AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# FLIGHT 253: LEARNING LESSONS FROM AN AVERTED TRAGEDY

## HEARING

BEFORE THE

## COMMITTEE ON HOMELAND SECURITY
## HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JANUARY 27, 2010

**Serial No. 111–51**

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

56–189 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

## COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
WILLIAM L. OWENS, New York
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
ERIC J.J. MASSA, New York
DINA TITUS, Nevada

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

# CONTENTS


Page

STATEMENTS

The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security .. 1
The Honorable Peter T. King, a Representative in Congress From the State of New York, and Ranking Member, Committee on Homeland Security ..... 2
The Honorable Laura Richardson, a Representative in Congress From the State of California:
Oral Statement ..... 5

WITNESSES

Ms. Jane Holl Lute, Deputy Secretary, Department of Homeland Security:
Oral Statement ..... 24
Prepared Statement ..... 26
Mr. Patrick F. Kennedy, Under Secretary, Management, Department of State:
Oral Statement ..... 31
Prepared Statement ..... 33
Mr. Michael E. Leiter, Director, National Counterterrorism Center:
Oral Statement ..... 36
Prepared Statement ..... 38

FOR THE RECORD

The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security:
Statement Submitted by Eileen R. Larence, Director, Homeland Security and Justice Issues, and Stephen M. Lord, Director, Homeland Security and Justice Issues, Government Accountability Office ..... 6
Statement Submitted by the American Civil Liberties Union ..... 17

APPENDIX

Questions Submitted by Honorable Sheila Jackson Lee for Jane Holl Lute, Deputy Secretary, Department of Homeland Security ..... 81
Questions Submitted by Chairman Bennie G. Thompson for Michael E. Leiter, Director, National Counterterrorism Center ..... 84
Questions Submitted by Honorable Christopher P. Carney for Michael E. Leiter, Director, National Counterterrorism Center ..... 84

# FLIGHT 253: LEARNING LESSONS FROM AN AVERTED TRAGEDY

**Wednesday, January 27, 2010**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:03 a.m., in Room 311, Cannon House Office Building, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Harman, DeFazio, Jackson Lee, Carney, Clarke, Richardson, Kirkpatrick, Luján, Owens, Pascrell, Cleaver, Green, Himes, Kilroy, Titus, King, Souder, Lungren, Rogers, McCaul, Dent, Bilirakis, Broun, Miller, Olson, and Austria.

Chairman THOMPSON [presiding]. The Committee on Homeland Security will come to order. The committee is meeting today to receive testimony on "Flight 253: Learning Lessons from an Averted Tragedy."

Good morning. I would like to thank our witnesses for being here today. Today's hearing will examine the circumstances surrounding the attempted Christmas day bombing of Northwest Flight 253. This committee will examine what happened, why it happened, and what this Nation can do to make sure it does not happen again.

We all know the facts. Abdulmutallab boarded Northwest Flight 253 in Amsterdam bound for Detroit. As the plane entered Detroit's airspace, he removed chemicals concealed in his clothing and mixed them together with the intention of causing an explosion. Thankfully, he failed. Courageous passengers and crew subdued and restrained him until the plane landed, and he was taken into custody.

Since September 11, this Nation has spent billions of dollars to fix the aviation security system, yet 9 years later it is clear that the safeguards put in place during the last administration did not prevent another terrorist from boarding a plane and trying to do harm to Americans.

This single failed terrorist act has brought those unsolved security vulnerabilities into sharp focus. Security weaknesses in the process of gaining legal admission to this country, gaps in the collection and dissemination of information, a confusing plethora of lists used to identify dangerous individuals, stovepipes that impede the progress of information analysis and sharing, and inconsistencies in the use of screening technology all combine to create the situation faced by the passengers on Flight 253.

The 9/11 Commission identified many of these problems, and while the previous administration engaged in much movement to

solve these problems, it appears that movement and progress are not the same. Within 2 weeks of this incident, President Obama issued his preliminary report. The President's report found incoherent, systematic weaknesses, and human errors were the root cause of the intelligence failures that led to this incident.

To any reasonable observer, one fact was certain. The system did not work. In fact, the President ordered a series of corrective actions, a clear and unflinching assessment followed by quick action designed to address this long-known vulnerability must be commended.

But it is important for all of us to realize that we will not address our problems with terrorism in a blink of an eye with a single technology. This Nation must begin to adopt a layered approach to achieve a secure environment. We must not begin our security assessment at the airport gate.

I want to thank our witnesses, and I look forward to their testimony.

The Chairman now recognizes the Ranking Member of the full committee, the gentleman from New York, Mr. King, for an opening statement.

Mr. KING. Thank you, Mr. Chairman. Like you, I want to thank the witnesses for their testimony here today.

I think this is an especially critical hearing. Everyone knows mistakes are made. Mistakes do happen. I think what concerns us and what should concern us as we go forward is how those mistakes are addressed and what is being done to protect our Nation in the future and to protect those types of mistakes from happening again.

Mr. Chairman, one of the concerns I have is what appears to me an uncoordinated response from the intelligence community. I say that not just based on what we have learned over the past month, but also from watching the Senate hearings last week, from looking at the testimony, listening to what former Congressman Hamilton had to say yesterday.

I say that is I still can't determine who is in charge, who makes the decisions. If we go back to the 2006 event, the liquid explosives from London, clearly, the Department of Homeland Security was in charge. It was Secretary Chertoff who was out front. It was Kip Hawley, head of TSA, who was out in front.

This time there was really no one in front. Secretary Napolitano made several appearances. Mr. Brennan made several appearances. But it appears that there was no one who was coordinating this from beginning to end. There was no one who was going to be out in front.

I am concerned what the role—I asked Deputy Secretary Lute just during her testimony what DHS sees as its role as being, and I know in your statement, I have heard Secretary Napolitano say this, that the Department is a consumer of intelligence. I thought when the Department was created, we expected more of an affirmative role by the Department, again, as what did occur, I thought, in the last several years of the previous administration.

I am not making this a political issue, but if this administration is deciding to change emphasis, then I think we should know that, as to who is going to be the main coordinator here.

Also, I think it is important for the President to come forward and to establish some order in the intelligence community. I saw Lee Hamilton said yesterday, "I do not believe the President yet has a firm grasp of the intelligence community."

All of us are aware that in the past 6 or 8 months, there has been an open dispute between Admiral Blair and Director Panetta. That has not been resolved, and if it is resolved, it is resolved at the margins. That feud, if you will, is still there.

We find out that the main decisions, some of the key decisions that were made on December 25 were not made by anyone in the intelligence community, but apparently by the Justice Department, and then after that it appears the main player was the White House itself, John Brennan, neither of whom is part of the intelligence community.

If we are going to have an effective response and effective defense set up, I believe that the professionals in the intelligence field should have more to say. The departments and agencies that have been created for that purpose should be in the forefront.

So the whole issue of the Miranda warning—currently, no one—no one here today, nor Director Blair nor Director Panetta were consulted when that decision was made. It was made by the Justice Department, apparently.

Similarly, let me add on that, when it comes to the Justice Department being involved, it was the attorney general, who we have learned, and some of us have known it for a while, but it has now become public, when he made the decision to bring the 9/11 trials to New York, he never consulted with one person, not one person in New York—police commissioner, anyone of the State police, anyone of the U.S. Marshals.

No one was consulted about the security implications of that, which appears to be what was repeated on Christmas day when the Justice Department made this decision without getting any input from anyone else in the intelligence community.

Let me also make a point here, and I want to make this very clearly. I hope this will be a bipartisan point. I am outraged by the lack of information we have gotten from this administration since Christmas day. The previous administration—I will ask the Chairman to vouch for me on this—again, using the liquid explosive incident in London, from the night before and for every day and every hour after that, we received any information we asked for, that we requested. It was given to us. We were told what was classified, what was not to be made public.

In this case on Christmas night, the White House—and I have heard this from a number of people—told other agencies and departments not to give information out. We could not get anything. Whatever we got was on our own. We were not given any information. I believe John Brennan has set up an iron curtain of secrecy in the White House and wants to control the intelligence community. He wants to control the information.

I ask the Chairman, again, to back me on this, and he can disagree if he wishes. I don't know one item in the last—when I was Chairman or he was Chairman or either of us was Ranking Member, one bit of information that was given to us that was ever

leaked out if it was classified. We never got one complaint from the Department of Homeland Security or from NCTC or CIA or anyone.

But now going back to September, but especially this Christmas day, I believe that the White House is trying to control intelligence, is trying to control counterterrorism, and it is doing it in a way which is highly restricting the powers of the departments here involved and is cutting off the Congress from the information we have to have.

We have constituents, we have responsibilities. This cannot be something where the White House gets all the information, massages it, manages it, and then puts out the facts later on. So I am putting that at the foot of John Brennan.

I am putting it also at the foot of Attorney General Holder the fact that decisions are being made by him almost unilaterally that should be made by the professionals in the field, certainly in consultation with people who can agree or disagree on these decisions. But to have them unilaterally made by someone who is outside what I believe is the intelligence world is wrong. I think the President should address that.

I also believe that as far as Congress, we have a different role of that information. We have time and time again have had to bring resolutions frequently to get information. On this in particular, I know that an iron curtain came down on Christmas night. That was wrong.

