to that, to inform that decision. So, again, the decision has to be one of the Attorney General, but that should be a decision informed by an interagency discussion, considering all of the Nation's national security priorities; homeland security and intelligence collection and the like.

Senator LEMIEUX. And you're the head of counterterrorism for the country. You're an advocate for trying to stop this terrorism before it starts. And certainly, I would think, in your role, you would want to make sure that someone like Abdulmutallab would be interviewed, and you could receive as much information as possible, to help you prevent another attack.

Mr. LEITER. Yes.

Senator LEMIEUX. And when someone is given their Miranda rights, the chance that they're going to give that information seems to be less likely.

Mr. LEITER. Senator, as a good lawyer and a former prosecutor, my answer is, it really is fact-specific. And I simply don't have the sufficient understanding of the facts on the ground as to when it was or was not appropriate to Mirandize him. I do think, again, that decision has to be informed by an interagency discussion, and I can tell you from having been a prosecutor, there's no shortage of times when you Mirandize someone and they keep talking.

Senator LEMIEUX. Sure. But, he's not an American citizen. He is a person who is fighting a war against our country, trying to blow up a plane over Detroit. He has none of the rights of an American citizen. Why does he get afforded the right of Miranda rights? Why should he?

Mr. LEITER. Senator, I really have to defer to the Department of Justice on their decision there. I simply have a different set of interests at that point. I do have a different set of interests, but that doesn't make the interests of the Department of Justice any less valid.

Senator LEMIEUX. I don't want to ask you to speak for them. But, in your role as the head of counterterrorism for the country, wouldn't you prefer that he be treated as an enemy combatant, and that he have the opportunity to be interrogated so that you could learn information and prevent future attacks?

Mr. LEITER. As the Director of NCTC, I absolutely have an interest in ensuring that intelligence is collected so it can be analyzed and put into action. I also do have an interest, although not the same interest as the Department of Justice, where it's, I think, even more overriding, of ensuring that basic laws, constitutional principles, are followed. I'm not suggesting either one of these paths would not have honored that. But, I do actually have an enormous interest, as the Director of NCTC, to make sure that

there is a level of trust, with the Congress and the American people, that any counterterrorism investigation is being pursued in a lawful, reasonable manner.

Senator LEMIEUX. Thank you.

Congressman Hamilton, it seems to me that we still don't know who's in charge of protecting the homeland. Obviously, the President of the United States is ultimately responsible, but we have an Attorney General, we have a Director of Intelligence, we have the head of the CIA, we have head of the FBI, we have Director Leiter. I mean, do we still need some kind of structural change in the U.S. Government so that one person is responsible and reports to the President as the ultimate person who is here to protect the country?

Mr. HAMILTON. Yes. You have the Intelligence Reform and Terrorism Prevention Act, and it's been very clear from the testimony here today that there is, at the very least, a good bit of ambiguity in that statute as to who has authority. That statute was very hard to pass, and it is not going to be amended quickly or soon. So, you're going to be living with it, and you're going to be—for a while; I don't know how long. And during that time, the ambiguities are still going to be there. So, the only person that can make it clear who has the authority to do what, is the President of the United States. And I believe that he has to make it very clear who has the authority within the intelligence community.

Now, I think it was the intent of the Congress to put that authority in the Director of National Intelligence. But, as you—if you read that statute, it is not crystal clear. So, I think there is a heavy burden, given the fact that you're operating under an ambiguous statute, that the President must say who has the authority on budget, on personnel, on coordination, on integration in the intelligence community. And I don't know who else can do it.

When you have ambiguity in a statute, it is an invitation to the bureaucracy to struggle, to fight, to protect their turf. And only the President can clear the deck.

Senator LEMIEUX. Thank you, Congressman.

Mr. LEITER. Senator, may I add, briefly? And I associate myself with all of The Very Honorable Lee Hamilton's comments. I think he's exactly right. But, I would add an additional layer of complexity here, because the issue to which he was speaking was really coordination of the intelligence community, and that intelligence community is just one bit of the larger national security counterterrorism effort, which obviously extends to DHS, to the Attorney General, as you've cited, the Secretary of Defense, the Secretary of State. So, to the extent that it might be a bridge too far right now to even significantly modify the Intelligence Reform and Terrorism Prevention Act with respect to the DNI's authorities and NCTC's authorities, I would simply add that an even broader reform, I think, starts to be a bridge much, much too far.

Senator LEMIEUX. I guess the challenge that we have is that, at some point, somebody has to be accountable. And when you know that you're the person in charge—and you've both had this experience—then you institute a different level of action and follow-up than if there is a collective group. And if one person knows that they're responsible for keeping the homeland safe, whether it's the

Secretary or the Attorney General or some other person, such as the Director of National Intelligence, the system is going to work differently. Right now it seems like it's collegial. And it didn't work. And we should be acting—and I know that you are—as if the plane blew up.

Mr. LEITER. Senator, I agree fully with what you just said. I think the President did make clear that the buck stops with him, ultimately. That's—but, also, in his tasking to the Director of NCTC, he made clear to give me the responsibility to ensure a system of follow-up on high—a prioritizing and follow-up of high-priority threats.

Now, consistent with the statutory language that created NCTC, I do not have the authority, nor am I seeking it, to direct the actions to follow up. But, at least we will establish a system whereby each of these threats, when we identify threats, can, in fact, be followed up through appropriate department or agency action, and the results of that follow-up are reported back to the National Security Council to ensure that they have the information they need to further direct action, as necessary.

Senator LEMIEUX. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Let me just actually ask one quick question and then turn to Lee Hamilton for a thought.

The—always the first question that the press asks is, "So, who's going to get fired?"

VOICE. Is what?

The CHAIRMAN. "Who's going to get fired?" In other words, there has got to be somebody who's accountable. Can't fire the President. And so, it's like it's the all-consuming answer to our problems. If somebody's fired, it means that somebody—that Farouk would have never gotten on an airplane, et cetera. I don't—I think the question of firing at a high level, if it places itself squarely in front of somebody because there has been a clear case of negligence, has to come before the President of the United States.

To make a—an absurd comparison, but the only one that I can think of right now, when I was Governor of West Virginia, the State still controlled liquor, had liquor stores. West Virginia has had its share of Governors who've done time in prison and things of this sort. This particular one didn't. However, our director of liquor took a vacation trip to Wyoming with a bunch of liquor lobbyists. Now, he's not a high person in government; he was a—you know, in the cabinet, so to speak. But, liquor and beer don't really make the first cut. I called him up in Wyoming and I fired him on the spot. And I never questioned my own honesty, but you off—you always have to worry about not just the people who are at the top, but the people who are down somewhere in the middle, who are making decisions, who are looking at—who are looking at some of the cable traffic and the interpretation, who are the analysts or whatever, and you get into this business of people who've been there for 20 or 25 years.

And I always compare it to HHS; you come in and you do—you do Medicare, and you come into the office every morning, somewhere out in Baltimore, and there are stacks of—big stack of paper

here, big stack of paper here, there's a big stack of paper here, big stack of paper here. And the question is, Do you just go from the top down? You come back the next day, and you do it. And after a number of years, you just wear out and you start to miss stuff.

And my question to you, Director Leiter, is, Is that on the minds—I mean, if you've got hundreds of thousands—and I think the number actually goes a lot higher than that—pieces of information coming in every day, you are overwhelmed with hearings, with pressure, with the terrifying nature of the modern world, and all of a sudden we're discussing Somalia and Djibouti and Yemen and Kenya, and they're not even in the Middle East. I don't think Yemen qualifies as that; that's Horn of Africa. So, that doesn't—that's not Iran, that's not Iraq, that's not Afghanistan. So, there's overwhelming obsession of the duties of the day, the responsibilities, what can get up to you.

I do think it's important that people in your position are able to look down—have a mechanism for being able to look down and fire the—find out who has gotten tired, who doesn't really want to come to work in an area where the Nation's citizens are at risk. And those folks, if there are—some of them who are removed quietly—I would say, without a lot of public attention—it will be understood throughout the entire intelligence community within 48 hours, maybe worldwide. I think that's important.

And I think what Senator LeMieux and what a lot of us—you know, we keep saying, "Somebody's accountable. Therefore, if it's not working, somebody ought to get fired." And sometimes, things don't rise to that easy an answer. Because, if you fire somebody who's way up here—and maybe that person should be fired, and that's up to the President—but then you've sort of taken the—you've sort of taken the pressure off of everybody else. And where a lot of the main work is going on is four or five levels down, but it's the crucial work. It's the crucial work. It's the selection of which piece of information took precedence over what, and they should be placed in this group or this group, or whatever.

Is this something which—is this—are you aware of this? I mean, I know you're aware of it; I've just talked about it, and you've been around a long time. But, I think that kind of thing is important.

Mr. LEITER. Senator, absolutely. And I hope—and I think he has—I think the President has had the same thoughts about his leadership, wondering if we've just been looking at paper, and not moving it as quickly. And I expect that he can ask that question. He should ask that question about me, as the Director of NCTC, decide if that's the case with me.

But, on—in terms of the workforce, it is certainly something we think about. And I'll tell you that I say something to every new class of people that come to NCTC. And I know you've met—you've come out and met many of our analysts, and you know most of them are 26, 27, 28. And I can tell you that the reaction to the events of Christmas Day has just been heartbreaking to many of them. Frankly, heartbreaking to me. I mean, it—we know that we should have done better. And it is traumatic, and we were—obviously dodged a bullet and very lucky that something more tragic did not occur. And it has been—caused soul-searching for many of us, myself included.

But, at every introduction to the new class of people coming to NCTC, as they rotate through from different agencies, I tell them that—at the entrance to our auditorium, there's a display that we put up on our fifth anniversary, just a month or two ago, which has the remnants of a flag that was recovered from the World Trade Center site, a piece of the Pentagon, and remnants of the steel—twisted steel from the World Trade Center. And I tell every one of them in those classes, "The day that you can no longer walk into this building and look at that display and say, 'I'm going to do everything I can to protect innocent people from getting killed by terrorists', is the day that you have to turn in your badge and go find something else to do."

And I think that this event will cause some people to have those thoughts, because the pace is so strenuous, the burnout is so high, the pressure is so high. But, my belief is, we fundamentally have the right set of people, that they've been walking in every day, they've been seeing that display, and they've been working as hard as humanly possible, in as cooperative a spirit as possible, to make sure events like Christmas Day don't happen again.

The CHAIRMAN. And I understand that, and I agree with it. You've left the judgment up to the individuals. And I'm saying, sometimes the judgment has to come from——

Mr. LEITER. Absolutely, Mr. Chairman. And to be clear, that is a judgment I——

Mr. HAMILTON. Mr. Chairman, let me just add that I'm certainly for accountability in government. And if a person clearly did not do their job, they ought to pay a penalty for that. The immediate problem is to correct the flaws that happened. This threat is ongoing; they're plotting, right now, how to get at us. And the urgent task—a prior task to accountability—is to correct the flaws that have been discussed here. That's the priority, from my point of view. Accountability, obviously important. But, correcting the flaw is more important.

The CHAIRMAN. Congressman——

Mr. HAMILTON. And incidentally, if I may go back a few years in history, the Hart-Rudman Commission, we made the observation that hiring and firing is a national security issue. I think it was, back then; I think it is, today. One of the really great weaknesses of our system is that managers like Director Leiter do not have the power to hire and to fire.

The CHAIRMAN. Well, that's pretty well put. And that goes on the agenda.

Congressman do you have, in closing, any thoughts that have occurred to you? I know you haven't been around very much, and don't have much experience, but——

Mr. HAMILTON. Well, I've learned a lot this afternoon, in listening to Director Leiter and Secretary Napolitano, and I've very much appreciated the opportunity to be with you.

The questions, I might say, from your Senators, have really been excellent and on the mark.

The only further comment I would make—and this has come up in the hearing, but not enough emphasis, from my standpoint—the fundamental problem—and I think that Director Leiter would agree with me here—is the analytical function. And if you want to

make sure this thing doesn't happen again, many things, perhaps, have to happen. But, by all odds, it seems to me, the most important thing that has to happen is, you have to strengthen this analytical capacity. When you're talking about connecting the dots, that's what you're really talking about.

We have the most remarkable collection ability, in producing all of this information, that any government or any entity could possibly have. But, analysis needs much, much more emphasis. You've got to have better-trained analysis, you've got to have—analysts—and more of them. And that would be one of my impressions from this hearing.

The second impression is that the analysts have to have the ability to follow up, to pursue a lead and to demand action against a potential threat.

Senator LEMIEUX. Mr. Chairman?

The CHAIRMAN. Yes?

Senator LEMIEUX. I just wanted to offer—is that better? Sorry. Broke the microphone.

You know, we have the finest computing people in the world, in this country, whether it's Google or other companies. I know folks in Florida who do unbelievable spinning of trillions of pieces of data for the private sector. I hope that you feel like you've got the freedom to reach out to the smartest minds in America to help you, because I know that they would. And I don't necessarily mean giving somebody a contract; that's one thing, and maybe you need to do that. But, just go out to these people, and have them come in and help you, because, you know, what Senator Cantwell was talking about with cloud computing and all the things that we've done—and I assume you have this. But, whatever else you need, you should go get.

Mr. LEITER. Senator. We absolutely have. We have, over several years, reached out to the private sector and the National Labs. We are doing so vigorously again now in response to this. And if you have particular companies or people that you think would be particularly useful, I am more than happy to speak with you and make sure we get those folks inside and see what our challenges are.

Senator LEMIEUX. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

And thank you all, the departed and the present. Thanks for your patience.

Thanks for you, in the audience, who have suffered, been through grief.

Thanks for those of you who have just simply come here to listen and to learn and to act out your citizenship.

This hearing is adjourned.

[Whereupon, at 5:22 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF THE AMERICAN CIVIL LIBERTIES UNION (MICHAEL W. MACLEOD-BALL, ACTING DIRECTOR, WASHINGTON LEGISLATIVE OFFICE AND CHRISTOPHER CALABRESE, LEGISLATIVE COUNSEL)

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee:

The American Civil Liberties Union (ACLU) has more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the Nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. In particular, throughout our history, we have been one of the Nation's pre-eminent advocates in support of privacy and equality. We write today to express our strong concern over the three substantive policy changes that are being considered in the wake of the attempted terror attack on Christmas Day: the wider deployment of whole body imaging (WBI) devices, the expanded use of terror watch lists and increased screening of individuals from fourteen so-called nations of interest. The ACLU believes that each of these technologies greatly infringe on civil liberties and face serious questions regarding its efficacy in protecting airline travelers.

The President has already identified a failure of intelligence as the chief cause of the inability to detect the attempted terror attack on Christmas Day. As such, the government's response must be directed to that end. These invasive and unjust airline security techniques represent a dangerous diversion of resources from the real problem. This diversion of resources promises serious harm to American's privacy and civil liberties while failing to deliver significant safety improvements.

I. Introduction

WBI uses millimeter wave or X-ray technology to produce graphic images of passengers' bodies, essentially taking a naked picture of air passengers as they pass through security checkpoints. This technology is currently deployed at 19 airports and the Department of Homeland Security (DHS) recently announced the roll out of 300 more machines by year end.[1] While initially described as a secondary screening mechanism, DHS is now stating that WBI will be used for primary screening of passengers.[2]

Another way of screening passengers is through terror watch lists. The terror watch lists are a series of lists of names of individuals suspected of planning or executing terrorist attacks. The master list is maintained by the Terrorist Screening Center (TSC) and contains more than one million names.[3] Subsets of this list include the No Fly list (barring individuals from air travel) and the Automatic Selectee list (requiring a secondary screening). The names on this list and the criteria for placement on these lists are secret.[4] There is no process allowing individuals to challenge their placement on a list or seek removal from a list.

Finally, individuals who were born in, are citizens of, or are traveling from fourteen nations will receive additional scrutiny under a policy announced by the U.S. Government after the attempted terror attack. As of January 19, 2010 these nations are Afghanistan, Algeria, Cuba, Iran, Lebanon, Libya, Iraq, Nigeria, Pakistan, Saudi Arabia, Somalia, Sudan, Syria and Yemen.

---

[1] Harriet Baskas, Air security: Protection at privacy's expense? Msnbc.com, January 14, 2010. *http://www.msnbc.msn.com/id/34846903/ns/travel-tips/*.

[2] Paul Giblin and Eric Lipton, New Airport X-Rays Scan Bodies, Not Just Bags, *New York Times,* February 24, 2007.

[3] *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Justice Department, Office of the Inspector General, Audit Report 09–25, May 2009, pg. 3. *http://www.justice.gov/oig/reports/FBI/a0925/final.pdf.*

[4] *Id.* at 70.

The ACLU believes that Congress should apply the following two principles in evaluating any airline security measure:

- *Efficacy.* New security technologies must be genuinely effective, rather than creating a false sense of security. The wisdom supporting this principle is obvious: funds to increase aviation security are limited, and any technique or technology must work and be substantially better than other alternatives to deserve some of the limited funds available. It therefore follows that before Congress invests in technologies or employs new screening methods, it must demand evidence and testing from neutral parties that these techniques have a likelihood of success.
- *Impact on Civil Liberties.* The degree to which a proposed measure invades privacy should be weighed in the evaluation of any technology. If there are multiple effective techniques for safeguarding air travel, the least intrusive technology or technique should always trump the more invasive technology.

II. Screening Techniques and Technologies Must Be Effective, or they Should Not be Utilized or Funded

The wider deployment of whole body imaging (WBI) devices, expanded use of terror watch lists and increased screening of individuals from fourteen so-called nations of interest each face significant questions regarding their efficacy in protecting air travelers and combating terrorism.

Whole Body Imaging

There are no magic solutions or technologies for protecting air travelers. Ben Wallace, a current member of the British parliament who advised a research team at *QinetiQ,* a manufacturer of body screening devices, has stated that their testing demonstrated that these screening devices would not have discovered a bomb of the type used on Christmas day, as they failed to detect low density materials like powders, liquids and thin plastics.[5] A current QinetiQ product manager admitted that even their newest body scan technology probably would not have detected the underwear bomb.[6] The British press has also reported that the British Department for Transport (DfT) and the British Home Office have already tested the scanners and were not convinced they would work comprehensively against terrorist threats to aviation.[7]

In addition we know that al Qaeda has already discovered a way to work around this technology. In September a suicide bomber stowed a full pound of high explosives and a detonator inside his rectum, and attempted to assassinate a Saudi prince by blowing himself up.[8] While the attack only slightly wounded the prince, it fully defeated an array of security measures including metal detectors and palace security. The bomber spent 30 hours in the close company of the prince's own secret service agents—all without anyone suspecting a thing. WBI devices—which do not penetrate the body—would not have detected this device.

The practical obstacles to effective deployment of body scanners are also considerable. In the United States alone, 43,000 TSA officers staff numerous security gates at over 450 airports and over 2 million passengers a day.[9] To avoid being an ineffective "Maginot line," these $170,000 machines will need to be put in place at all gates in all airports; otherwise a terrorist could just use an airport gate that does not have them. Scanner operators struggle constantly with boredom and inattention when tasked with the monotonous job of scanning thousands of harmless individuals when day after day, year after year, no terrorists come through their gate. In addition to the expense of buying, installing and maintaining these machines, additional personnel will have to be hired to run them (unless they are shifted from other security functions, which will degrade those functions).

The efficacy of WBI devices must be weighed against not only their impact on civil liberties (discussed further below) but also their impact on the U.S. ability to implement other security measures. Every dollar spent on these technologies is a dollar that is not spent on intelligence analysis or other law enforcement activity. The President has already acknowledged that it was deficiencies in those areas—not aviation screening—that allowed Umar Farouk Abdulmutallab to board an airplane.

---

[5] Jane Merrick, Are Planned Airport Scanners Just a Scam? *The Independent*, January 3, 2010.

[6] *Id.*

[7] *Id.*

[8] Sheila MacVicar , *Al Qaeda Bombers Learn from Drug Smugglers, CBSnews.com,* September 28, 2009.

[9] *http://www.tsa.gov/what_we_do/screening/security_checkpoints.shtm.*

Watch Lists

The events leading up to the attempted Christmas attack are a telling indictment of the entire watch list system. In spite of damning information, including the direct plea of Abdulmutallab's father, and other intelligence gathered about terrorist activity in Yemen, Abdulmutallab was not placed into the main Terrorist Screening Database. We believe that fact can be directly attributed to the bloated and overbroad nature of the list—now at more than a million names. [10] The size of the list creates numerous false positives, wastes resources and hides the real threats to aviation security. As we discuss below it also sweeps up many innocent Americans—falsely labeling them terrorists and providing them with no mechanism for removing themselves from the list.

These problems are not hypothetical. They have real consequences for law enforcement and safety. An April 2009 report from the Virginia Fusion Center states

> According to 2008 Terrorism Screening Center ground encounter data, al-Qa'ida was one of the three most frequently encountered groups in Virginia. In 2007, at least 414 encounters between suspected al-Qa'ida members and law enforcement or government officials were documented in the Commonwealth. Although the vast majority of encounters involved automatic database checks for air travel, a number of subjects were encountered by law enforcement officers.[11]

Every time a law enforcement officer encounters someone on the terrorist watch list (as determined by a check of the National Crime Information Center (NCIC) database) they contact the TSC. So in essence Virginia law enforcement is reporting that there are more than 400 al Qaeda terrorists in Virginia in a given year. This is difficult to believe.[12] In reality most, if not all, of these stops are false positives, mistakes regarding individuals who should not be on the list. These false positives can only distract law enforcement from real dangers.

A 2009 report by the Department of Justice Inspector General found similarly troubling results. From the summary:

> We found that the FBI failed to nominate many subjects in the terrorism investigations that we sampled, did not nominate many others in a timely fashion, and did not update or remove watchlist records as required. Specifically, in 32 of the 216 (15 percent) terrorism investigations we reviewed, 35 subjects of these investigations were not nominated to the consolidated terrorist watchlist, contrary to FBI policy. We also found that 78 percent of the initial watchlist nominations we reviewed were not processed in established FBI time frames.
>
> Additionally, in 67 percent of the cases that we reviewed in which a watchlist record modification was necessary, we determined that the FBI case agent primarily assigned to the case failed to modify the watchlist record when new identifying information was obtained during the course of the investigation, as required by FBI policy. Further, in 8 percent of the closed cases we reviewed, we found that the FBI failed to remove subjects from the watchlist as required by FBI policy. Finally, in 72 percent of the closed cases reviewed, the FBI failed to remove the subject in a timely manner.[13]

This is only the latest in a long string of government reports describing the failure of the terror watch lists.[14] In order to be an effective tool against terrorism these

---

[10] DOJ OIG Audit Report 09–25, pg 3. *http://www.justice.gov/oig/reports/FBI/a0925/final.pdf.*

[11] Virginia Fusion Center, *2009 Virginia Terrorism Threat Assessment*, March 2009, pg 27.

[12] The report does not state that any of these individuals were arrested.

[13] DOJ OIG Audit Report 09–25, pg iv–v. *http://www.justice.gov/oig/reports/FBI/a0925/final.pdf*

[14] *Review of the Terrorist Screening Center* (Redacted for Public Release), Justice Department, Office of the Inspector General, Audit Report 05–27, June 2005; *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program* (Redacted for Public Release), Justice Department, Office of the Inspector General, Audit Report 05–34, August 2005; *Follow-Up Audit of the Terrorist Screening Center* (Redacted for Public Release), Justice Department, Office of the Inspector General, Audit Report 07–41, September 2007; *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Justice Department, Office of the Inspector General, Audit Report 09–25, May 2009; *DHS Challenges in Consolidating Terrorist Watch List Information,* Department of Homeland Security, Office of Inspector General, OIG–04–31, August 2004; *Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing,* GAO Report to Congressional Requesters, GAO–03–322, April 2003; *Congressional Memo Regarding Technical Flaws in the Terrorist Watch List,* House Committee on Science and Technology, August 2008.

lists must shrink dramatically with names limited to only those for whom there is credible evidence of terrorist ties or activities.

Aviation Screening on the Basis of Nationality

Numerous security experts have already decried the use of race and national origin as an aviation screening technique.