It doesn't matter who is in power, whether Republican or Democrat, we need information as Members of Congress to get the job done. We are not getting it done, and I fault this administration. It is disgraceful and outrageous, and I put that at John Brennan.

I yield back.

Chairman THOMPSON. Thank you very much.

Ranking Member King is partially correct in terms of the committee's need to know with respect to any of this. I absolutely support his premise that this committee has a function. It cannot function without information in real time. That information should not be gleaned from the news media, but it should be gleaned from the proper source. It should not be screened.

But I would also say that the Secretary Lute, Deputy Secretary Lute, did contact me the night of Christmas on this event, and I think she probably reached out to you. But now, I am not aware of anybody else who tried to get in touch with us.

Mr. KING. Deputy Secretary Lute reached out to me, discussed what was going to be done as far as the future, as far as airline precautions, but nothing about the facts of this case.

Chairman THOMPSON. Okay, well——

Mr. KING. We were told by other agencies they could not give us any information.

Chairman THOMPSON. Well, no question the committee has the right to know, and others have a responsibility to provide it, and we will pursue that also.

Other Members of the committee are reminded that under committee rules, opening statements may be submitted for the record.

[The statement of Hon. Richardson follows:]

PREPARED STATEMENT OF HONORABLE LAURA RICHARDSON

JANUARY 27, 2010

Mr. Chairman, thank you for convening this very important hearing today focusing on the circumstances surrounding the attempted terrorist bombing of Northwest Flight 253 on December 25, 2009. It is important for the House to get answers regarding the events of that day. I thank our distinguished panel of witnesses for appearing before us today to share with us the lessons learned from this averted tragedy.

Like millions of Americans, I am a frequent air traveler, which makes the events of December 25 particularly personal to us all. While air travel still ranks as one of the safest ways to travel, this is an industry where a single incident can become an enormous tragedy. Beyond the lives lost and the damage to our economy, both the air travel industry and the Nation suffers as the public loses confidence in the integrity of our homeland security system.

It is disturbing to think what could have happened without the brave actions of the passengers aboard Flight 253. Those passengers are heroes and we cannot thank them enough for what they did. But what the committee is focusing on today is what should have happened, what systems should have worked, before we reached that point.

There are several questions to be explored today: (1) Why our intelligence agencies did not connect the dots regarding the suspect, (2) the efficiency of our visa and watch lists systems, (3) the expanding nature of al-Quaeda, and (4) what technology we use, or should be using, that would have prevented the events of December 25.

Also, I think we need to address why all the Members of this committee were not notified and briefed in a timely fashion.

In the days and hours immediately after Christmas day, Members of this committee were not briefed by the administration or TSA. As Members of the committee tasked with jurisdiction over the agencies responsible for security, that cannot be allowed to happen again. I look forward to working with the Chairman, my colleagues, and the administration to ensure that timely and meaningful consultation and information sharing takes place.

I look forward to the testimony of our distinguished panel of witnesses. We need to know exactly what went wrong and what we can do to prevent these repeated mistakes from happening again.

Thank you again, Mr. Chairman, for convening this hearing. I yield back the balance of my time.

Chairman THOMPSON. Before I welcome our witnesses, I want to indicate that Secretary Napolitano was invited to this hearing. We were told that she would be out of the country. I now understand she is no longer out of the country, but she is not here, so maybe Deputy Secretary Lute, you can pull us in on where the Secretary is.

Our first witness is Dr. Jane Holl Lute, the Deputy Secretary for the Department of Homeland Security. Dr. Lute has been before the committee a number of times and has been very straightforward in her presentations, and we appreciate that.

Our second witness is Mr. Patrick Kennedy, Under Secretary of Management at the Department of State. Our final witness is Mr. Michael Leiter, Director of the National Counterterrorism Center.

Without objection, the witnesses' full statement and a statement provided by GAO and a statement by the ACLU will be inserted into the record. I now ask each witness to summarize their statement for 5 minutes, beginning with Deputy Secretary Lute.

[The statements of the Government Accountability Office and the American Civil Liberties Union follow:]

STATEMENT OF EILEEN R. LARENCE, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, AND STEPHEN M. LORD, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

JANUARY 27, 2010

GAO HIGHLIGHTS

Highlights of GAO–10–401T, a statement for the record to the Committee on Homeland Security, House of Representatives.

*Why GAO Did This Study*

The December 25, 2009, attempted bombing of Flight 253 raised questions about the Federal Government's ability to protect the homeland and secure the commercial aviation system. This statement focuses on the Government's efforts to use the terrorist watch list to screen individuals and determine if they pose a threat, and how failures in this process contributed to the December 25 attempted attack. This statement also addresses the Transportation Security Administration's (TSA) planned deployment of technologies for enhanced explosive detection and the challenges associated with this deployment. GAO's comments are based on products issued from September 2006 through October 2009 and selected updates in January 2010. For these updates, GAO reviewed Government reports related to the December 25 attempted attack and obtained information from the Department of Homeland Security (DHS) and TSA on use of the watch list and new technologies for screening airline passengers.

*What GAO Recommends*

GAO is not making new recommendations, but has made recommendations in prior reports to DHS, the Federal Bureau of Investigation (FBI), and the White House Homeland Security Council to enhance the use of the watch list and to TSA related to checkpoint technologies. The agencies generally agreed and are making some progress, but full implementation is needed.

HOMELAND SECURITY.—BETTER USE OF TERRORIST WATCH LIST INFORMATION AND IMPROVEMENTS IN DEPLOYMENT OF PASSENGER CHECKPOINT TECHNOLOGIES COULD FURTHER STRENGTHEN SECURITY

*What GAO Found*

The intelligence community uses standards of reasonableness to evaluate individuals for nomination to the consolidated terrorist watch list. In making these determinations, agencies are to consider information from all available sources. However, for the December 25 subject, the intelligence community did not effectively complete these steps and link available information to the subject before the incident. Therefore, agencies did not nominate the individual to the watch list or any of the subset lists that are used during agency screening processes, such as the "No-Fly" list. Weighing and responding to the potential impacts that changes to the nomination criteria would have on the traveling public will be an important consideration in determining what changes may be needed. Also, screening agencies stated that they do not check against all records in the watch list, partly because screening against certain records may not be needed to support a respective agency's mission or may not be possible because of the requirements of computer programs used to check individuals against watch list records. In October 2007, GAO reported that not checking against all records may pose a security risk and recommended that DHS and the FBI assess potential vulnerabilities, but they have not completed these assessments. TSA is implementing an advanced airline passenger prescreening program—known as Secure Flight—that could potentially result in the Federal Government checking passengers against the entire watch list under certain security conditions. Further, the Government lacks an up-to-date strategy and implementation plan—supported by a clearly defined leadership or governance structure—which are needed to enhance the effectiveness of terrorist-related screening and ensure accountability for the process. In the 2007 report, GAO recommended that the Homeland Security Council ensure that a governance structure exists that has the requisite authority over the watch list process. The council did not comment on this recommendation.

As GAO reported in October 2009, since TSA's creation, 10 passenger screening technologies have been in various phases of research, development, procurement, and deployment, including the Advanced Imaging Technology (AIT)—formerly known as the Whole Body Imager. TSA expects to have installed almost 200 AITs in airports by the end of calendar year 2010 and plans to install a total of 878 units

by the end of fiscal year 2014. In October 2009, GAO reported that TSA had not yet conducted an assessment of the technology's vulnerabilities to determine the extent to which a terrorist could employ tactics that would evade detection by the AIT. Thus, it is unclear whether the AIT or other technologies would have detected the weapon used in the December 25 attempted attack. GAO's report also noted the problems TSA experienced in deploying another checkpoint technology that had not been tested in the operational environment. Since GAO's October report, TSA stated that it has completed the testing as of the end of 2009. We are currently verifying that all functional requirements of the AIT were tested in an operational environment. Completing these steps should better position TSA to ensure that moving ahead with a costly deployment of AIT machines will enhance passenger checkpoint security.

Mr. Chairman and Members of the committee: We are pleased to submit this statement on the progress Federal agencies have made and the challenges they face in key areas of terrorism information sharing and the deployment of checkpoint technologies. The December 25, 2009, attempted bombing of Flight 253 has led to increased scrutiny of how the Government creates and uses the consolidated terrorist screening database (the watch list) to screen individuals and determine if they pose a security threat, and highlighted the importance of detecting improvised explosive devices and other prohibited items on passengers before they board a commercial aircraft. The White House's initial review of these events exposed gaps in how intelligence agencies collected, shared, and analyzed terrorism-related information to determine if the subject—Umar Farouk Abdulmutallab—posed enough of a threat to warrant placing him on the watch list, which could have altered the course of events that day. To enhance its ability to detect explosive devices and other prohibited items on passengers, the Transportation Security Administration (TSA) is evaluating the use of Advanced Imaging Technology (AIT)—formerly called the Whole Body Imager—as an improvement over current screening capabilities.

In October 2007, we released a report on the results of our review—conducted at your request—of how the watch list is created and maintained, and how Federal, State, and local security partners use the list to screen individuals for potential threats to the homeland.[1] As a result of that review, we identified potential vulnerabilities, including ones created because agencies were not screening against all records in the watch list. We made a number of recommendations aimed at addressing these potential vulnerabilities and helping to enhance the effectiveness of the watch list process, which the agencies have not yet fully addressed. These recommendations—which we discuss later in this statement—are still important to address and can inform on-going reviews of the December 25 attempted terrorist attack.