Noted security expert Bruce Schneier stated recently:

> [A]utomatic profiling based on name, nationality, method of ticket purchase, and so on . . . makes us all less safe. The problem with automatic profiling is that it doesn't work.
>
> Terrorists can figure out how to beat any profiling system.
>
> Terrorists don't fit a profile and cannot be plucked out of crowds by computers. They're European, Asian, African, Hispanic, and Middle Eastern, male and female, young and old. Umar Farouk Abdul Mutallab was Nigerian. Richard Reid, the shoe bomber, was British with a Jamaican father. Germaine Lindsay, one of the 7/7 London bombers, was Afro-Caribbean. Dirty bomb suspect Jose Padilla was Hispanic-American. The 2002 Bali terrorists were Indonesian. Timothy McVeigh was a white American. So was the Unabomber. The Chechen terrorists who blew up two Russian planes in 2004 were female. Palestinian terrorists routinely recruit "clean" suicide bombers, and have used unsuspecting Westerners as bomb carriers.
>
> Without an accurate profile, the system can be statistically demonstrated to be no more effective than random screening.
>
> And, even worse, profiling creates two paths through security: one with less scrutiny and one with more. And once you do that, you invite the terrorists to take the path with less scrutiny. That is, a terrorist group can safely probe any profiling system and figure out how to beat the profile. And once they do, they're going to get through airport security with the minimum level of screening every time.[15]

Schneier is not alone in this assessment. Philip Baum is the managing director of an aviation security company:

> Effective profiling is based on the analysis of the appearance and behavior of a passenger and an inspection of the traveler's itinerary and passport; it does not and should not be based on race, religion, nationality or color of skin. . . .
>
> Equally, the decision to focus on nationals of certain countries is flawed and backward. Perhaps I, as a British citizen, should be screened more intensely given that Richard Reid (a.k.a. "the Shoebomber") was a U.K. passport holder and my guess is there are plenty more radicalized Muslims carrying similar passports. Has America forgotten the likes of Timothy McVeigh? It only takes one bad egg and they exist in every country of the world.[16]

Former Israeli airport security director Rafi Ron:

> My experience at Ben Gurion Airport in Tel Aviv has led me to the conclusion that racial profiling is not effective. The major attacks at Ben Gurion Airport were carried out by Japanese terrorists in 1972 and Germans in the 1980s. [They] did not belong to any expected ethnic group. Richard Reid [known as the shoe bomber] did not fit a racial profile. Professionally as well as legally, I oppose the idea of racial profiling.[17]

This should be the end of the discussions. Policies that don't work have no place in aviation security. When they are actively harmful—wasting resources and making us less safe—they should be stopped as quickly as possible.

III. The Impact on Privacy and Civil Liberties Must be Weighed in Any Assessment of Aviation Security Techniques

Each of the three aviation security provisions discussed in these remarks represents a direct attack on fundamental American values. As such they raise serious civil liberties concerns.

---

[15] *http://roomfordebate.blogs.nytimes.com/2010/01/04/will-profiling-make-a-difference/.*

[16] *Id.*

[17] Katherine Walsh, *Behavior Pattern Recognition and Why Racial Profiling Doesn't Work,* CSO Online, (Feb. 1, 2006), at: *http://www.csoonline.com/article/220787/Behavior__Pattern__Recognition__and__Why__Racial__Profiling__Doesn__t__Work.*

Whole Body Imaging

WBI technology involves a striking and direct invasion of privacy. It produces strikingly graphic images of passengers' bodies, essentially taking a naked picture of air passengers as they pass through security checkpoints. It is a virtual strip search that reveals not only our private body parts, but also intimate medical details like colostomy bags. Many people who wear adult diapers feel they will be humiliated. That degree of examination amounts to a significant assault on the essential dignity of passengers. Some people do not mind being viewed naked but many do and they have a right to have their integrity honored.

This technology should not be used as part of a routine screening procedure, but only when the facts and circumstances suggest that it is the most effective method for a particular individual. And such technology may be used in place of an intrusive search, such as a strip search—when there is reasonable suspicion sufficient to support such a search.

TSA is also touting privacy safeguards including blurring of faces, the non-retention of images, and the viewing of images only by screeners in a separate room. Scanners with such protections are certainly better than those without; however, we are still skeptical of their suggested safeguards such as obscuring faces and not retaining images.

Obscuring faces is just a software fix that can be undone as easily as it is applied. And obscuring faces does not hide the fact that rest of the body will be vividly displayed. A policy of not retaining images is a protection that would certainly be a vital step for such a potentially invasive system, but it is hard to see how this would be achieved in practice. TSA would almost certainly have to create exceptions—for collecting evidence of a crime or for evaluation of the system (such as in the event of another attack) for example—and it is a short step from there to these images appearing on the Internet.

Intrusive technologies are often introduced very gingerly with all manner of safeguards and protections, but once the technology is accepted the protections are stripped away. There are substantial reasons for skepticism regarding TSA promised protections for WBI devices. In order for these protections to be credible Congress must enshrine them in law.

Finally, the TSA should invest in developing other detection systems that are less invasive, less costly and less damaging to privacy. For example, "trace portal detection" particle detectors hold the promise of detecting explosives while posing little challenge to flyers' privacy. A 2002 Homeland Security report urged the "immediate deployment" of relatively inexpensive explosive trace detectors in European airports, as did a 2005 report to Congress, yet according to a 2006 Associated Press article, these efforts "were frustrated inside Homeland Security by 'bureaucratic games, a lack of strategic goals and months-long delays in distributing money Congress had already approved."[18] Bureaucratic delay and mismanagement should not be allowed to thwart the development of more effective explosive detection technologies that do not have the negative privacy impact of WBI devices.

Watch Lists

The creation of terrorist watch lists—literally labeling individuals as a terrorist—has enormous civil liberties impact. It means ongoing and repetitive harassment at all airports—foreign and domestic, constant extra screening, searches and invasive questions. For the many innocent individuals on the lists this is humiliating and infuriating.

For some it is worse. Individuals on the No Fly List are denied a fundamental right, the right to travel and move about the country freely. Others are threatened with the loss of their job. Erich Sherfen, commercial airline pilot and Gulf War veteran, has been threatened with termination from his job as a pilot because his name appears on a government watch list, which prevents him from entering the cockpit.[19] Sherfen is not the only innocent person placed on a terror watch list. Others individual who are either on a list or mistaken for those on the list include a former Assistant Attorney General, many individuals with the name Robert Johnson, the late Senator Edward Kennedy and even Nelson Mandela.[20]

---

[18] John Solomon, Bureaucracy Impedes Bomb Detection Work, *Washington Post*, Aug. 12, 2006, at: *http://www.washingtonpost.com/wp-dyn/content/article/2006/08/12/AR2006081200269.html.*

[19] Jeanne Meserve, *Name on government watch list threatens pilot's career*, CNN.com, August 22, 2008, *http://www.cnn.com/2008/US/08/22/pilot.watch.list/index.html?iref=newssearch.*

[20] && For details on these individuals and many other please see: *http://www.aclu.org/technology-and-liberty/unlikelysuspects.*

The most recent case—revealed just last week—is that of Mikey Hicks, an 8 year old boy who has been on the selectee list seemingly since birth. According to Hicks' family their travel tribulations that began when Mikey was an infant. When he was 2 years old, the kid was patted down at airport security. He's now, by all accounts, an unassuming bespectacled Boy Scout who has been stopped every time he flies with his family.[21]

In addition, to stops at the airport watch list information is also placed in the National Criminal Information Center database. That means law enforcement routinely run names against the watch lists for matters as mundane as traffic stops. It's clear that innocent individuals may be harassed even if they don't attempt to fly.

Nor is there any due process for removing individuals from the list—there is simply no process for challenging the government's contention that you are a terrorist. Even people who are mistaken for those on the list face challenges. A September 2009 report by the Inspector General of the Department of Homeland Security found that the process for clearing innocent travelers from the list is a complete mess.[22]

In light of the significant and ongoing harm to innocent Americans as well as the harm to our national security caused by the diversion of security resources these watch lists must be substantial reduced in size and fundamental due process protections imposed. Innocent travelers must be able to remove themselves from the list both for their sake and the sake of national security.

Aviation Screening on the Basis of Nationality

This history of the civil rights movement in the 20th and 21st Century is a long, compelling rejection of the idea that individuals should be treated differently on the basis of their race or nation of origin. Because of that, the administration's decision to subject the citizens of fourteen nations flying to the United States to intensified screening is deeply troubling. Longstanding constitutional principles require that no administrative searches, either by technique or technology, be applied in a discriminatory matter. The ACLU opposes the categorical use of profiles based on race, religion, ethnicity, or country of origin. This practice is nothing less than racial profiling. Such profiling is ineffective and counter to American values.

But the harm that profiling on the basis of national origin does to civil liberties is not an abstraction—it also has direct impact on American security interests. These harmful policies have a direct impact on the Muslim and Arab communities. The Senate Homeland Security and Government Affairs committee has heard testimony from several witnesses who cited the growth of Islamophobia and the polarization of the Muslim community as risk factors that could raise the potential for extremist violence.[23] Unfairly focusing suspicion on a vulnerable community tends to create the very alienation and danger that we need to avoid.

Indeed a recent United Kingdom analysis based on hundreds of case studies of individuals involved in terrorism reportedly identified "facing marginalization and racism" as a key vulnerability that could tend to make an individual receptive to extremist ideology.[24] The conclusion supporting tolerance of diversity and protection of civil liberties was echoed in a National Counterterrorism Center (NCTC) paper published in August 2008. In exploring why there was less violent homegrown extremism in the U.S. than the U.K., the authors cited the diversity of American communities and the greater protection of civil rights as key factors.[25]

At the January 7, 2009 White House briefing regarding the security failures surrounding the Christmas attack, DHS Secretary Janet Napolitano raised a question about "counterradicalization."[26] She asked, "How do we communicate better Amer-

---

[21] Lizette Alvarez, Meet Mikey, 8: U.S. Has Him on Watch List, *New York Times*, January 13, 2010.

[22] Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program, Department of Homeland Security, Office of the Inspector General OIG 09–10, September 2009. *http://www.dhs.gov/xoig/assets/mgmtrpts/OIG–09–103r Sep09.pdf.*

[23] *See for example,* Hearing of the Senate Homeland Security and Governmental Affairs Committee, *Violent Islamist Extremism: The European Experience,* (June 27, 2007), particularly the testimony of Lidewijde Ongering and Marc Sageman, available at: *http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=9c8ef805–75c8–48c2–810dd778af31cca6.*

[24] Alan Travis, "MI5 Report Challenges Views on Terrorism in Britain," The Guardian, (August 20, 2008) at: *http://www.guardian.co.uk/uk/2008/aug/20/uksecurity.terrorism1* and; Alan Travis, "The Making of an Extremist," *The Guardian* (Aug. 20, 2008) at*: http://www.guardian.co.uk/uk/2008/aug/20/uksecurity.terrorism.*

[25] National Counterterrorism Center Conference Report, Toward a Domestic Counterradicalization Strategy, (August 2008).

[26] Briefing by Homeland Security Secretary Napolitano, Assistant to the President for Counterterrorism and Homeland Security Brennan, and Press Secretary Gibbs, 1/7/10, at:

ican values and so forth, in this country but also around the globe?" Of course the Secretary should know American values are communicated through U.S. Government policies, which is why adopting openly discriminatory policies can be so damaging and counterproductive to our national interests.

IV. Conclusion

Ultimately security is never absolute and never will be. It is not wise security policy to spend heavily to protect against one particular type of plot, when the number of terrorist ideas that can be hatched—not only against airlines, but also against other targets—is limitless. The President has identified a failure "connect the dots" by intelligence analysts as the main reason that Umar Farouk Abdulmutallab was able to board a flight to the U.S.[27] We must not lose sight of that reality. Limited security dollars should be invested where they will do the most good and have the best chance of thwarting attacks. That means investing them in developing competent intelligence and law enforcement agencies that will identify specific individuals who represent a danger to air travel and arrest them or deny them a visa.

Invasive screening mechanisms, enlarging already bloated watch lists, targeting on the basis of national origin—none of these approaches go to the heart of what went wrong on Christmas day. Instead they are a dangerous sideshow—one that harms our civil liberties and ultimately makes us less safe.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO HON. MICHAEL E. LEITER

Question 1. I understand there is a complex system the intelligence services and the NCTC use to adjudicate whether or not an individual is placed on a watch list. Does everyone involved in the system, including State Consular officers in country, understand the information that must be supplied in order to add an individual to the No Fly list?

[This answer has been designated "For Official Business Only" and has been provided to Senator Warner.]

Question 2. Please describe the data mining tools available to NCTC analysts. What commercial search technology is being leveraged? Does NCTC work with companies such as Google to improve its search technologies and database managing?

[This answer has been designated "Classified" and has been provided to Senator Warner.]

Question 3. How many intelligence databases relating to terrorism exist in the U.S. Government? How many are fully integrated?

[This answer has been designated "Classified" and has been provided to Senator Warner.]

Question 4. How are critical pieces of intelligence regarding threats to the homeland identified? Is it solely dependent on human input/action?

[This answer has been designated "For Official Business Only" and has been provided to Senator Warner.]

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK BEGICH TO HON. MICHAEL E. LEITER

Question 1. The suspect in this case had a valid visa to travel the U.S. Why wasn't Mr. Abdulmutallab's visa revoked, and what are the criteria by which a visa is revoked?

This answer was forwarded to the Department of State as requested by NCTC and is answered below:

Answer from the Department of State. In accordance with procedures in place at the time, upon receiving the information provided, the consular officer forwarded a Visas Viper report to the National Counterterrorism Center (NCTC) for a determination regarding whether the information was sufficient to watchlist Mr.Abdulmutallab. At that point the intelligence and law enforcement communities determine if there is sufficient information to list him in the Terrorist Screening

---

http://www.whitehouse.gov/the-pressoffice/briefing-homeland-security-secretary-napolitano-assistant-president-counterterroris.

[27] Jake Tapper and Sunlen Miller, *Obama: Intelligence Community Failed to "Connect the Dots" in a "Potentially Disastrous Way"*, ABCNews.com, January 05, 2010. *http://blogs.abcnews.com/politicalpunch/2010/01/obamaintelligence-community-failed-to-connect-the-dots-in-a-potentially-disastrous-way.html.*

Database. That action would have triggered notification to State. The State Department as a matter of standard procedure would have prudentially revoked the visa absent any law enforcement or intelligence community interest in not doing so, or some other valid reason (such as waiver of ineligibility approved by the Department of Homeland Security). In this case, as NCTC did not forward Abdulmutallab's name and biodata to the Terrorist Screening Center, and as there was no indication from the information provided to the USG in Abuja that he posed any immediate threat to the United States, there was no basis for a prudential revocation of his visa.

In this case, information in the Visas Viper report on Mr. Abdulmutallab did not meet the minimum derogatory standard to watchlist. The Department's procedures now require that Visas Viper cables contain information regarding an applicant's visa status, and it is our policy to revoke any visa held by the subject of a Visas Viper cable, absent any law enforcement or intelligence community interest in not doing so, or some other valid reason (such as waiver of ineligibility approved by the Department of Homeland Security).

Question 2. What are the criteria by which a visa is revoked?

Answer from the Department of State. Visas may be revoked by a consular officer abroad or by the Department. A consular officer abroad may revoke a visa only when he or she has made an actual finding that the holder is ineligible for a visa. When a consular officer abroad wishes to revoke a visa in a category that requires a Security Advisory Opinion (SAO),* the officer must first seek the SAO but may request it be expedited. The consular officer may also request that the Department revoke the visa.

The Department has broad discretion and may revoke a visa even if a ground of ineligibility is merely suspected. The normal process is for the case to undergo an interagency review first although the Department sometimes revokes visas without consulting other U.S. Government agencies. However, interagency coordination offers many benefits, including giving U.S. Government agencies with law enforcement or intelligence equities in the case the opportunity to provide input into the Department of State's decision to revoke or not.

Question 3. Are there any information-sharing barriers that contributed to the failure to place Mr. Abdulmutallab on the selectee or No Fly watch list?

[This answer has been designated "For Official Business Only" and has been provided to Senator Begich.]

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO HON. MICHAEL E. LEITER

Question 1. While the preliminary review of this incident suggests a failure to connect-the-dots, rather than a failure to share information, your analysts were apparently deprived of at least some information: The State Department cable—perhaps due to a simple misspelling—failed to indicate that this would-be terrorist held a U.S. visa; and press reports indicate that a contemporaneous report authored by the CIA was also not shared in a timely manner. *The Washington Post* reported on January 12 that "lack of information about Abdulmutallab's open visa affected the NCTC's determination of the threat he presented and thus the list he was put on." Do you agree? If your analysts had had the visa information or the CIA report, do you think they would have recommended watch-listing for this subject?

Answer. A classified response was submitted to the Senate Commerce Committee.

Question 2. You testified that, in recent years, the watchlisting community has been pressured to shrink the size of the No Fly and Selectee Lists. In the Department of Homeland Security Appropriations Act of 2008 (Public Law 110–161, Division E, Title II), however, Congress expressed its concern about the fact that the full TSDB was not being used for airline passenger screening by requiring the Assistant Secretary of Homeland Security (Transportation Security Administration) to certify "that no significant security risks are raised by screening airline passenger names only against a subset of the full terrorist watch list." Would you agree that, notwithstanding calls to improve the screening process to minimize false-positive matches, Congress has applied pressure to use the full TSDB for airline passenger screening?

Answer. A classified response was submitted to the Senate Commerce Committee.

---

*The Security Advisory Opinion is the mechanism used by the Department of State to provide consular officers advice and background information to adjudicate visa applications abroad in cases of security or foreign policy interest.

Question 3. The media has reported that, on November 13, 2009, a Somali man was stopped in Mogadishu attempting to board a commercial air carrier flight while carrying powdered chemicals, liquid, and a syringe that could have been used as an explosive device. In addition to the Somali incident, news accounts state that investigators "are hoping to compare the remnants of a similar explosive device used in an August attempt to kill a senior Saudi government official to determine whether it employed the same technology and possibly was constructed by the same bombmaker" as Mr. Abdulmutallab's device. (See Karen DeYoung & Michael A. Fletcher, *The Washington Post*, "Obama: Security Agencies Failed," January 6, 2010.) Moreover, on January 15, 2010, the press reported that Al Qaeda in the Arabian Peninsula may be currently planning more attacks on the U.S. (Eric Lipton, *The New York Times*, "Possibility of Plots Prompts More Checks for Explosives at Airports," January 15, 2010.) Given NCTC's role as "the primary organization in the U.S. Government for analyzing and integrating all intelligence possessed or acquired by the USG pertaining to [international] terrorism and counterterrorism" (Public Law 108–458), do you assess that these incidents are connected? Do you believe Mr. Abdulmutallab's attempted attack was part of a larger conspiracy or series of planned attacks?

Answer. A classified response was submitted to the Senate Commerce Committee.

Question 4. Yemeni authorities have reportedly acknowledged that Mr. Abdulmutallab met with radical Yemeni cleric Anwar at Awlaki last fall in Yemen. (See, *e.g.,* Haley Sweetland Edwards, the *Los Angeles Times*, "Yemen's Role Minimized," January 8, 2010.) At the hearing, you testified that intelligence about the Yemeni cleric and his associates had been scrubbed based on his association with Major Nidal M. Hasan, who is charged with killing 13 people at Fort Hood, Texas, in November 2009. In response to a question from Senator Ensign, however, you stated that no communications between the cleric and Mr. Abdulmutallab had been intercepted before December 25, 2009. Please describe, in a classified response if necessary, what, if any, intelligence about the connection between Mr. Abdulmutallab and Anwar al Awlaki was known before December 25, 2009.

Answer. A classified response was submitted to the Senate Commerce Committee.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. OLYMPIA J. SNOWE TO HON. MICHAEL E. LEITER

Question 1. The findings of the Administration's report released January 7, 2010, reviewing the intelligence failures leading up to Christmas Day, 2009, concluded "the information that was available to analysts, as is usually the case, was fragmented and embedded in a large volume of other data," and that both "NCTC and CIA personnel who are responsible for watch-listing did not search all available databases to uncover additional derogatory information that could have been correlated with Mr. Abdulmutallab." It is my understanding that most intelligence analysis is currently a process of manual searches of various databases.

It strikes me that this could easily reoccur, based on Director Leiter's testimony concerning the vast volume of data processed by the NCTC on a daily, if not hourly, basis. The Administration's review makes clear that the current intelligence-sorting processes today could be improved by utilizing technology that can be programmed to differentiate among specific types of threats, assign roles and responsibilities to each, and manage the response and escalation procedures, including the follow-up on such threats. Could this potential gap be remedied with automation?

Is the Department or the NCTC actively developing, or seeking, technology that can process such large volumes of data effectively, not missing intelligence-gathering opportunities, and if so, when will such technology be operational?

Answer. The NCTC submitted a classified response to the Senate Commerce Committee.

Question 2. Although our security and intelligence networks constantly are working to keep America safe, and their efforts have thwarted numerous terrorist attempts, it is evident that the existing workforce is spread thinly in many areas, and could face an even greater burden if heightened security measures are put in place. While I believe personnel increases would go a long way toward minimizing the risks we now face, I believe in some cases technology could reduce human errors and the failure to consider pertinent and currently inaccessible data or pass it on to other relevant parties. Do you believe the Department of Homeland Security and the Counter-Terrorism Center has sufficient resources to secure the latest technologies that would allow us to close these gaps?

Answer. Since the events of 12/25, NCTC has worked closely with the ODNI and the White House to address resource shortfalls related to both technology and per-

sonnel. Because the ODNI is seeking to determine how to optimize technological solutions across the IC, no final determination has been made as to what solution, or solutions, will be pursued for the Community. However, in the interim, the ODNI and White House have submitted, as part of the Overseas Contingency Operations request for FY 2010 and FY 2011, a robust program for NCTC to address our most pressing issues and to lay the ground work for addressing the findings of the ODNI directed studies. Should these studies indicate that additional requirements are necessary; the results will be the subject of further discussions with the ODNI and White House, as part of the FY 2012 program build.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO HON. JANET NAPOLITANO

Question 1. Has the Department of Homeland Security (DHS) given appropriate consideration to tightening the standards by which they certify security at foreign airports or increasing its oversight of security compliance at foreign airports? How often does DHS or TSA conduct audits of foreign airports? What is the biggest challenge that the U.S. security system confronts when working in the international environment?

Answer. As required by 49 U.S.C. § 114 (f)(14), the Transportation Security Administration (TSA) continues to work with the International Civil Aviation Organization (ICAO) and appropriate authorities of foreign governments to address security concerns and standards for passenger flights by international air carriers.

Under 49 U.S.C. § 44907, TSA is charged with assessing all foreign airports from which flights operate to the United States and those at which U.S. air carriers operate (regardless of the destination). TSA has a cadre of Security Specialists who visit the nearly 300 airports at intervals between one and 3 years. The frequency of the visits is based on risk analysis of current threat, documented vulnerabilities, and flight data. More frequent assessments are conducted if circumstances warrant, including previous deficiencies requiring follow-up visits, recent threat information, start-up service requests, and infrastructure changes at a particular foreign airport (*e.g.,* Haiti earthquake).

As signatories to the Convention on International Civil Aviation of 1944 (Chicago Convention), all Contracting States are required to provide for the security of their airports serving international civil aviation and the security screening of passengers and property prior to boarding an aircraft engaged in international civil aviation operations, in accordance with the Standards of Annex 17 to the Chicago Convention as established by ICAO. ICAO is the United Nations' specialized agency that oversees international civil aviation safety and security matters. ICAO's Universal Security Audit Program (USAP) oversees and monitors each Contracting State's implementation of and compliance with the international security standards ICAO has established. Under the USAP's current framework, the audit results are highly confidential. TSA has been working through ICAO's Aviation Security Panel to enhance the USAP's effectiveness and oversight capabilities and to increase the transparency of the USAP audit results among Contracting States. TSA fully supports the ICAO USAP, and routinely provides technical experts to serve on USAP audit teams.

As a result of these international obligations, nearly every Contracting State to ICAO has established its own national legislation governing civil aviation security and its airports serving international civil aviation in its territory and under its jurisdiction. Through TSA's Foreign Airport Assessment Program, TSA works closely with its foreign government counterparts to ensure these international standards are effectively implemented at all foreign airports with service to the United States or that are otherwise served by U.S. air carriers. Moreover, TSA works with these partners to ensure that special enhanced security measures for U.S. air carriers and all flights to the United States are also implemented, to the extent these foreign government authorities are responsible for carrying out such requirements and oversee air carrier security operations at their own airports, under their national laws. Given the different legal regimes within which other civil aviation authorities operate, most of TSA's foreign government counterparts address international aviation security responsibilities differently than in the United States, resulting in divergent authorities and shared responsibilities. As a result, implementation and sustainment of measures frequently proves difficult. TSA continues to actively engage with our international partners to ensure the security of flights bound for the United States and to enhance the overall security of international civil aviation.

Question 2. Will smaller airports be utilized in the initial run up of WBI machines this year?

Answer. Transportation Security Administration (TSA) deployment strategies for security technologies are based on risk, airport readiness, and operational suitability, as well as facility constraints. Many of these deployment factors make it is less likely that smaller airports will be slated to receive initial AIT systems. By the end of 2010, TSA expects to have 450 units deployed and has budgeted for an additional 500 units in 2011. However, TSA will continue to work toward full deployment of AIT systems, to include all category X (largest airports) through category IV airports (smallest airports). This would require a total of approximately 1,800 units.

Question 3. Do you have any concerns that an inability to apply advance screening technologies across the entire system will leave vulnerabilities in the aviation security system that could be exploited by terrorist?

Answer. The Transportation Security Administration employs a layered security approach that combines technology and process to address the wide variety of aviation security threats. While Advanced Imaging Technology (AIT) provides enhanced capabilities to detect person-borne threats, other technologies and screening processes, such as explosives trace detectors and pat-downs, are used to increase the probability of threat detection when an AIT is not available or installed at the checkpoint.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO HON. JANET NAPOLITANO

Question 1. TSA is reportedly not positive whether a full body imaging machine would have picked up on the explosives Abdulmutallab was carrying, but some suggest that it would have; but, if a passenger can elect a pat-down instead of going through an AIT machine, is TSA confident a pat-down would have been effective in this case?