Also, in January 2005, we designated information sharing for homeland security a high-risk area because the Government faced formidable challenges in analyzing and disseminating this information in a timely, accurate, and useful manner.[2] Since then, we have been monitoring and making recommendations to improve the Government's efforts to share terrorism-related information, not only among Federal agencies but also with their State, local, Tribal, and private sector security partners.[3] Addressing this high-risk area is important to help remove barriers that lead to agencies maintaining information in stove-piped systems, and to hold them accountable to the Congress and the public for ensuring terrorism information is shared, is used, and makes a difference. We are continuing to review Federal agencies' efforts to share terrorism-related information and expect to report the results of this work later this year.[4]

---

[1] GAO, *Terrorist Watchlist Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List,* GAO–08–110 (Washington, DC: Oct. 11, 2007).

[2] See GAO, *High-Risk Series: An Update,* GAO–09–271 (Washington, DC: January 2009), for our most recent update.

[3] See, for example, GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information,* GAO–06–385 (Washington, DC: Mar. 17, 2006); *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress,* GAO–08–492 (Washington, DC: June 25, 2008); and *Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed,* GAO–10–41 (Washington, DC: Dec. 18, 2009).

[4] We have three on-going reviews of terrorism-related information sharing that are being conducted based on separate requests from your committee, the House Committee on Oversight and

Continued

In addition, in October 2009, we released a report on TSA's efforts to deploy checkpoint technologies and the challenges the agency faces in these efforts.[5] We made eight recommendations related to the research, development, and deployment of these technologies. The Department of Homeland Security (DHS) agreed with our recommendations and identified actions planned or under way to implement them. While DHS is taking steps to address our recommendations related to conducting risk assessments, the actions DHS reported that TSA had taken or plans to take do not fully address the intent of the majority of our recommendations.

This statement for the record discusses: (1) The Government's efforts to use the terrorist watch list to screen individuals and determine if they pose a threat, as well as how aspects of this process contributed to the December 25 attempted terrorist attack and (2) TSA's planned deployment of the AIT for enhanced explosive detection and the challenges associated with this deployment.

This statement is based on products GAO issued from September 2006 through October 2009.[6] In conducting our prior work, we reviewed documentation obtained from and interviewed officials at the various departments and agencies with responsibilities for compiling and using watch list records. We also reviewed documentation and obtained information on current checkpoint screening technologies being researched, developed, and deployed. Our previously published reports contain additional details on the scope and methodology for those reviews. In addition, this statement contains selected updates conducted in December 2009 and January 2010. For the updates, GAO reviewed Government reports and other information related to the December 25 attempted attack, obtained information from DHS and TSA on the use of watch list records and new technologies for screening airline passengers, and interviewed a senior TSA official. We conducted our updated work in December 2009 and January 2010 in accordance with generally accepted Government auditing standards.

## IN SUMMARY

Because the subject of the December 25 attempted terrorist attack was not nominated for inclusion on the Government's consolidated terrorist screening database, Federal agencies responsible for screening activities missed several opportunities to identify him and possibly take action. We have previously reported on a number of issues related to the compilation and use of watch list records, such as the potential security risk posed by not checking against all records on the watch list. We also identified the need for an up-to-date strategy and implementation plan—one that describes the scope, governance, outcomes, milestones, and metrics, among other things—for managing the watch list process across the Federal Government. Such a strategy and plan, supported by a clearly defined leadership or governance structure, can be helpful in removing cultural, technological, and other barriers—such as those problems that the December 25 attempted terrorist attack exposed—that inhibit the effective use of watch list information.

With regard to the deployment of technology to detect explosives on passengers, TSA expects to have installed almost 200 AITs in airports by the end of calendar year 2010, and plans to procure and install a total of 878 units by the end of fiscal year 2014. While recently providing GAO with updated information to our October 2009 report, TSA stated that operational testing for the AIT was completed as of the end of calendar year 2009. We are in the process of verifying that TSA tested all of the AIT functional requirements in an operational environment. Moreover, we previously reported that TSA had not yet conducted an assessment of the technology's vulnerabilities to determine the extent to which a terrorist could employ tactics that would evade detection by the AIT. While we recognize that the AIT could provide an enhanced detection capability, completing these steps should better position TSA to have the information necessary to ensure that moving ahead with a costly deployment of AIT machines will enhance passenger checkpoint security.

---

Government Reform, and the Senate Committee on Homeland Security and Governmental Affairs.

[5] GAO, *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges,* GAO–10–128 (Washington, DC: Oct. 7, 2009).

[6] See GAO, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public,* GAO–06–1031 (Washington, DC: Sept. 29, 2006); GAO–08–110; *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks,* GAO–09–292 (Washington, DC: May 13, 2009); and GAO–10–128.

## BACKGROUND

*Terrorist Watch List Process*

The Terrorist Screening Center (TSC)—administered by the Federal Bureau of Investigation (FBI)—is responsible for maintaining the U.S. Government's consolidated watch list and providing it to Federal agencies as well as State, local, and selected foreign partners for their use in screening individuals. TSC receives the vast majority of its watch list nominations and information from the National Counterterrorism Center (NCTC), which compiles information on known or suspected international terrorists from Executive branch departments and agencies.[7] In addition, the FBI provides TSC with information on known or suspected domestic terrorists who operate primarily within the United States. To support agency screening processes, TSC first determines if each nomination contains specific minimum derogatory information for inclusion in its terrorist screening database. TSC then sends applicable records from the terrorist watch list to screening agency systems for use in efforts to deter or detect the movements of known or suspected terrorists. For instance, applicable TSC records are provided to TSA for use in prescreening airline passengers; to a U.S. Customs and Border Protection (CBP) system for use in screening travelers entering the United States; to a Department of State system for use in screening visa applicants; and to an FBI system for use by State and local law enforcement agencies pursuant to arrests, detentions, and other criminal justice purposes.[8]

*Airline Passenger Screening Using Checkpoint Screening Technology*

Passenger screening is a process by which screeners inspect individuals and their property to deter and prevent an act of violence or air piracy, such as the carrying of any unauthorized explosive, incendiary, weapon, or other prohibited item on board an aircraft or into a sterile area.[9] Screeners inspect individuals for prohibited items at designated screening locations. TSA developed standard operating procedures for screening passengers at airport checkpoints. Primary screening is conducted on all airline passengers before they enter the sterile area of an airport and involves passengers walking through a metal detector and carry-on items being subjected to X-ray screening. Passengers who alarm the walkthrough metal detector or are designated as selectees—that is, passengers selected for additional screening—must then undergo secondary screening, as well as passengers whose carry-on items have been identified by the X-ray machine as potentially containing prohibited items.[10] Secondary screening involves additional means for screening passengers, such as by hand-wand; physical pat-down; or, at certain airport locations, an explosives trace portal (ETP), which is used to detect traces of explosives on passengers by using puffs of air to dislodge particles from their bodies and clothing into an analyzer. Selectees' carry-on items are also physically searched or screened for explosives, such as by using explosives trace detection machines.

## ASSESSING POTENTIAL VULNERABILITIES RELATED TO NOT SCREENING AGAINST ALL WATCH LIST RECORDS AND ENSURING CLEAR LINES OF AUTHORITY OVER THE WATCH LIST PROCESS WOULD PROVIDE FOR ITS MORE EFFECTIVE USE

*Agencies Rely Upon Standards of Reasonableness in Assessing Individuals for Nomination to TSC's Watch List, but Did Not Connect Available Information on Mr. Abdulmutallab to Determine Whether a Reasonable Suspicion Existed*

Federal agencies—particularly NCTC and the FBI—submit to TSC nominations of individuals to be included on the consolidated watch list. For example, NCTC receives terrorist-related information from Executive branch departments and agencies, such as the Department of State, the Central Intelligence Agency, and the FBI, and catalogs this information in its Terrorist Identities Datamart Environment database, commonly known as the TIDE database. This database serves as the U.S. Government's central classified database with information on known or suspected

[7] By law, NCTC, which is within the Office of the Director of National Intelligence, serves as the primary organization in the U.S. Government for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except for intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. See 50 U.S.C. §404o(d)(1).

[8] See GAO–08–110 for additional details on the compilation and use of terrorist watch list records.

[9] Sterile areas are generally located within the terminal where passengers are provided access to boarding aircraft, and access is controlled in accordance with TSA requirements.

[10] A nonselectee passenger who alarms the walk-through metal detector on the first pass is offered a second pass. If the passenger declines the second pass, the passenger must proceed to additional screening. If the nonselectee passenger accepts the second pass and the machine does not alarm, the passenger may generally proceed without further screening.

international terrorists. According to NCTC, agencies submit watch list nomination reports to the center, but are not required to specify individual screening systems that they believe should receive the watch list record, such as the No-Fly list of individuals who are to be denied boarding an aircraft.[11] NCTC is to presume that agency nominations are valid unless it has other information in its possession to rebut that position.