Answer. While no technologies or procedures will detect 100 percent of all threats, the pat-down is the Transportation Security Administration's (TSA) designated alternate screening procedure if an individual declines to be screened by the advanced imaging technology. TSA is adding procedures to increase our ability to detect explosives on individuals and in accessible property. TSA is also reviewing its pat-down procedures to improve explosive detection capabilities.

Question 2. Are current TSA regulations for flight attendant counterterrorism training sufficient and effective?

Answer. The current Transportation Security Administration (TSA) regulations for flight attendant security training are sufficient and effective. Current flight attendant security training is required by 49 U.S.C. § 44918, enacted by section 603 Vision-100 Century of Aviation Reauthorization Act, Public Law 108–176 (2003), and title 49, Code of Federal Regulations (49 CFR, Part 1544). Title 49 CFR 1544, Subpart B requires the aircraft operators to adopt and implement a security program. The specific elements of flight attendant security training are outlined in the Aircraft Operator Standard Security Program. Section 44918 requires aircraft operators to develop and submit crew security training to TSA for review and approval; that approval function is delegated to the operators' assigned TSA Principal Security Inspector (PSI). Each air carrier has submitted a training program that has been determined to be acceptable by the PSI.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HON. JANET NAPOLITANO

Question 1. Without security cameras, TSA would not have been able to verify the security breach at Newark Airport or identify the suspect. Should all airports, particularly the largest and most at-risk, have security cameras at all checkpoints and secure area exits? How many airports currently do not have security cameras at security checkpoints and exits?

Answer. The Transportation Security Administration (TSA) encourages airports to have video surveillance capabilities with available and immediate access to views and video recordings at security checkpoints and secure area exits. A TSA survey of airports indicates that most large airports do have security cameras at checkpoints.

Question 2. In the Newark Airport breach, the security of a busy, heavily traveled exit was left to just one TSA guard. The suspect was able to sneak in when that lone guard was distracted. What are you doing to fortify security at secure area exits?

Answer. The exit lane breach at Newark Liberty International Airport has been discussed with every Federal Security Director (FSD) in the Nation, focusing on the specific exit lane failure at Newark, remediation measures taken there, and mitigation efforts to avoid similar breaches at other airports. All FSDs have been instructed in writing to review their local exit lane procedures with their senior staff and to increase the frequency of local breach drills.

In addition, TSA will be executing an Exit Lane Breach Control Pilot early this summer to establish a set of initial capabilities for an Exit Lane Breach Control system that will deter, prevent, or render ineffective an attempt to use the exit lane as a means to bypass a security checkpoint.

Question 3. The suspect in the Newark Airport security breach is being charged under New Jersey state law with "defiant trespassing." In other cases around the country, individuals who purposely breached security at airport exits also walked away with a slap on the wrist. Is deterring and prosecuting these offenders a national security issue that should rest with the Federal Government, rather than individual states or local governments?

Answer. A wide range of sanctions, under Federal and State law, should be available to law enforcement and prosecutors. Because the circumstances surrounding these types of violations can vary tremendously from unintentional breaches of security to criminal and willful conduct, the more varied the legal options the better equipped the prosecutor is to seek the appropriate sanction. Under Federal law there are significant penalties for those persons who knowingly and willfully enter an aircraft or airport area in violation of security requirements (49 U.S.C. 46314); for those who interfere with security screening personnel (49 U.S.C. 46503, which includes an enhanced penalty of life imprisonment if the crime involves use of a dangerous weapon); or those who attempt to board an aircraft with a dangerous and concealed weapon or explosive (49 U.S.C. 46505).

Question 4. At a Senate Judiciary Committee hearing this past November, Attorney General Holder expressed his support for my legislation to close the Terror Gap that allows known and suspected terrorists to buy guns legally. Does the Department of Homeland Security also support closing this loophole?

Answer. The Administration does not have a formal position on S. 1317 at this time.

Question 5 In the 9/11 Act, Congress required TSA to conduct a pilot project to test different security technologies at airport secure area exits. It's been over two and half years since this Act was signed into law, but TSA has yet to complete this pilot project. Why hasn't the Department completed this important project and what is the Administration doing to strengthen security at airport secure area exits?

Answer. In June 2009, the Transportation Security Administration (TSA) issued a solicitation for the piloting of exit lane technology systems at Dallas Fort Worth International Airport and Seattle-Tacoma International Airport and is working closely with the airport authorities to implement the project. The negotiation process with the vendors should begin in March 2010 and take approximately 30 days to complete. The National Laboratories, under the Department of Energy, will be working with TSA and the airport authorities on the evaluation and demonstration effort.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO HON. JANET NAPOLITANO

Question 1. What is being done to improve the situation regarding our TSA workforce? TSA employee morale is very low and attrition rates at the agency are unusually high. I've heard from airports in my home state that say screening equipment is not being adequately staffed. What are we doing to make sure that TSA has a robust and capable staff?

Answer. The Transportation Security Administration's (TSA) morale and attrition have improved over the last year. TSA's attrition for 2009 was 10 percent. This is a 48 percent reduction from 2008, which had an attrition rate of 19 percent, and is less than the government-wide rate of 11 percent as reported by the Bureau of Labor Statistics.

Our workforce survey results have consistently shown improvements in our employees' job satisfaction beginning at 45 percent on the 2004 Federal Human Capital Survey (FHCS) to TSA's most recent 2008 Organizational Satisfaction Survey (OSS) where 64 percent of employees were satisfied with their job. Analysis shows that across survey efforts (*e.g.,* OSS, the Department of Homeland Security All Employee Survey, and the FHCS) TSA's overall job satisfaction can be further improved by

continuing to focus on the areas of improving the quality of leadership and continuing to involve employees in decisions that affect the workforce. In the 2008 FHCS, the most recent comprehensive survey for which data is available, there were improvements in many dimensions. Notable category results include: TSA's "Employee Skills/Mission Match" score went up by 8 percent, "Performance-Based Rewards" score went up by 16 percent, and "Training and Development" improved by more than 12 percent. The "Support for Diversity" score increased by nearly 19 percent, "Pay and Benefits" went up by 8 percent, and "Work/Life Balance" improved by 23 percent. TSA's biggest gains were in the "Effective Leadership" category, where the scores improved by 25 percent.

TSA is committed to making the agency a collaborative and engaging workplace, and encourages employee involvement in meeting this goal. In addition, TSA provides extensive training to Transportation Security Officers (TSOs) to maintain a highly capable and robust staff. TSO training includes basic training for initial hires, on-the-job training, lead and supervisory technical training, recurrent training, advanced technical skills training, remedial training, and return-to-duty training. TSOs were also trained on ENGAGE!, an extensive retraining program that brought together the latest thinking from intelligence, explosives detection, and inhuman factors that can affect security. TSA also has implemented employee development programs such as the Career Evolution Program and the Associates Program. The TSA Career Evolution Program (CEP) is a hiring initiative, for internal candidates only, designed to identify and maximize the incredible talents and experience of our diverse workforce. The program is an exceptional opportunity for intensive training in the stimulating environment of TSA Headquarters.

The TSA Associates Program Pilot is a Career Development Program for our Transportation Security Officers (TSO's) to help them to achieve an Associate's Degree in Homeland Security with the initial three courses at their work place. Currently, less than 10 percent of TSO's have an associate's degree and higher. As this program is implemented in a wider scope it will allow our diverse workforce the opportunity to further their education, thus affording them more opportunities for advancement within the agency.

Currently, all screening equipment is fully staffed. To ensure that the screening equipment will continue to be fully staffed, the Fiscal Year 2011 budget request for additional equipment also includes a request for TSO and support staff.

Question 2. With all the focus on screening equipment hardware, there is also promising technology in the form of threat detection and identification software. More effective threat detection software and imaging analysis technology could serve as a good complement to scanner equipment that we are employing. What efforts have DHS and TSA taken to employ threat detection and identification software as part of its security program? Do you have standards in place for the threat detection software that is being used in conjunction with scanner equipment being used at TSA checkpoints?

Answer. Currently, the Transportation Security Administration is exploring the development of Automated Targeting (ATR) software. The goal is to utilize ATR detection algorithms to provide comparable detection capabilities without the need of an image interpretation operator. The Department of Homeland Security Science and Technology Directorate is also working to develop data input and output standards under the Digital Imaging Communications on Systems program.

Question 3. I am sure you recall the conversation we had last time you were before this committee concerning TSA's refusal to reimburse airports around the country that had, on good faith, installed in-line explosive detection equipment at the request of TSA. As we work toward securing our aviation system, it is important that TSA work in close cooperation with our airports on security initiatives. What is the TSA doing to include, coordinate and share information with the airport operators around the country who have first responder responsibilities for aviation security events?

Answer. The Transportation Security Administration (TSA) has established many programs to coordinate and share information with the airport operators around the country who have first responder responsibilities for aviation security events, both from the local and the headquarters level. At many airports located around the country, the Federal Security Director (FSD) has an Assistant Federal Security Director for Law Enforcement on staff to interact with local operators regarding aviation security events. The FSD also has Transportation Security Inspectors on staff to ensure stakeholder compliance with Federal regulations such as those pertaining to Law Enforcement Support and Personnel, Recordkeeping for Law Enforcement Personnel, Contingency Plans (including plan review and exercise mandates), Security Directive Measures, and Incident Management Procedures. In addition, the TSA

Office of Intelligence has assembled a Field Support Unit, through which Field Intelligence Officers located at airports around the Nation can work with airport operators and local law enforcement entities on aviation security issues.

TSA's Office of Transportation Sector Network Management (TSNM) interacts with airport operators from the headquarters level by working with the local FSDs and the TSA Personnel Security Office to process security clearances for stakeholders. The SECRET level clearance provides a means to share pertinent security and/or threat information with the stakeholder and assist with understanding the need to implement certain security measures to mitigate threat. TSNM interacts directly with stakeholders on a routine basis by supporting a TSA secure web board and electronic information mailbox. This office also participates in industry workgroups and conferences in an effort to exchange information and identify aviation security enhancements.

Question 4. What is the status of NSEERS (National Security Entry/Exit Registration System) and how is it impacted by the Christmas Day attempted bombing?

Answer. The NSEERS program is currently operational. DHS has not made any changes as a result of the failed Christmas Day bombing.

NSEERS was originally created to record certain actions, such as entry and exit, of designated travelers. At the time the designations were established, they were geared toward providing the capability to conduct extra scrutiny for those categories of individuals considered most likely to present a national security threat, given the intelligence available. Since the time NSEERS was initiated, DHS has implemented many new capabilities that broadly address the ever-evolving threats to the United States. The information regarding entry and exit recorded under NSEERS is also tracked more effectively, and for a much broader population, though other DHS programs. DHS is also able to use intelligence-driven criteria to target individuals for additional immigration and border screening, rather than relying on fixed country-based criteria. DHS is currently reviewing the future of the NSEERS program.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK BEGICH TO HON. JANET NAPOLITANO

Question 1. What steps is the Department of Homeland Security taking to ensure the relevant intelligence information is getting to the correct people to keep extremists and terrorists off of our planes and outside of our borders?

Answer. On June 3, 2008, Department of Homeland Security's (DHS) Office of Intelligence and Analysis issued a memorandum (Subject: DHS Protocol for Terrorist Watchlisting) to the Heads of all DHS Components. This document includes the instructions, format, and points of contact information required to make a nomination to the Terrorist Screening Data base (TSDB). The TSDB is the terrorist watchlist and is used by all agencies (including DHS) for terrorist screening. Additionally, the Department is currently working with the interagency collection and screening communities to review the current criteria for possible updating and enhancement.

Question 2. After the determination that this event was in fact a terrorist attack, were the flight crews on inbound flights notified? If so, how long did it take to notify the crews and what was the process and method of notification?

Answer. On December 25, 2009, at 2:40 p.m., under the direction of Transportation Security Administration senior leadership, the Federal Aviation Administration representative initiated a communiqué to all inbound aircraft from Europe to continental United States (CONUS). A telecom was held with all airline carriers and air traffic control centers to provide incident overview and flight information relating to Northwest Airline 253 (*i.e.,* origination/destination). In addition, airline carriers were instructed to require all passengers to remain seated during the final hour of flight prior to entering CONUS airspace. Airline carriers transmitted this information via Aircraft Communications Addressing and Reporting System to inbound CONUS aircraft.

Question 3. Advanced Imaging Technology is currently optional for all passengers. Those who choose not to undergo this type of screening are required to use the walk-through metal detector and undergo a pat-down procedure to ensure they receive an equivalent level of screening. Will this continue to be the policy of the TSA?