To decide if a person poses enough of a threat to be placed on the watch list, agencies are to follow Homeland Security Presidential Directive (HSPD) 6, which states that the watch list is to contain information about individuals "known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."[12] HSPD–24 definitively established the "reasonable suspicion" standard for watchlisting by providing that agencies are to make available to other agencies all biometric information associated with "persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security."[13] NCTC is to consider information from all available sources and databases to determine if there is a reasonable suspicion of links to terrorism that warrants a nomination, which can involve some level of subjectivity. The guidance on determining reasonable suspicion, which TSC most recently updated in February 2009, contains specific examples of the types of terrorism-related conduct that may make an individual appropriate for inclusion on the watch list.

The White House's review of the December 25 attempted terrorist attack noted that Mr. Abdulmutallab's father met with U.S. Embassy officers in Abuja, Nigeria, to discuss his concerns that his son may have come under the influence of unidentified extremists and had planned to travel to Yemen.[14] However, according to NCTC, the information in the State Department's nomination report did not meet the criteria for watchlisting in TSC's consolidated terrorist screening database per the Government's established and approved nomination standards. NCTC also noted that the State Department cable nominating Mr. Abdulmutallab had no indication that the father was the source of the information. According to the White House review of the December 25 attempted attack, the U.S. Government had sufficient information to have uncovered and potentially disrupted the attack—including by placing Mr. Abdulmutallab on the No-Fly list—but analysts within the intelligence community failed to connect the dots that could have identified and warned of the specific threat.

After receiving the results of the White House's review of the December 25 attempted attack, the President called for members of the intelligence community to undertake a number of corrective actions—such as clarifying intelligence agency roles, responsibilities, and accountabilities to document, share, and analyze all sources of intelligence and threat threads related to terrorism, and accelerating information technology enhancements that will help with information correlation and analysis. The House Committee on Oversight and Government Reform has asked us, among other things, to assess Government efforts to revise the watch list process, including actions taken related to the December 25 attempted attack.

As part of our monitoring of high-risk issues, we also have on-going work—at the request of the Senate Committee on Homeland Security and Governmental Affairs—that is assessing agency efforts to create the Information Sharing Environment, which is intended to break down barriers to sharing terrorism-related information, especially across Federal agencies.[15] Our work is designed to help ensure that Federal agencies have a road map that defines roles, responsibilities, actions, and time frames for removing barriers, as well as a system to hold agencies accountable to the Congress and the public for making progress on these efforts. Among other things, this road map can be helpful in removing cultural, technological, and other

---

[11] As discussed later in this statement, agencies generally do not use the full terrorist watch list to screen individuals. Rather, they generally use subsets of the full list based on each agency's mission and other factors.

[12] The White House, *Homeland Security Presidential Directive/HSPD–6, Subject: Integration and Use of Screening Information* (Washington, DC, Sept. 16, 2003).

[13] The White House, *Homeland Security Presidential Directive/HSPD–24, Subject: Biometrics for Identification and Screening to Enhance National Security* (Washington, DC, June 5, 2008).

[14] The White House, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack* (Washington, DC, Jan. 7, 2010).

[15] The Intelligence Reform and Terrorism Prevention Act of 2004, as amended, defines the Information Sharing Environment as "an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out [section 1016]." See Pub. L. No. 108–458, § 1016(a)(2), 118 Stat. 3638, 3665 (codified as amended at 6 U.S.C. § 485(a)(3)). See also Homeland Security Act of 2002, 6 U.S.C. § 482 (requiring the establishment of procedures for the sharing of homeland security information, as defined by this section).

barriers that lead to agencies maintaining information in stove-piped systems so that it is not easily accessible, similar to those problems that the December 25 attempted attack exposed. We expect to issue the results of this work later this year.

*By Not Placing Mr. Abdulmutallab on the Consolidated Watch List or Its Subsets, the Government Missed Opportunities to Use These Counterterrorism Tools*

Following the December 25 attempted terrorist attack, questions were raised as to what could have happened if Mr. Abdulmutallab had been on TSC's consolidated terrorist screening database. We created several scenarios to help explain how the watch list process is intended to work and what opportunities agencies could have had to identify him if he was on the watch list. For example, according to TSC, if a record from the terrorist screening database is sent to the State Department's system and the individual in that record holds a valid visa, TSC would compare the identifying information in the watch list record against identifying information in the visa and forward positive matches to the State Department for possible visa revocation. If an individual's visa is revoked, under existing procedures, this information is to be entered into the database CBP uses to screen airline passengers prior to their boarding, which we describe below. According to CBP, when the individual checks in for a flight, the on-site CBP Immigration Advisory Program officers already would have been apprised of the visa revocation by CBP and they would have checked the person's travel documents to verify that the individual was a match to the visa revocation record. Once the positive match was established, the officers would have recommended that he not be allowed to board the flight.

Under another scenario, if an individual is on TSC's terrorist screening database, existing processes provide CBP with the opportunity to identify the subject of a watch list record as part of the checks CBP is to conduct to see if airline passengers are eligible to be admitted into the country. Specifically, for international flights departing to or from the United States (but not for domestic flights), CBP is to receive information on passengers obtained, for example, when their travel document is swiped. CBP is to check this passenger information against a number of databases to see if there are any persons who have immigration violations, criminal histories, or any other reason for being denied entry to the country, in accordance with the agency's mission. According to CBP, when it identifies a U.S.-bound passenger who is on the watch list, it coordinates with other Federal agencies to evaluate the totality of available information to see what action is appropriate. In foreign airports where there is a CBP Immigration Advisory Program presence, the information on a watchlisted subject is forwarded by CBP to program officers on-site. The officers would then intercept the subject prior to boarding the aircraft and confirm that the individual is watchlisted, and when appropriate based on the derogatory information, request that the passenger be denied boarding.

In a third scenario, if an individual is on the watch list and is also placed on the No-Fly or Selectee list, when the person checks in for a flight, the individual's identifying information is to be checked against these lists. Individuals matched to the No-Fly list are to be denied boarding. If the individual is matched to the Selectee list, the person is to be subject to further screening, which could include physical screening, such as a pat-down. The criteria in general that are used to place someone on either of these two lists include the following:

- Persons who are deemed to be a threat to civil aviation or National security and should be precluded from boarding an aircraft are put on the No-Fly list.
- Persons who are deemed to be a threat to civil aviation or National security but do not meet the criteria of the No-Fly list are placed on the Selectee list and are to receive additional security screening prior to being permitted to board an aircraft.[16]

The White House Homeland Security Council devised these more stringent sets of criteria for the No-Fly and Selectee lists in part because these lists are not intended as investigative or information-gathering tools or tracking mechanisms, and TSA is a screening but not an intelligence agency.[17] Rather, the lists are intended

[16] Of all of the screening databases that accept watch list records, only the No-Fly and Selectee lists require certain nomination criteria or inclusion standards that are narrower than the "known or appropriately suspected" standard of HSPD–6. The most recent guidance related to the No-Fly and Selectee list criteria was issued in February 2009.

[17] The Homeland Security Council originally was established in 2001 by Executive Order and subsequently codified into law by the Homeland Security Act of 2002 for the purpose of more effectively coordinating the policies and functions of the Federal Government relating to homeland security. See Exec. Order No. 13,228; Pub. L. No. 107–296, tit. IX, 116 Stat. 2135, 2258–59 (codified at 6 U.S.C. §§ 491–496). On May 26, 2009, the President announced the full integration of White House staff supporting National security and homeland security into a new "Na-

Continued

to help ensure the safe transport of passengers and facilitate the flow of commerce. However, the White House's review of the December 25 attempted terrorist attack raised questions about the effectiveness of the criteria, and the President tasked the FBI and TSC with developing recommendations for any needed changes to the nominations guidance and criteria.

Weighing and responding to the potential impacts that changes to the nominations guidance and criteria could have on the traveling public and the airlines will be important considerations in developing such recommendations. In September 2006, we reported that tens of thousands of individuals who had similar names to persons on the watch list were being misidentified and subjected to additional screening, and in some cases delayed so long as to miss their flights.[18] We also reported that resolving these misidentifications can take time and, therefore, affect air carriers and commerce. If changes in criteria result in more individuals being added to the lists, this could also increase the number of individuals who are misidentified, exacerbating these negative effects. In addition, we explained that individuals who believe that they have been inappropriately matched to the watch list can petition the Government for action and the relevant agencies must conduct research and work to resolve these issues. If more people are misidentified, more people may trigger this redress process, increasing the need for resources. Finally, any changes to the criteria or process would have to ensure that watch list records are used in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law.

*Agencies Do Not Screen Individuals Against All Records in the Watch List, Which Creates Potential Security Vulnerabilities; GAO Continues to Recommend That Agencies Assess and Address These Gaps*

In reacting to the December 25 attempted terrorist attack, determining whether there were potential vulnerabilities related to the use of watch list records when screening—not only individuals who fly into the country but also, for example, those who cross land borders—are important considerations. Screening agencies whose missions most frequently and directly involve interactions with travelers generally do not check against all records in the consolidated terrorist watch list. In our October 2007 report, we noted that this is because screening against certain records may not be needed to support a respective agency's mission or may not be possible because of computer system limitations, among other things.[19]

For example, CBP's mission is to determine if any traveler is eligible to enter the country or is to be denied entry because of immigration or criminal violations. As such, CBP's computer system accepts all records from the consolidated watch list database that have either a first name or a last name and one other identifier, such as a date of birth. Therefore, TSC sends CBP the greatest number of records from the consolidated watch list database for its screening. In contrast, one of the State Department's missions is to approve requests for visas. Since only non-U.S. citizens and nonlawful permanent residents apply for visas, TSC does not send the department records on citizens or lawful permanent residents for screening visa applicants.

Also, the FBI database that State and local law enforcement agencies use for their missions in checking individuals for criminal histories, for example, also receives a smaller portion of the watch list. According to the FBI, its computer system requires a full first name, last name, and other identifier, typically a date of birth. The FBI noted that this is because having these identifiers helps to reduce the number of times an individual is misidentified as being someone on the list, and the computer system would not be effective in making matches without this information. Finally, the No-Fly and Selectee lists collectively contain the lowest percentage of watch list records because the remaining ones either do not meet the nominating criteria, as described above, or do not meet system requirements—that is, include full names and dates of birth, which TSA stated are required to minimize misidentifications.

TSA is implementing a new screening program that the agency states will have the capability to screen an individual against the entire watch list.[20] Under this program, called Secure Flight, TSA will assume from air carriers the responsibility of

---

tional Security Staff" supporting all White House policy-making activities relating to international, transnational, and homeland security matters. The Homeland Security Council was maintained as the principle venue for interagency deliberations on issues that affect the security of the homeland, such as terrorism, weapons of mass destruction, natural disasters, and pandemic influenza.

[18] GAO–06–1031.

[19] GAO–08–110.

[20] GAO–09–292.

comparing passenger information against the No-Fly and Selectee lists.[21] According to the program's final rule, in general, Secure Flight is to compare passenger information only to the No-Fly and Selectee lists.[22] The supplementary information accompanying the rule notes that this will be satisfactory to counter the security threat during normal security circumstances. However, the rule provides that TSA may use the larger set of watch list records when warranted by security considerations, such as if TSA learns that flights on a particular route may pose increased risks. TSA emphasized that use of the full terrorist screening database is not routine. Rather, TSA noted that its use is limited to circumstances in which there is information concerning an increased risk to transportation security, and the decision to use the full watch list database will be based on circumstances at the time. According to TSA, as of January 2010, the agency was developing administrative procedures for utilizing the full watch list when warranted.

In late January 2009, TSA began to assume from airlines the watch list matching function for a limited number of domestic flights, and has since phased in additional flights and airlines. TSA expects to assume the watch list matching function for all domestic and international flights departing to and from the United States by December 2010. It is important to note that under the Secure Flight program, TSA requires airlines to provide the agency with each passenger's full name and date of birth to facilitate the watch list matching process, which should reduce the number of individuals who are misidentified as the subject of a watch list record. We continue to monitor the Secure Flight program at the Congress's request.

In our October 2007 watch list report, we recommended that the FBI and DHS assess the extent to which security risks exist by not screening against certain watch list records and what actions, if any, should be taken in response.[23] The agencies generally agreed with our recommendations but noted that the risks related to not screening against all watch list records needs to be balanced with the impact of screening against all records, especially those records without a full name and other identifiers. For example, more individuals could be misidentified, law enforcement would be put in the position of detaining more individuals until their identities could be resolved, and administrative costs could increase, without knowing what measurable increase in security is achieved. While we acknowledge these tradeoffs and potential impacts, we maintain that assessing whether vulnerabilities exist by not screening against all watch list records—and if there are ways to limit impacts—is critical and could be a relevant component of the Government's on-going review of the watch list process. Therefore, we believe that our recommendation continues to have merit.

*Identifying Additional Screening Opportunities and Determining Whether There Are Clear Lines of Authority for and Accountability Over the Watch List Process Would Help Ensure Its Effective Use*

As we reported in October 2007, the Federal Government has made progress in using the consolidated terrorist watch list for screening purposes, but has additional opportunities to use the list. For example, DHS uses the list to screen employees in some critical infrastructure components of the private sector, including certain individuals who have access to vital areas of nuclear power plants or transport hazardous materials. However, many critical infrastructure components are not using watch list records, and DHS has not finalized guidelines to support such private sector screening, as HSPD–6 mandated and we previously recommended.[24]

In that same report, we noted that HSPD–11 tasked the Secretary of Homeland Security with coordinating across other Federal departments to develop: (1) A strategy for a comprehensive and coordinated watchlisting and screening approach and (2) a prioritized implementation and investment plan that describes the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of necessary activities.[25] We reported that without such a strategy, the Government could not provide accountability and a basis for monitoring to ensure that: (1) The intended goals for, and expected results of, terrorist screening are being achieved and (2) use of the watch list is consistent with privacy and civil lib-

[21] Pub. L. No. 108–458, 4012(a), 118 Stat. 3638, 3714–15 (codified at 49 U.S.C. § 44903(j)(2)(C)).

[22] See 73 Fed. Reg. 64,018 (Oct. 28, 2008) (codified at 49 C.F.R. pt. 1560).

[23] GAO–08–110.

[24] The identification of critical infrastructure components that are not using watch list records for screening is considered Sensitive Security Information that cannot be disclosed in a public statement.

[25] The White House, *Homeland Security Presidential Directive/HSPD–11, Subject: Comprehensive Terrorist-Related Screening Procedures* (Washington, DC, Aug. 27, 2004).

erties. We recommended that DHS develop a current interagency strategy and related plans.

According to DHS's Screening Coordination Office, during the fall of 2007, the office led an interagency effort to provide the President with an updated report, entitled, *HSPD–11, An Updated Strategy for Comprehensive Terrorist-Related Screening Procedures.*[26] The office noted that the report was formally submitted to the Executive Office of the President through the Homeland Security Council and reviewed by the President on January 25, 2008. Further, the office noted that it also provided a sensitive version of the report to the Congress in October 2008. DHS provided us an excerpt of that report to review, stating that it did not have the authority to share excerpts provided by other agencies, and we were unable to obtain a copy of the full report. The information we reviewed only discussed DHS's own efforts for coordinating watch list screening across the Department. Therefore, we were not able to determine whether the HSPD–11 report submitted to the President addressed all of the components called for in the directive or what action, if any, was taken as a result. We maintain that a comprehensive strategy, as well as related implementation and investment plans, as called for by HSPD–11, continue to be important to ensure effective Government-wide use of the watch list process.

In addition, in our October 2007 report, we noted that establishing an effective governance structure as part of this strategic approach is particularly vital since numerous agencies and components are involved in the development, maintenance, and use of the watch list process, both within and outside of the Federal Government. Also, establishing a governance structure with clearly-defined responsibility and authority would help to ensure that agency efforts are coordinated, and that the Federal Government has the means to monitor and analyze the outcomes of such efforts and to address common problems efficiently and effectively. We determined at the time that no such structure was in place and that no existing entity clearly had the requisite authority for addressing interagency issues. We recommended that the Homeland Security Council ensure that a governance structure was in place, but the council did not comment on our recommendation.

At the time of our report, TSC stated that it had a governance board in place, comprised of senior-level agency representatives from numerous departments and agencies. However, we also noted that the board provided guidance concerning issues within TSC's mission and authority. We also stated that while this governance board could be suited to assume more of a leadership role, its authority at that time was limited to TSC-specific issues, and it would need additional authority to provide effective coordination of terrorist-related screening activities and interagency issues Government-wide. In January 2010, the FBI stated that TSC has a Policy Board in place, with representatives from relevant departments and agencies, that reviews and provides input to the Government's watch list policy. The FBI also stated that the policies developed are then sent to the National Security Council Deputies Committee (formerly the Homeland Security Council) for ratification. The FBI noted that this process was used for making the most recent additions and changes to watch list standards and criteria. We have not yet been able to determine, however, whether the Policy Board has the jurisdiction and authority to resolve issues beyond TSC's purview, such as issues within the intelligence community and in regard to the nominations process, similar to the types of interagency issues the December 25 attempted attack identified. We maintain that a governance structure with the authority for and accountability over the entire watch list process, from nominations through screening, and across the Government is important.

On January 7, 2010, the President tasked the National Security Staff with initiating an interagency review of the watch list process—including the business processes, procedures, and criteria—and the interoperability and sufficiency of supporting information technology systems. This review offers the Government an opportunity to develop an updated strategy, related plans, and governance structure that would provide accountability to the administration, the Congress, and the American public that the watch list process is effective at helping to secure the homeland.

---

[26] DHS established the Screening Coordination Office in July 2006 to enhance security measures by integrating the Department's terrorist-and immigration-related screening efforts, creating unified screening standards and policies, and developing a single redress process for travelers.