Answer. Yes, individuals who choose not to undergo advanced imaging technology screening will continue to be required to undergo a pat down search and may request private screening.

Question 4. How many different companies make Advanced Imaging Technology for passenger screening?

Answer. There are a number of Advanced Imaging Technology (AIT) vendors. The Transportation Security Administration has operationally tested units from three vendors, and an additional three vendors are currently undergoing laboratory testing at the Transportation Security Laboratories under the current AIT solicitation. TSA encourages a competitive market, and as more vendors meet TSA's operational testing requirements, they will be given the opportunity to compete for TSA's business.

Question 5. When will Secure Flight be fully deployed across airlines operating domestically? Why has implementation of Secure Flight fallen behind schedule?

Answer. Secure Flight is scheduled for deployment with the domestic carriers by spring 2010 and the international carriers by the end of calendar year 2010. The delay has been caused by technological challenges within some of the domestic carriers. However, the Transportation Security Administration (TSA) and the affected carriers have diligently worked together to solve the challenges and minimize the delays. With regard to international carriers, TSA is working with carriers on an alternate process to meet program requirements on schedule.

Question 6. How frequently does the TSA audit airport and aviation security in foreign countries? What recourse does TSA have if they find an airport does not meet U.S. security standards?

Answer. The Transportation Security Administration (TSA) is charged with assessing all foreign airports from which flights operate to the United States and those at which U.S. air carriers operate (regardless of the destination). TSA has a cadre of Security Specialists who visit the nearly 300 airports at intervals between one and 3 years. The frequency of the visits is based on risk analysis of current threat, documented vulnerabilities, and flight data. More frequent assessments are conducted if circumstances warrant, including previous deficiencies requiring follow-up visits, recent threat information, start-up service requests, and infrastructure changes at a particular foreign airport (*e.g.,* Haiti earthquake).

If TSA finds that an airport does not effectively carry out security measures, several options are available that range from providing on-the-spot correction recommendations, conducting formal training, recommending a Public Notice that the airport does not implement adequate security measures, or recommending that service to/from the United States be suspended. Recommending a Public Notice is ordinarily only employed when all other attempts have failed in assisting the airport or appropriate foreign government authorities to improve the security posture of the subject foreign airport, and in accordance with the requirements of 49 U.S.C. § 44907.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO HON. JANET NAPOLITANO

Question 1. Public reports indicate that the No Fly and Selectee Lists include about 18,000 people combined. By contrast, the Terrorist Screening Data base (TSDB), the master watchlist, includes approximately 400,000 people. Thus, more than 95 percent of the known or suspected terrorists deemed worthy of inclusion on the consolidated watchlist are not required to undergo additional airport screening. In your opinion, is that defensible?

Answer. The interagency established very stringent requirements (*e.g.,* an operational threat to aviation) for a record to be included in the No Fly or Selectee lists, which are subsets of the Terrorist Screening Data base (TSDB). In response to the December 25 attempted bombing, on December 27, 2010, President Obama ordered reviews of airport security measures and watchlist policies to determine if there are specific areas that warrant change or significant modifications that should be made. The Department of Homeland Security (DHS) is working with our interagency partners to re-evaluate the criteria and processes used to create the consolidated terrorist watchlist, including evaluating the process by which identities are added to the No Fly and Selectee lists. As part of these reviews, DHS is taking into account changes in our process, such as the implementation of Secure Flight, so that we may identify opportunities for further enhancements to the watchlisting process.

Question 2. One of the 9/11 Commission Recommendations that was not entirely adopted was that air passengers be screened against the full Terrorist Screening Data base (TSDB). Why wasn't this done? Do you now expect to make this change? And what are the consequences of doing so to the traveling public?

Answer. For international flights, U.S. Customs and Border Protection (CBP) screens all passengers with reservations to fly to the United States against the full Terrorist Screening Data base (TSDB) within 72 hours of departure. Passengers are

also screened against the TSDB prior to takeoff and upon entry to the United States. In addition, foreign nationals are screened against the TSDB when applying for a visa or obtaining Electronic System for Travel Authorization (ESTA) prior to flying to the United States.

DHS is working with our interagency partners to re-evaluate the criteria and processes used to create the consolidated terrorist watchlist, including evaluating the process by which identities are added to the No-Fly and Selectee lists.

The Secure Flight program currently compares passenger information only to the No-Fly and Selectee components of the TSDB. Secure Flight will become the primary mechanism to screen flights within the United States. In general, comparing passenger information against the No-Fly and Selectee components of the TSDB during normal security circumstances will enable the Transportation Security Administration (TSA) to counter the security threat to aviation. According to the Secure Flight Final Rule, TSA may use the larger set of TSDB records when warranted by security considerations.

Matching passenger information against the full TSDB would result in a significant increase in the number of "possible" matches, meaning individuals whose names or other information are similar to a person on the larger TSDB, and potentially cause unnecessary traveler delays and frustration without enhancing aviation security. The criteria for records on the No-Fly and Selectee lists were established to specifically include those individuals most likely to present a threat, while minimizing the potential for misidentification of passengers. Other records don't indicate the same level of threat, or may not have adequate information to enable DHS to rapidly distinguish a positive match from misidentification. Matching against the entire TSDB would result in a significant increase in misidentifications.

Question 3. In the Department of Homeland Security Appropriations Act of 2008 (Public Law 110–161, Division E, Title II), Congress expressed concern about the fact that the full TSDB was not being used for airline passenger screening. Specifically, the bill directed that, if the Assistant Secretary of Homeland Security (Transportation Security Administration) determines that the Secure Flight program does not need to check airline passenger names against the full terrorist watch list, then the Assistant Secretary shall certify to the Committees on Appropriations of the Senate and the House of Representatives that no significant security risks are raised by screening airline passenger names only against a subset of the full terrorist watch list. Has this required certification been made? If not, why not? If so, please provide a copy of the certification with your response.

Answer. The Assistant Secretary of Homeland Security (Transportation Security Administration) transmitted to Congress on December 9, 2008 his determination that no significant security risks are raised by screening airline passenger names only against the No-Fly and Selectee components of the full terrorist watch list.

Question 4. In the aftermath of the Christmas plot, do you believe, or can you confidently state, that our current advanced screening technologies would have detected the substance and/or devices on the Christmas Day terrorist, considering the amount of explosive material and the method in which it was concealed?

Answer. The Transportation Security Administration (TSA) employs a layered security approach that combines technology and process to address the wide variety of aviation security threats. While no technology is a silver bullet in stopping a terrorist attack, a number of technologies, when employed as part of a multi-layered security strategy, can increase our ability to detect dangerous materials. For example, Advanced Imaging Technology provides enhanced capabilities to detect person-borne threats. Other technologies and screening processes are also important, such as well-trained Transportation Security Officers, Behavior Detection Officers, Bomb Appraisal Officers, Federal Air Marshals, canine teams, and an engaged traveling public.

Question 5. Our country's experience combating drug trafficking demonstrates the willingness of smugglers to conceal contraband in body cavities. As publicly described, even our most advanced screening technologies do not have the capability to detect explosives or explosive devices concealed in body cavities. Given this known security weakness, do we need to further utilize explosive sniffing canines across our transportation system? What additional training and resources would be required to train canines to detect explosives on humans?

Answer. The President's FY 2011 budget requests $71 million for an additional 275 explosives detection canine teams for Category X and I airports. The Transportation Security Administration's (TSA) National Explosives Detection Canine Team Program (NEDCTP) develops, trains, deploys, and certifies explosives detection canine teams to deter and detect the introduction of explosive detection devices into the transportation system.

As a result of the December 25, 2009, attempted terrorist attack, TSA is accelerating its efforts to develop a program to train canines for the detection of Person-Born Improvised Explosive Devices (PBIED). This initiative, taken in cooperation with the science community, will include canines physically searching humans as well as utilizing a method known as Vapor Wake Detection. This method relies on the canine's ability to process air currents and recognize odors the canine has been specifically trained to detect, regardless of whether the person is moving or standing still. TSA's goal is to institute PBIED training in new canine training.

Question 6. In the years following the September 11 attacks, many terrorist acts and attempted plots have involved so-called "clean skin" terrorists: people with spotless records whose documents would not arouse suspicion. How can we protect the homeland effectively from such perpetrators, without unduly impeding the millions of travelers who have no ill will toward the United States?

Answer. The use of "clean skins" is a recognized threat and is a significant focus in the Department of Homeland Security's (DHS) counterterrorism strategy. No matter how good the watchlist check process is, the terrorists will seek ways to identify and use individuals who are unknown to the U.S. Government. To combat this threat, DHS relies on layers of defense, including the use of physical screening technologies, analytical targeting tools to identify unknown threats, canine teams, behavior detection officers, and other security measures. This integrated, layered approach increases our ability to deter, detect, and prevent someone from doing us harm.

DHS is constantly examining potential areas of threat and is investing in countermeasures. For example, DHS has established a partnership with the Department of Energy and its National Laboratories to develop new and effective technologies to detect known threats, and to anticipate new ways by which terrorists could board an aircraft with weapons or other materials.

In addition, DHS is accelerating the deployment of Advanced Imaging Technology (*i.e.,* "full body" scanners) to provide additional capability to identify objects or materials hidden on a person, such as those used in the attempted December 25 attack. We are also encouraging foreign aviation security authorities to use similar technologies and increase their security capabilities.

Question 7. During a December 2, 2009, hearing before this committee, I asked you whether Attorney General Holder had consulted you on the decision to move the Guantanamo Bay detainee trials to New York City. At that hearing you responded that you were not consulted but were confident U.S. soil could be protected. Given recent events and apparent weaknesses in our security system, evident from the Christmas Day plot, do you still agree with the decision to move the trial to New York? And do you stand by the notion that any shortcomings in our security system can be nullified in order to protect all U.S. citizens during that highly stressful time?

Answer. The President has stated that no final decision has been made on whether to try the case in New York or to identify an alternate venue given the concerns that have recently been raised by local officials. The Federal courts have had a long history of successfully prosecuting terrorists in a secure manner that brings them to justice and protects sensitive information. The previous Administration successfully prosecuted hundreds of terrorists in Federal courts.

I am confident we can bring the GITMO detainees to justice in a safe and secure manner, and I expect to be involved in security preparations for the trial when a final decision is made about the venue.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. OLYMPIA J. SNOWE TO HON. JANET NAPOLITANO

Question 1. The findings of the Administration's report released January 7, 2010, reviewing the intelligence failures leading up to Christmas Day, 2009, concluded "the information that was available to analysts, as is usually the case, was fragmented and embedded in a large volume of other data," and that both "NCTC and CIA personnel who are responsible for watch-listing did not search all available databases to uncover additional derogatory information that could have been correlated with Mr. Abdulmutallab."

It is my understanding that most intelligence analysis is currently a process of manual searches of various databases.

It strikes me that this could easily reoccur, based on Director Leiter's testimony concerning the vast volume of data processed by the NCTC on a daily, if not hourly, basis. The Administration's review makes clear that the current intelligence-sorting processes today could be improved by utilizing technology that can be programmed

to differentiate among specific types of threats, assign roles and responsibilities to each, and manage the response and escalation procedures, including the follow-up on such threats. Could this potential gap be remedied with automation? Is the Department or the NCTC actively developing, or seeking, technology that can process such large volumes of data effectively, not missing intelligence-gathering opportunities, and if so, when will such technology be operational?

Answer. The Department of Homeland Security (DHS) is investigating ways to improve our ability to identify whether an individual has been previously encountered by a DHS entity by searching across the large number of systems in the Department. In response to the December 25, 2009 incident, the Department established a DHS Threat Task Force (DTTF) that established a single operations center allowing DHS personnel access to 47 government information systems individually in order to perform name traces. While the operations center represented a positive step forward and yielded actionable insights, there is still a need for the capability to search across multiple systems, including the intelligence systems, and to combine the results from across the Department and partner agencies. A federated search tool would allow DHS and partner agencies to "connect the dots" better.

Cross database search will enable DHS to search individual names, submit lists of names for search, and to set up alerts which are tripped when new information on individuals of interest comes in.

While technically feasible, we must ensure that we perform searches across databases in a manner that protects privacy and civil rights and civil liberties. It requires a review of applicable System of Records Notices (SORN) and Privacy Impact Assessments (PIA) to ensure that we use the databases in a manner consistent with what we have publicly stated about them. The Department will continue to work through these issues to make available for search the kinds of sensitive U.S. Persons data that are currently not easily shared with the Intelligence Community in a manner that protects civil rights and civil liberties, and ensuring DHS can achieve its mission to detect threats to the homeland.