RECENT WORK HIGHLIGHTS THE IMPORTANCE OF CONDUCTING VULNERABILITY ASSESSMENTS AND OPERATIONAL TESTING PRIOR TO DEPLOYMENT OF NEW CHECKPOINT TECHNOLOGIES

*While TSA Has Not Yet Deployed Any New Checkpoint Technologies Nationwide, It Plans to Have Installed Almost 200 AITs by the End of 2010*

As we reported in October 2009, in an effort to improve the capability to detect explosives at aviation passenger checkpoints, TSA has 10 passenger screening technologies in various phases of research, development, procurement, and deployment, including the AIT (formerly Whole Body Imager).[27] TSA is evaluating the AIT as an improvement over current screening capabilities of the metal detector and pat-downs specifically to identify nonmetallic threat objects and liquids. The AITs produce an image of a passenger's body that a screener interprets. The image identifies objects, or anomalies, on the outside of the physical body but does not reveal items beneath the surface of the skin, such as implants. TSA plans to procure two types of AIT units: One type uses millimeter wave and the other type uses backscatter X-ray technology. Millimeter wave technology beams millimeter wave radio frequency energy over the body's surface at high speed from two antennas simultaneously as they rotate around the body.[28] The energy reflected back from the body or other objects on the body is used to construct a three-dimensional image. Millimeter wave technology produces an image that resembles a fuzzy photo negative. Backscatter X-ray technology uses a low-level X-ray to create a two-sided image of the person. Backscatter technology produces an image that resembles a chalk etching.[29]

As we reported in October 2009, TSA has not yet deployed any new technologies Nation-wide. However, as of December 31, 2009, according to a senior TSA official, the agency has deployed 40 of the millimeter wave AITs, and has procured 150 backscatter X-ray units in fiscal year 2009 and estimates that these units will be installed at airports by the end of calendar year 2010. In addition, TSA plans to procure an additional 300 AIT units in fiscal year 2010, some of which will be purchased with funds from the American Recovery and Reinvestment Act of 2009.[30] TSA plans to procure and deploy a total of 878 units at all category X through category IV airports.[31] Full operating capability is expected in fiscal year 2014. TSA officials stated that the cost of the AIT is about $130,000 to $170,000 per unit, excluding installation costs. In addition, the estimated training costs are $50,000 per unit.

While TSA stated that the AIT will enhance its explosives detection capability, because the AIT presents a full body image of a person during the screening process, concerns have been expressed that the image is an invasion of privacy. According to TSA, to protect passenger privacy and ensure anonymity, strict privacy safeguards are built into the procedures for use of the AIT. For example, the officer who assists the passenger never sees the image that the technology produces, and the officer who views the image is remotely located in a secure resolution room and never sees the passenger. Officers evaluating images are not permitted to take cameras, cell phones, or photo-enabled devices into the resolution room. To further protect passengers' privacy, ways have been introduced to blur the passengers' images. The millimeter wave technology blurs all facial features, and the backscatter X-ray technology has an algorithm applied to the entire image to protect privacy. Further, TSA has stated that the AIT's capability to store, print, transmit, or save the image will be disabled at the factory before the machines are delivered to airports, and each image is automatically deleted from the system after it is cleared by the remotely located security officer. Once the remotely located officer determines that threat items are not present, that officer communicates wirelessly to the officer assisting the passenger. The passenger may then continue through the security process. Potential threat items are resolved through a direct physical pat-down before

[27] GAO–10–128.

[28] According to TSA, this description of the millimeter wave technology applies only to the machine manufactured by L3 and does not apply to other millimeter wave technologies that TSA is evaluating, such as the Smiths millimeter wave AIT.

[29] Research and development of the AIT technology is continuing, specifically, to develop passive terahertz (THz) and active gigahertz (GHz) technologies to improve detection performance and reduce operational costs of commercially available systems.

[30] According to TSA, some of the 300 AIT units to be procured in fiscal year 2010 will begin to be deployed to airports in the latter half of fiscal year 2010.

[31] TSA classifies the commercial airports in the United States into one of five security risk categories (X, I, II, III, and IV). In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest. Categories X, I, II, and III airports account for more than 90 percent of the Nation's air traffic.

the passenger is cleared to enter the sterile area.[32] In addition to privacy concerns, the AITs are large machines, and adding them to the checkpoint areas will require additional space, especially since the operators are segregated from the checkpoint to help ensure passenger privacy.

*TSA Reports That It Is Taking Steps to Operationally Test AITs but Has Not Conducted Vulnerability Assessments*

We previously reported on several challenges TSA faces related to the research, development, and deployment of passenger checkpoint screening technologies and made a number of recommendations to improve this process.[33] Two of these recommendations are particularly relevant today, as TSA moves forward with plans to install a total of 878 additional AITs—completing operational testing of technologies in airports prior to using them in day-to-day operations and assessing whether technologies such as the AIT are vulnerable to terrorist countermeasures, such as hiding threat items on various parts of the body to evade detection.

First, in October 2009, we reported that TSA had relied on technologies in day-to-day airport operations that had not been proven to meet their functional requirements through operational testing and evaluation, contrary to TSA's acquisition guidance and a knowledge-based acquisition approach. We also reported that TSA had not operationally tested the AITs at the time of our review, and we recommended that TSA operationally test and evaluate technologies prior to deploying them.[34] In commenting on our report, TSA agreed with this recommendation. A senior TSA official stated that although TSA does not yet have a written policy requiring operational testing prior to deployment, TSA is now including in its contracts with vendors that checkpoint screening machines are required to successfully complete laboratory tests as well as operational tests. The test results are then incorporated in the source selection plan. The official also stated that the test results are now required at key decision points by DHS's Investment Review Board. While recently providing GAO with updated information to our October 2009 report, TSA stated that operational testing for the AIT was completed as of the end of calendar year 2009. We are in the process of verifying that TSA has tested all of the AIT's functional requirements in an operational environment.

Deploying technologies that have not successfully completed operational testing and evaluation can lead to cost overruns and underperformance. TSA's procurement guidance provides that testing should be conducted in an operational environment to validate that the system meets all functional requirements before deployment. In addition, our reviews have shown that leading commercial firms follow a knowledge-based approach to major acquisitions and do not proceed with large investments unless the product's design demonstrates its ability to meet functional requirements and be stable.[35] The developer must show that the product can be manufactured within cost, schedule, and quality targets and is reliable before production begins and the system is used in day-to-day operations.

TSA's experience with the ETPs, which the agency uses for secondary screening, demonstrates the importance of testing and evaluation in an operational environment. The ETP detects traces of explosives on a passenger by using puffs of air to dislodge particles from the passenger's body and clothing that the machine analyzes for traces of explosives. TSA procured 207 ETPs and in 2006 deployed 101 ETPs to 36 airports, the first deployment of a checkpoint technology initiated by the agency.[36] TSA deployed the ETPs even though agency officials were aware that tests conducted during 2004 and 2005 on earlier ETP models suggested that they did not demonstrate reliable performance. Furthermore, the ETP models that were subsequently deployed were not first tested to prove their effective performance in an operational environment, contrary to TSA's acquisition guidance, which recommends such testing. As a result, TSA procured and deployed ETPs without assurance that they would perform as intended in an operational environment. TSA officials stated that they deployed the machines without resolving these issues to respond quickly to the threat of suicide bombers. In June 2006, TSA halted further deployment of

[32] TSA stated that it continues to evaluate possible display options that include a "stick figure" or "cartoonlike" form to provide greater privacy protection to the individual being screened while still allowing the unit operator or automated detection algorithms to detect possible threats.

[33] GAO–10–128.

[34] Operational testing refers to testing in an operational environment in order to verify that new systems are operationally effective, supportable, and suitable.

[35] GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition,* GAO–04–386SP (Washington, DC: January 2004).

[36] TSA deployed the ETPs from January to June 2006. Since June 2006, TSA removed all but 9 ETPs from airports because of maintenance issues.

the ETP because of performance, maintenance, and installation issues. According to a senior TSA official, as of December 31, 2009, all but 9 ETPs have been withdrawn from airports and 18 ETPs remain in inventory. TSA estimates that the 9 remaining ETPs will be removed from airports by the end of calendar year 2010. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security. Furthermore, retaining existing screening procedures until the effectiveness of future technologies has been validated could provide assurances that use of checkpoint technologies improves aviation security.

Second, as we reported in October 2009, TSA does not know whether its explosives detection technologies, such as the AITs, are susceptible to terrorist tactics. Although TSA has obtained information on vulnerabilities at the screening checkpoint, the agency has not assessed vulnerabilities—that is, weaknesses in the system that terrorists could exploit in order to carry out an attack—related to passenger screening technologies, such as AITs, that are currently deployed. According to TSA's threat assessment, terrorists have various techniques for concealing explosives on their persons, as was evident in Mr. Abdulmutallab's attempted attack on December 25, where he concealed an explosive in his underwear. However, TSA has not assessed whether these and other tactics that terrorists could use to evade detection by screening technologies, such as AIT, increase the likelihood that the screening equipment would not detect the hidden weapons or explosives. Thus, without an assessment of the vulnerabilities of checkpoint technologies, it is unclear whether the AIT or other technologies would have been able to detect the weapon Mr. Abdulmutallab used in his attempted attack. TSA is in the process of developing a risk assessment for the airport checkpoints, but the agency has not yet completed this effort or clarified the extent to which this effort addresses any specific vulnerabilities in checkpoint technology.

TSA officials stated that to identify vulnerabilities at airport checkpoints, the agency analyzes information such as the results from its covert testing program. TSA conducts National and local covert tests, whereby individuals attempt to enter the secure area of an airport through the passenger checkpoint with prohibited items in their carry-on bags or hidden on their persons. However, TSA's covert testing programs do not systematically test passenger and baggage screening technologies Nation-wide to ensure that they identify the threat objects and materials the technologies are designed to detect, nor do the covert testing programs identify vulnerabilities related to these technologies. We reported in August 2008 that while TSA's local covert testing program attempts to identify test failures that may be caused by screening equipment not working properly or caused by screeners and the screening procedures they follow, the agency's National testing program does not attribute a specific cause of a test failure.[37] We recommended, among other things, that TSA require the documentation of specific causes of all National covert testing failures, including documenting failures related to equipment, in the covert testing database to help TSA better identify areas for improvement. TSA concurred with this recommendation and stated that the agency will expand the covert testing database to document test failures related to screening equipment.