Question 2. The findings of the Administration's report released January 7, 2010, reviewing the intelligence failures leading up to Christmas Day, 2009, concluded "the information that was available to analysts, as is usually the case, was fragmented and embedded in a large volume of other data," and that both "NCTC and CIA personnel who are responsible for watch-listing did not search all available databases to uncover additional derogatory information that could have been correlated with Mr. Abdulmutallab."

It is my understanding that most intelligence analysis is currently a process of manual searches of various databases.

Although our security and intelligence networks constantly are working to keep America safe, and their efforts have thwarted numerous terrorist attempts, it is evident that the existing workforce is spread thinly in many areas, and could face an even greater burden if heightened security measures are put in place. While I believe personnel increases would go a long way toward minimizing the risks we now face, I believe in some cases technology could reduce human errors and the failure to consider pertinent and currently inaccessible data or pass it on to other relevant parties. Do you believe the Department of Homeland Security and the Counter-Terrorism Center has sufficient resources to secure the latest technologies that would allow us to close these gaps?

Answer. The Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) believes that if DHS were able to perform integrated queries against a variety of databases within the Department and Intelligence Community (IC) reporting data bases, the Department would be in a better position to connect individuals like Abdulmutallab to certain types of derogatory data and prevent the next terrorist attack.

Records on Abdulmutallab existed in DHS's TECS database and the Department of State's Consolidated Consular Database (CCD). If IC reporting on Abdulmutallab had been more accessible and of sufficient depth, there is a greater likelihood that a link would have been found that could have provided warning about this individual. DHS is piloting technology that can enhance information sharing and analysis. The pilot is adapting technology that the Federal Bureau of Investigation has successfully used in counterterrorism financing cases. I&A is interested in the possibility of applying the technology to the work of the DHS Threat Task Force, the Intelligence Watch and Warning Branch, and the Immigration and Travel Security branch, where it has the potential to provide major analytic "lift." The pilot has made over 10 billion records available for search, but much more engineering rigor, and the time associated with employing that rigor, is needed to make it a fully operational system. If the pilots are successful and the technology found to be suitable

to the envisioned applications, DHS will review what additional resources are required and incorporate appropriate requests through the budget planning process.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHNNY ISAKSON TO HON. JANET NAPOLITANO

Question 1. Madam Secretary, almost 2 million people board aircraft in, or bound for, the United States every day. Odds are that a bottle of water or tube of hair gel in the hands of the vast majority of these individuals is not a threat. As we know the real aim of terrorists is to disrupt our way of life and provoke responses that are, often times, large-scale, ineffective, inefficient, counterproductive, and expensive.

Instead of these overreactions, and inconveniencing the vast majority of the 2 million travelers mentioned above, shouldn't we have a more robust watch list that is available to all relevant agencies of government and the airlines?

Wouldn't this help us isolate the small percentage of these average 2 million fliers each day who are suspicious and allow us to pay extra attention to them, instead of focusing on the young family, elderly grandmother, or soldier in uniform? Of course these groups should have to go through some form of security, but aren't our resources better spent focusing on the bad guys?

Answer. This issue is one that we face everyday at the Department of Homeland Security (DHS). It is embedded in the Department's mission to protect the homeland while facilitating legitimate trade and travel. We strive to create a balance between security and the personal freedoms individuals have come to associate with the United States. One of the primary goals of the Nation's counterterrorism efforts is to identify known or suspected terrorists in order to prevent them from harming U.S. citizens, both at home and abroad.

In response to the December 25 attempted bombing, on December 27, 2010, President Obama ordered reviews of airport security measures and watchlist policies to determine if there are specific areas that warrant change or significant modifications that should be made. DHS is working with our interagency partners to re-evaluate the criteria and processes used to create the consolidated terrorist watchlist, including evaluating the process by which identities are added to the No Fly and Selectee lists and how the lists are operationally managed by Federal agencies involved in the watchlisting process.

In addition, we must also work to enhance aviation security in other ways—including enhancing our physical screening capabilities. The terrorist use of "clean skins" (*i.e.,* persons with no previous records connecting them to a terrorist threat) as agents is a recognized threat and is a significant focus in DHS' counterterrorism strategy. It is important to remember that no matter how good our watchlist is, the terrorists will seek ways to identify and use individuals who are unknown to us. To combat the various types of threats, we rely on layers of defense, including use of algorithms to identify unknown threats, use of canine teams, behavior detection officers, and also improvements to our physical screening capabilities in addition to our use of the watchlist. This integrated, layered approach increases our ability to deter, detect, and prevent someone from doing us harm.

In an effort to better focus security efforts in accordance with potential risk, DHS is exploring the incorporation of new technology solutions and practices in the security process. For example, DHS has established a partnership with the Department of Energy and its National Laboratories to develop new and effective technologies to detect known threats, and to anticipate new ways by which terrorists could board an aircraft with weapons or harmful materials. The Transportation Security Administration also uses highly trained Behavior Detection Officers as a security layer to identify potential threats.

In addition, DHS is accelerating the deployment of additional Advanced Imaging Technology (*i.e.,* full body scanners) to provide additional capability to identify materials such as those used in the attempted December 25 attack. We are also encouraging foreign aviation security authorities to use similar technologies and increase their security capabilities.

Question 2. Madam Secretary, please update us, in a classified manner if need be, on the deployment of TSA's Behavior Detection Officer (BDO) program? How many airports is that program in now? How many officers are participating? Is this program in place at Hartsfield-Jackson airport?

Answer. The Transportation Security Administration (TSA) has completed deployment of Behavior Detection Officers (BDOs) at currently funded levels. The pending Fiscal Year (FY) 2011 President's Budget includes a request for an additional 350 BDOs. Screening of Passengers by Observation Techniques (SPOT) programs are

operational full-time at 161 of the Nation's airports. There are approximately 3,000 BDOs deployed at these airports. The specific locations where the SPOT program has been deployed is Sensitive Security Information. The Transportation Security Administration can provide this information to the Committee at your convenience in a non-public setting.

Question 3. Madam Secretary, my understanding is that the airlines incur the cost of returning passengers who are denied entry into the United States because of visa revocations, even though they boarded these passengers without the knowledge that these passengers have visas that have been revoked.

I know it wouldn't have been helpful in the Abdulmutallab case since the signs were missed and Abdulmutallab wasn't on the revocation list, but rather than have these airlines board these passengers only to have to return them, why doesn't DHS or CBP make the visa revocation list known to airlines via APIS Quick Query so they can deny boarding at the point of embarkation?

Instead of stopping these individuals at the point of entry at the airport, wouldn't you agree that denying these individuals the ability to board the aircraft in a foreign country is a more efficient, and in some instances safer, method? Is this something DHS is planning on doing? If not, why not?

Answer. The Department of Homeland Security (DHS) agrees that it is preferable to prevent the travel of an individual who will clearly be found inadmissible on entry, such as a traveler whose visa has been revoked.

Since December 25, 2009, CBP has implemented a manual process to notify carriers and advise them not to board an individual whose visa has been revoked or for other appropriate reasons. Further, CBP is in the process of developing an automated solution.

Question 4. Madam Secretary, it would seem that passengers who are willing to submit to background checks should be allowed to pass through an expedited screening. Can you update us on DHS and TSA's plans, if any, for a registered traveler program?

Answer. The Transportation Security Administration (TSA) concluded a two-year Registered Traveler (RT) pilot at 19 airports on July 30, 2008. As announced in the Federal Register—73 Fed. Reg. 44275 et. seq. (July 30, 2008), the TSA no longer regulates the RT business model and has completed a formal transition of RT to a fully private-sector model. The value of a trusted passenger program remains a worthwhile concept. The Department of Homeland Security continues to encourage interested vendors to work directly with airports and airlines on developing options for RT. TSA remains open to considering proposals that could provide a security benefit to the traveling public.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO HON. JANET NAPOLITANO

Question 1. Would you agree that the Christmas Day plot could well have been launched from a domestic airport? Given that the threat isn't the Secure Flight program which flags suspicious travelers on domestic flights for additional screening or ensure individuals on the No-Fly List don't get on a domestic flight vitally important? Has Congress done everything it can do to make sure this program is successful?

Answer. Secure Flight is indeed vital to enhancing the security of domestic and international flights in the United States. The Federal Government's assumption of responsibility for watchlist matching was a key recommendation of the 9/11 Commission and is mandated by the Intelligence Reform and Terrorism Prevention Act of 2004. The program serves to: (1) identify known and suspected terrorists, (2) prevent individuals on the No-Fly list from boarding and aircraft, (3) require individuals on the Selectee list to go through enhanced screening at the checkpoint, (4) facilitate passenger air travel with less confusion, and (5) protect individuals' privacy. Secure Flight provides a fair, equitable, and consistent matching process across all airlines; reduces instances of misidentified individuals; and offers consistent application of an integrated redress process for misidentified individuals through the Department of Homeland Security Travel Redress Inquiry Program (DHS TRIP). Congress has been very supportive of the Secure Flight program and the Transportation Security Administration's efforts to ensure passenger security. Continued Congressional support is vital as the Secure Flight program implements the program incrementally over the course of 2010. Secure Flight is on schedule to assume watchlist matching responsibilities from all domestic airlines by spring 2010 and international airlines by the end of 2010.

Question 2. If such a plot were launched from a domestic airport would a program like REAL ID have helped identify a terrorist who used a fraudulent driver's license as proof of identity to board a plane? A program like REAL ID was one of the top recommendations of the 9/11 Commission. Does TSA support moving forward with REAL ID as quickly as possible?

Answer. The REAL ID Act was established to increase the security in driver's licenses to reduce the threat of these documents being used to establish a fraudulent identity for official purposes, such as boarding a commercial aircraft—and thereby increasing aviation security. REAL ID was intended to establish minimum standards for the issuance of secure state issued driver licenses and identification cards to ensure that the individual who is applying for a secure document is who they say they are and is in lawful status in the U.S.

Unfortunately, as DHS had warned earlier in the year, 46 of the 56 states and territories were unable to meet the objectives for material compliance with REAL ID this past December. If we establish requirements that only a few states can meet, we can't achieve our security objectives. Over the last year, DHS has worked diligently with Congress to pass the widely-supported PASS ID bill—breaking the impasse and putting us on a path to the security enhancements we all support. Unfortunately, Congress has not enacted PASS ID.

In going forward, DHS plans to work with all the states to create a path that allows for the majority of states to rejoin our collaborative efforts to enhance security.

Question 3. From the TSA perspective can you explain the White House Vision for Aviation Security? In the aftermath of the Christmas Day plot, the Obama Administration's first response was to put in place a plethora of feel-good but meaningless initiatives aimed at the Transportation Security Administration (TSA) screening process. For instance, the TSA announced it would single out travelers from 14 countries for additional screening. This move made little sense. Terrorists, including al-Qaeda operatives, have long understood the need to route their attacks through countries that are not the most suspicious.

Answer. DHS has a multi-faceted approach to enhancing aviation security capabilities both at home and abroad following the December 25th attack. DHS has the lead for the Federal Government in three areas in the President's overall plan for corrective action:

- Aggressively pursuing enhanced screening technology, protocols, and procedures, especially in regard to aviation and other transportation sectors, consistent with privacy rights and civil liberties;
- Strengthening international partnerships and coordination on aviation security issues; and
- Developing recommendations on long-term law enforcement requirements for aviation security in coordination with the Department of Justice.

In addition, DHS provides a significant supporting role in re-evaluating and modifying the criteria and processes used to create watch lists.

As our overall aviation security posture is strengthened with the deployment of the capabilities and programs discussed in this report, DHS will review whether and how the enhanced security requirements for travelers originating from specified countries can be reduced or eliminated. This review will result in a balanced and sustainable approach to aviation security over the long term.

As DHS continues to explore avenues for strengthening aviation security, we will do so in a manner consistent with our civil rights, civil liberties and privacy responsibilities. Specifically, DHS will work to:

- Improve the processes available for identifying errors in U.S. Government data bases and making corrections to reduce the number of false-positives and misidentifications in the screening process;
- Ensure a more effective redress process is available for individuals who have inquiries or seek resolution of difficulties they experienced during their travel screening;
- Ensure that new technologies and techniques avoid or minimize the impact on civil liberties and privacy; and
- Continue our engagement with key ethnic and religious communities and other groups so that they understand aviation security policies and procedures, as well continuing to be able to express concerns to and seek information from Department officials.

Question 4. From the TSA perspective can you explain why was the Government able to foil a Similar 2006 Liquid Explosives Plot when it was unable to do so on

Christmas Day? In 2006, the U.S. was able to work effectively with its U.K. security counterparts to foil plans for a simultaneous attack on 10 airliners headed toward the U.S. This success was the result of information sharing, good intelligence gathering, and "connecting the dots." Clearly, there is a system in place that can work effectively to stop acts of terrorism against Americans.