In our 2009 report, we also recommended that the Assistant Secretary for TSA, among other actions, conduct a complete risk assessment—including threat, vulnerability, and consequence assessment—for the passenger screening program and incorporate the results into TSA's program strategy, as appropriate. TSA and DHS concurred with our recommendation, but have not completed these risk assessments or provided documentation to show how they have addressed the concerns raised in our 2009 report regarding the susceptibility of the technology to terrorist tactics.

Mr. Chairman, this concludes our statement for the record.

---

STATEMENT OF THE AMERICAN CIVIL LIBERTIES UNION

JANUARY 27, 2010

Chairman Thompson, Ranking Member King, and Members of the committee: The American Civil Liberties Union (ACLU) has more than half a million members, countless additional activists and supporters, and 53 affiliates Nation-wide. 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

[37] See GAO, *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests,* GAO–08–958 (Washington, DC: Aug. 8, 2008).

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 changes greatly infringe on civil liberties and face serious questions regarding their 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.

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.

---

[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.

*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.

*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]

---

[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.*
[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.

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 watch list 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 watch list, contrary to FBI policy. We also found that 78 percent of the initial watch list nominations we reviewed were not processed in established FBI timeframes.

"Additionally, in 67 percent of the cases that we reviewed in which a watch list record modification was necessary, we determined that the FBI case agent primarily assigned to the case failed to modify the watch list 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 watch list as required by FBI policy. Finally, in 72 percent of the closed cases reviewed, the FBI failed to remove the subject in a timely manner."[13]

This is only the latest in a long string of Government reports describing the failure of the terror watch lists.[14] In order to be an effective tool against terrorism these lists must shrink dramatically with names limited to only those for whom there is credible evidence of terrorist ties or activities.

*Aviation Screening on the Basis of Nationality*

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

Noted security expert Bruce Schneier stated recently:

"[A]utomatic profiling based on name, nationality, method of ticket purchase, and so on . . . makes us all less safe. The problem with automatic profiling is that it doesn't work.

"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.

---

[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.

"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.

*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

---

[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.*

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 on-going 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. Other individuals who are either on a list or mistaken for those on the list include a former Assistant Attorney General, many individuals with the name Robert Johnson, the late Senator Edward Kennedy and even Nelson Mandela.[20]

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

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 on-going 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.

---

[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*.

[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*.

*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. Long-standing 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 United States than the United Kingdom, the authors cited the diversity of American communities and the greater protection of civil rights as key factors.

At the January 7, 2009 White House briefing regarding the security failures surrounding the Christmas attack, DHS Secretary Janet Napolitano raised a question about "counterradicalization."[25] She asked, "How do we communicate better American values and so forth, in this country but also around the globe?" Of course the Secretary should know American values are communicated through U.S. Government policies, which is why adopting openly discriminatory policies can be so damaging and counterproductive to our National interests.

## IV. CONCLUSION

Ultimately security is never absolute and never will be. It is not wise security policy to spend heavily to protect against one particular type of plot, when the number of terrorist ideas that can be hatched—not only against airlines, but also against other targets—is limitless. The President has identified a failure "connect the dots" by intelligence analysts as the main reason that Umar Farouk Abdulmutallab was able to board a flight to the United States.[26] We must not lose sight of that reality. Limited security dollars should be invested where they will do the most good and have the best chance of thwarting attacks. That means investing them in developing competent intelligence and law enforcement agencies that will identify specific individuals who represent a danger to air travel and arrest them or deny them a visa.

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

---

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

[25] Briefing by Homeland Security Secretary Napolitano, Assistant to the President for Counterterrorism and Homeland Security Brennan, and Press Secretary Gibbs, 1/7/10, at: *http://www.whitehouse.gov/the-pressoffice/briefing-homeland-security-secretary-napolitano-assistant-president-counterterroris[sic].*

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

**STATEMENT OF JANE HOLL LUTE, DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY**

Ms. LUTE. Good morning, Mr. Chairman, Ranking Member King, Members of the committee. Thank you for this opportunity to testify on the attempted attack on December 25.

Secretary Napolitano, Mr. Chairman, as you noted, was scheduled to be out of the country. In view of that, although her plans have changed, we have been in touch with your staff that I would be here to testify for the Department.

As President Obama made clear immediately following the attack, at the Department of Homeland Security and across the Federal Government, we are determined to find and fix the vulnerabilities that led to this breach.

Protecting the United States against terrorism calls upon the expertise and authority of multiple agencies and many partners. In addition to the men and women of the Department of Homeland Security, this includes the efforts of the departments of State, Defense, Justice, FBI, NCTC, and the broader intelligence community. It also importantly includes our State and local law enforcement agencies and our international partners and allies around the world.

I am very pleased this morning to be joined by my colleagues from the Department of State and the National Counterterrorism Center.

As this committee is well aware of, Mr. Chairman, boarding the plane means fulfilling three basic requirements. The individual must retain proper documentation, including a passport, visa, or other travel authorization, a ticket, and boarding pass. He or she must pass through the checkpoint screening to ensure that they are not concealing a dangerous weapon or other dangerous material on their person or in their baggage.

Finally, the individual must be cleared through a pre-flight screening process that seeks to determine if that individual poses a threat to the homeland security and thus should be denied permission to fly.

Within this set of requirements, let me briefly describe the specific role the Department of Homeland Security plays. First, to conduct pre-flight screening, the Department is one of the principal consumers of intelligence gathered by other agencies, including the terrorist watch list, which includes the No-Fly list. DHS checks passengers against these lists to keep potential terrorists from boarding flights and to identify travelers who should undergo additional screening.

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

Third, outside of the United States, the Department works with foreign governments and airlines to advise them on the required security measures for flights bound for the United States and on which passengers may prove a threat. TSA nor any other part of the Department, however, does not screen people or baggage at international airports.

Let me say emphatically, as the President of the United States has said and as the Secretary of Homeland Security has said, that with regard to the attempted attack on December 25, Omar Farouk Abdulmutallab should never have been allowed to board a U.S.-bound airplane with explosives. As Secretary Napolitano has detailed in recent weeks, DHS has implemented numerous steps and is working closely with our Federal partners to fix the vulnerabilities that led to the attempted attack.

As a consumer or a terrorist watch list information, the Department works closely with the FBI, with the Office of the Director of National Intelligence and NCTC to improve our ability to connect and assimilate intelligence. We are also taking steps to strengthen standards for international aviation screening and bolstering international partnerships to guard against a similar type of attack.

But to be clear, Abdulmutallab was not on the No-Fly list and hence, did not come to our attention prior to his boarding the flight in Amsterdam. His presence on this list would have flagged him to be prevented from boarding. He was not either on the Selectee list, which would have flagged him for secondary screening. Furthermore, the physical screenings that were performed by foreign authorities at the airports in Nigeria and the Netherlands failed to detect the explosive on his person.

Immediately following the attempted attack, the Department took steps to secure incoming and future flights. We directed the FAA to alert all 128 flights inbound to the United States from Europe of the situation. We increased security measures at domestic airports. We implemented an enhanced screening for all international flights coming into the United States, and we reached out to State and local law enforcement, air carriers, international partners, and relevant agencies to provide information they needed on the ground to take appropriate measures.

In January 3, Secretary Napolitano dispatched me and my colleagues in the Department to meet with international leadership on the crisis in aviation security that was illustrated through the events of 12/25. We met with senior officials from 11 countries, plus the European Union, to discuss ways to strengthen aviation security, and we are determined to follow through on these contacts. I can report, as questioned, Mr. Chairman, on the results of those discussions.

The Secretary has herself been in touch with international colleagues to identify ways to strengthen the international aviation security standards and procedures.

As the Secretary said last week, and as the President has said, there are no 100 percent guarantees against another terrorist attempt to take down a plane or attack us in some other fashion. But what we can give you, Mr. Chairman, is the 100 percent commitment of the Secretary, myself, Department leadership, and the hundreds of thousands of men and women who work in homeland security to do everything we can to minimize the risk of terrorist attack.

Thank you again for this opportunity, Mr. Chairman, to appear before this committee. I look forward to your questions.

[The statement of Ms. Lute follows:]

PREPARED STATEMENT OF JANE HOLL LUTE

JANUARY 27, 2010

Chairman Thompson, Ranking Member King, 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 watch list, 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 airports, and of air marshals in flight; and directing the FAA to notify the 128 flights already in-bound 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 watch list 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 attack on December 25, and how we are moving forward to further bolster aviation security.