Answer. In response to the December 25 attempted bombing, on December 27, 2010, President Obama ordered reviews of airport security measures and watchlist policies to determine if there are specific areas that warrant change or significant modifications that should be made. DHS is working with our interagency partners to re-evaluate the criteria and processes used to create the consolidated terrorist watchlist, including evaluating the process by which identities are added to the No Fly and Selectee lists and how the lists are operationally managed by Federal agencies involved in the watchlisting process.

DHS maintains a close relationship with the United Kingdom and other international partners to strengthen international security measures and standards for aviation security. Secretary Napolitano is fully committed to making whatever changes are necessary to protect the safety of the traveling public. Following the Christmas attack, senior DHS officials traveled to Europe and other locations where they met with officials and discussed the primary findings of President Obama's aviation security review. Rather than a failure to collect and share information, it was a failure to connect and understand the intelligence that we already had.

DHS continues to work with global leaders on ways to collectively bolster tactics for defeating terrorists wherever they may seek to launch an attack. DHS is reviewing security procedures and technology being used to screen passengers on U.S.-bound flights from airports in Africa, Asia, Europe, the Middle East and South America. DHS is also joining our international counterparts in a series of global meetings intended to bring about broad consensus on new international aviation security standards and procedures.

Question 5. How can TSA work better with the Department of State and with International Partners to improve security practices overseas? The relationship between DHS and the Department of State is weak and needs to be vastly improved. Specifically, the two agencies fail to coordinate on visa security matters. Abdulmutallab's visa was not revoked on December 25, 2009, despite information to warrant this type of action, nor was this information communicated to the National Counterterrorism Center.

Answer. In light of the attempted attack on December 25, 2009, as part of the Presidentially-mandated review, Department of Homeland Security (DHS) is working via the interagency process to examine methods to enhance security.

DHS and the Department of State (DOS) have a strong relationship and coordinate closely on national security as well as on a variety of other issues. Secretary Napolitano and Secretary of State Hillary Clinton meet regularly, as do officials at every level in offices and components from their respective departments, including the Transportation Security Administration (TSA). Interaction is frequent and both formal and informal. In March 2009, Secretaries Clinton and Napolitano established a Deputy Assistant Secretary-level forum that meets regularly to further improve coordination. Regular coordination also occurs through existing forums such as the Deputies Committee and Sub Interagency Policy Council.

DHS and DOS regularly share information on all visa applicants. This cooperation ensures that U.S. Customs and Border Protection (CBP) can act appropriately when encountering a visa holder. Additionally DHS makes its encounter records—including biometric and biographic records—available to DOS for their use.

The two departments also collaborate via the Visa Security Program (VSP), which has enabled significant improvements in information sharing and visa security mechanisms and through which DOS and DHS continue to evaluate areas for further cooperation. Pursuant to Section 428 of the Homeland Security Act (HSA), U.S. Immigration and Customs Enforcement's (ICE) VSP works cooperatively with DOS and other partners to protect U.S. national security. ICE is currently conducting VSP operations at 14 posts in 12 countries, offering a DHS law enforcement capability and providing an important complement to DOS efforts in the consular visa process. The VSP seeks to uncover ineligible applicants previously unknown to the U.S. Government, deny them access to visas and generate additional outcomes beyond the visa denial. These outcomes include creating new watch list records, updating existing records with new information, identifying trends, uncovering and halting fraud schemes which may be exploited by applicants with ties to terrorism, investigating criminals, supporting ongoing domestic criminal investigations, and generating intelligence products. ICE Special Agents accomplish this by working in a collaborative process at post with consular officials.

In May 2007, Congress passed H.R. 2206, mandating the creation of a Security Advisory Opinion Unit (SAOU) within VSP. VSP's SAOU is currently operating a pilot program at the Human Smuggling and Trafficking Center (HSTC) that screens one SAO category (the Condor category) and communicates any potential admissibility concerns to DOS. The SAOU has access to sensitive information and is available to assist Visa Security Units (VSUs) overseas as needed. VSP also has a presence at the National Targeting Center-Passenger and will deploy representatives to the National Counterterrorism Center this month.

Question 6. If an alert Federal Air Marshal was on that flight he might have spotted and prevented the intended attack. The Administration plans to expand the FAM program. Can you tell me what efforts are underway to work with other countries to convince them to adopt similar programs or start them?

Answer. The Transportation Security Administration (TSA) encourages other governments to develop and implement their own In Flight Security Officer (IFSO) Programs. TSA coordinates the approval process for foreign armed air marshals on foreign air carrier flights to and from the U.S. through bilateral agreements and facilitates movement/entry of foreign air marshals through U.S. airports. TSA provides an International Air Marshal Training Program, a Training Needs Assessment and a Trainer Exchange Program for countries interested in implementing IFSO programs. Since 2004, the Federal Air Marshal Service (FAMS) has provided training to 10 countries to promote IFSO programs, 16 tours were provided to international partners that expressed an interest, and 11 international site visits, instructor exchanges, or aviation conferences were attended.

TSA participates in the annual International Air Marshal Conference (IAMC). The IAMC provides a unique platform to exchange views and share best practices with air marshal programs from around the world.

Question 7. Most people don't realize that under the criteria required of new countries that enter the Visa Waiver Program, the U.S. is able to obtain more information, in a more timely manner, that would make it easier to identify a potential malicious traveler than an individual flying from a country where all they had to do was get a travel visa to the United States? Would it not be in the interest of TSA if the Congress allowed the U.S. Government more flexibility to bring countries into the program—authorities that Congress had allowed under the Bush Administration? This would not only strengthen travel security with friendly allies, it would allow the State Department to concentrate more of its counselor resources on countries of concern. Wouldn't the TSA support that?

Answer. Visa Waiver Program (VWP) countries are among our closest international partners. Countries participating in the VWP are required to meet strict security standards. These standards include information sharing agreements with the U.S. Government regarding known or suspected terrorists and perpetrators of other serious crimes, the sharing of lost and stolen passport information with INTERPOL, as well as standards for transportation security, border security, and document integrity. In addition, VWP travelers are subject to more stringent passport security standards and information disclosure procedures than other international travelers. The prospect of VWP membership accordingly is a superb tool for incentivizing security enhancements by foreign countries, upgrading the U.S. Government's screening capacity, and furthering partnerships with foreign governments.

DHS—in cooperation with other departments and agencies—conduct intense reviews of any prospective VWP country before the country can be admitted. The 35 current members of the program must meet and maintain the same standards, including information-sharing and transportation, border, and document standards, and they are subject to in-country biennial security reviews led by DHS. As a result, no other mechanism provides DHS with the opportunity to conduct as broad and consequential inspections of foreign security standards as does the VWP.

DHS and the Department of State continue to consult with valued allies to determine whether VWP designation is possible. For example, the respective U.S. embassies hold regular working groups to discuss VWP-related issues and DHS frequently hosts visiting delegations of foreign officials to discuss the statutory requirements of the VWP.

It is important to note that individuals applying for a visa to enter the United States go through extensive checks conducted by the Department of State at application, as well as a personal interview. Additionally, before flying to the United States, airlines provide U.S. Customs and Border Protection (CBP) with information from passenger reservations as well as manifest information so that CBP can conduct appropriate security checks.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HON. LEE HAMILTON AND HON. TOM KEAN

Question 1. The suspect in the Newark Airport security breach is being charged under New Jersey state law with "defiant trespassing." In other cases around the country, individuals who purposely breached security at airport exits also walked away with a slap on the wrist. Is deterring and prosecuting these offenders a national security issue that should rest with the Federal Government, rather than individual states or local governments?

Answer. Deterring and prosecuting airport security offenders strikes us as an important part of a multi-layered aviation security program. However, our National Security Preparedness Group has not studied the specific issue of Federal versus state prosecution. We would welcome the opportunity to discuss this issue with you further.

Question 2. The Christmas Day attack and the security breach at Newark airport highlighted glaring gaps in our aviation security, but the 9/11 Commission report noted that, "opportunities to do harm are as great or greater in maritime and surface transportation." What should the Federal Government be doing to improve our rail and port security?

Answer. The Executive Branch and the Congress have made tremendous strides on maritime and surface transportation since the publication of the 9/11 Commission report. Part of the mandate of the NSPG is to continue to study the implementation of our recommendations, including the effectiveness of the actions the Congress and the President have taken on these issues. We would welcome the opportunity to discuss these issues further with you and work together to ensure we are doing all we can.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARK WARNER TO HON. LEE HAMILTON AND HON. TOM KEAN

Question. In your testimony and in your recent op-ed in USA Today, you mention that it should be a priority of the DNI (Director of National Intelligence) to break down the wall between foreign and domestic intelligence and to create an architecture that would enable such sharing. How would you rate our progress thus far in that regard? What specific steps must be taken to improve this situation?

Answer. We have asked this very question throughout our work at the Bipartisan Policy Center. It is our sense that the DNI made a substantial step forward with the promulgation of Intelligence Community directive 501 entitled "Discovery and Dissemination or Retrieval of Information within the Intelligence Community." But now the issue is implementation. The Congress can play a very important role in ensuring effective implementation through its oversight function. As you are aware, the failure to share information was among the most serious problems evident on 9/11 and it is incumbent upon us to monitor these issues carefully to help ensure continued progress.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK BEGICH TO HON. LEE HAMILTON AND HON. TOM KEAN

Question 1. What lessons from 9/11 have we failed to take appropriate action on?

Answer. It is our sense that we as a country have not solved the issues of interoperable communications nor establishing effective command and control at incident sites. Certainly these topics require more attention and cooperation among state, local, and Federal authorities.

Two other prominent items of unfinished business from the 9/11 Commission pertain to civil liberties and Congressional oversight. We recommended the creation of a Civil Liberties Board. It was stood up in Bush Administration but later lapsed after Congress enacted changes to its mandate. We have publicly urged President Obama to swiftly appoint members and send them to the Senate for confirmation.

With regard to Congressional oversight, we recommended two options to increase the authority of the permanent select Committees on Intelligence. Congress did not adopt either recommendation. We remain seriously concerned regarding Congressional oversight over the intelligence community and are open to ideas outside of the ones we recommended. Finally, we recommended consolidating jurisdiction over the Department of Homeland Security. We are increasingly concerned that DHS has too many masters in the Congress, which inhibits quality oversight. Throughout the years we have repeatedly urged the leadership to make progress on this issue and

will continue to look for opportunities to press this important piece of unfinished business.

Question 2. Your joint testimony cites the vast amount of incoming information counterterrorist analysts are inundated with. What steps do we need to take to make sure the relevant data and information collected by the intelligence community is being analyzed properly and that the dots are being connected before incidents like the Christmas Day attack occur?

Answer. We believe the answer to this question lies with utilizing new technology and ensuring that we recruit and retain the best people for the job. We're gratified that apparently there was not a failure to share information in the Christmas attack. The problem was a failure of analysis, and we're fortunate to be able to use this episode to underscore the importance of this issue in stopping future attacks.

Question 3. What are the remaining recommendations of the 9/11 Commission that have not either been introduced as legislation or signed into law?

Answer. See response to Question #1.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN ENSIGN TO HON. LEE HAMILTON AND HON. TOM KEAN

Question 1. After Vietnam and the failed attempt to rescue American Hostages in Iran, the Congress took it upon itself to fix some of problems and tensions that existed between the military services. The concept of "jointness" or of having the different military services increase cooperation has served our Nation well. In order for officers to be promoted to the Flag or General Officer rank, they have to complete at least one joint duty assignment and their joint professional military education. This "sharing" of personnel with the Joint Staff and other military services, along with this formalized course work, has forced the different services to interact and has led to greater efficiency and communication between them. Does the IC have any program such as this where individuals in one IC agency can spend time working for another?

Answer. Yes, The Director of National Intelligence, pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004, on May 16, 2006, promulgated Intelligence Community Policy Guidance 601.01, an Intelligence Community Civilian Joint Duty Program. The directive provides that joint duty certification is a mandatory qualification requirement for promotion.

Question 2. If so, is spending time with another IC agency a prerequisite for promotion within the community?

Answer. Yes, the directive provides that joint duty certification is a mandatory qualification requirement for promotion.

Question 3. If not, is this something that you have looked at? Do you believe the IC needs some sort of joint billeting requirement? Should this IC billeting requirement be a prerequisite for promotion to a certain level?

Answer. The 9/11 Commission studied this issue closely and concluded that the intelligence community needed to act more like a joint enterprise and less like a series of specialized intelligence agencies. One way to achieve this was a joint duty system and we recommended that the Defense Department's Goldwater-Nichols Reforms be a model for the intelligence community. We have not conducted an exhaustive study of the IC's Joint Duty program but our understanding is that it is working well and we look forward to studying this issue further.

○