DHS' ROLE IN MULTIPLE LAYERS OF DEFENSE

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

DHS oversees several programs to prevent individuals with terrorist ties from boarding flights that are headed to, within, or traveling over the United States or, in appropriate cases, to identify them for additional screening. Specifically, DHS uses information held in the Terrorist Screening Database (TSDB), a resource managed by the Terrorist Screening Center (TSC), as well as other information provided through the intelligence community, to screen individuals; operates the travel authorization program for people who are traveling to the United States under the Visa Waiver Program (VWP);[1] and works with foreign governments, international, and regional organizations, and airlines to design and implement improved security standards worldwide. This includes routine checks against Interpol databases on

[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 United Kingdom, only citizens with an unrestricted right of permanent abode in the United Kingdom are eligible for VWP travel authorizations).

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 United States 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.

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 watch list matches and immediately trigger law enforcement notification and coordination.

---

[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.

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

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

*Checkpoint Screenings and In-Flight Security*

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

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

In an effort to enhance international screening standards, TSA conducts security assessments in accordance with security standards established by the International Civil Aviation Organization (ICAO) at more than 300 foreign airports, which include foreign airports from which flights operate directly to the United States and all airports from which U.S. air carriers operate. If an airport does not meet these standards, TSA works with the host government to rectify the deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues.

In long-term circumstances of non-compliance with international standards, TSA may recommend suspension of flight service from these airports to the United States. In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level. If an airport is located within one of the 35 VWP countries, DHS conducts additional audits and inspections as part of the statutorily mandated VWP designation and review process.

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

DHS RESPONSE TO THE ATTEMPTED DECEMBER 25 ATTACK

The facts of the December 25 attempted bombing are well established and were relayed in the report on the incident that the President released on 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 United States, which mandated enhanced screening prior to departure and additional security measures during flight.

From the first hours following the attempted attack, Secretary Napolitano worked closely with the President, senior Department leadership, and agencies across the Federal Government. Secretary Napolitano and I communicated with international partners and Members of Congress. The Secretary also engaged in dialogue with State and local leadership, the aviation industry, and 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, Secretary Napolitano dispatched me 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 total, we met with senior officials from 11 countries, plus the European Union in order to discuss new ways to bolster collective tactics for improving global aviation security. Last week, Secretary Napolitano travelled to Spain to meet with her European Union counterparts in the first of a series of global meetings intended to bring about broad consensus on new, stronger, and more consistent international aviation security standards and procedures.

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

close contact with all of these partners since the attempted attack, and will continue to do so.

On January 3, TSA issued a new Security Directive, effective on January 4, mandating enhanced passenger screening.

STEPS FORWARD TO IMPROVE AVIATION SECURITY

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. On January 7, Secretary Napolitano was joined by 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 watch list, 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 watch list system.

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

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

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

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

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

CONCLUSION

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.

As Secretary Napolitano said last week, there is no 100 percent guarantee that we can prevent a terrorist from trying to take down a plane or attack us in some other fashion. That is not the nature of the world we live in, nor of the threats that we face. What we can give you, however, is the 100 percent commitment of the Sec-

retary, myself, DHS leadership, and the entire DHS enterprise to do everything we can to minimize the risk of terrorist attacks.

Chairman Thompson, Representative King, and Members of the committee: Thank you for this opportunity to testify. I am happy to answer any questions you may have.

Chairman THOMPSON. Thank you for your testimony, Dr. Lute.

I now recognize Under Secretary Kennedy to summarize his statement for 5 minutes.

**STATEMENT OF PATRICK F. KENNEDY, UNDER SECRETARY, MANAGEMENT, DEPARTMENT OF STATE**

Mr. KENNEDY. Thank you, sir. Chairman Thompson, Ranking Member King, distinguished Members of the committee, thank you for the opportunity to appear before you today.

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

This introspective review and the concurrent interagency review are on-going. We appreciate this committee's interest and support as we continue this review process, noting in particular the recent committee staff visit to our consular facility in London. We recognize the gravity of the threat we face, and we consider ourselves the first line of defense in our National security efforts. We acknowledge that processes need to be improved, and here are the steps we have already taken.

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

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

New watchlisting information coming from the intelligence and law enforcement community is continually checked every day against the database of previously issued visas. We can and do revoke visas and circumstances where an immediate threat is recognized. We can and do revoke visas to the point of people seeking to board aircraft, preventing their boarding in coordination with the FBI's National Targeting Center. We revoke visas under these circumstances almost daily. We are standardizing procedures for triggering revocations from the field and are adding revocation recommendations to the Visas Viper report.

At the same time, expeditious coordination with our National security partners is not to be underestimated. There have been numerous cases where a State Department unilateral and uncoordinated revocation would have disrupted important investigations that were under way by one of our National security partners.

The individual involved was under active investigation, and our revocation action would have disclosed the United States Government's interest in that individual and ended our National security colleague's ability to pursue the case and identify terrorist plans and co-conspirators.

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

The State Department has close and productive relationships with our interagency partners, particularly with the Department of Homeland Security, which has statutory authority for visa policy. The State Department brings unique assets and capabilities to this partnership. Our global presence, international expertise, and highly trained personnel provide us singular advantages in supporting the visa function throughout the world.

We developed and implemented intensive screening processes requiring personal interviews and supported by a sophisticated global information network. This front line of border security has visa offices in virtually every country of the world and are staffed by highly trained, multilingual, culturally aware personnel of the State Department.

We support them with the latest technology and access to enhanced screening tools and information systems. We are introducing a new generation of visa software to more efficiently manage our growing mission and the increasing amounts of data we handle. We are pioneers in the use of biometrics, a leader in the field of facial recognition, and we are expanding into the field of iris screening. We have and will continue to automate processes to reduce the possibility of human error.

The State Department makes all visa information available to other agencies, giving them immediate access to over 13 years of data. We introduced on-line visa applications in 2009, which expanded our data collection tenfold and provide new information readily available for analysis by the State Department and by other agencies. This system is being rolled out worldwide in a few months.

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

At the same time we believe that U.S. interests in legitimate trade, travel, and educational exchanges are not in opposition to border security. In fact, the United States must strive to meet both goals to guarantee our long-term security.

Again, the multi-agency team effort to which each agency brings its particular strengths and expertise results in a robust and secure process, a process based on broadly shared information. We re-

main fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information.

We fully recognize that we are not perfect in our reporting in connection with this case. However, we are working and will continue to work not only to address shortcomings, but to continually enhance our border security screening capabilities and the contributions we make to this interagency effort.

Thank you very much, Mr. Chairman. I look forward to your questions.

[The statement of Mr. Kennedy follows:]

PREPARED STATEMENT OF PATRICK F. KENNEDY

JANUARY 27, 2010

Chairman Thompson, Ranking Member King and distinguished Members of the committee, thank you for the opportunity to address you today. As a result of the attempted terrorist attack on Flight 253, the President ordered corrective steps to address systemic failures in procedures we use to protect the people of the United States. Secretary Clinton reiterated this direction when she stated, "we all are looking hard at what did happen in order to improve our procedures to avoid human errors, mistakes, oversights of any kind. We in the State Department are fully committed to accepting our responsibility for the mistakes that were made, and we're going to be working hard with the rest of the Administration to improve every aspect of our efforts." Therefore, the Department of State now is working on reviewing visa issuance and revocation criteria and determining how technological enhancements can facilitate and strengthen visa-related business processes.

Our immediate attention is on addressing the deficiencies identified following the attempted attack on Flight 253. At the same time we continue to plan for the future, incorporating new technology, increasing data sharing and enhancing operational cooperation with partner agencies. We have a record of quickly adapting and improving our procedures to respond to security imperatives. We have a highly trained global team working daily to protect our borders and fulfill the overseas border security mission and other critical tasks ranging from crisis management to protection of American interests abroad. Within the Department we have a dynamic partnership between the Bureau of Consular Affairs and the Bureau of Diplomatic Security that adds a valuable law enforcement and investigative component to our capabilities. We will use these strengths to address the continuing security threats.

In the case of Umar Farouk Abdulmutallab, on the day following his father's November 19 visit to the Embassy, we sent a cable to the Washington intelligence and law enforcement community through proper channels (the Visas Viper system) that "Information at post suggests [that Farouk] may be involved in Yemeni-based extremists." At the same time, the Consular Section entered Abdulmutallab into the Consular Lookout and Support System database known as CLASS. In sending the Visas Viper cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, but entered it correctly into CLASS. As a result of the misspelling in the cable, information about previous visas issued to him and the fact that he currently held a valid U.S. visa was not included in the cable. At the same time the CLASS entry resulted in a lookout using the correct spelling that was shared automatically with the primary lookout system used by the Department of Homeland Security (DHS) and accessible to other agencies.

We have taken immediate action to improve the procedures and content requirements for Visas Viper cable reporting that will call attention to the visa application and issuance material that is already in the data that we share with our National security partners. All officers have been instructed to include complete information about all previous and current U.S. visa(s). This guidance includes specific methods to comprehensively and intensively search the database of visa records so that all pertinent information is obtained.

In addition to this change in current procedures to search visa records, we immediately began working to refine the capability of our current systems. When dealing with applications for visas, we employ strong, sophisticated name searching algorithms to ensure matches between names of visa applicants and any derogatory information contained in the 27 million records found in CLASS. This strong searching capability has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We will use

our significant experience with search mechanisms for derogatory information to improve the systems for checking our visa issuance records.

The Department of State has been matching new threat information with our records of existing visas since 2002. We have long recognized this function as critical to the way we manage our records and processes. This system of continual vetting has evolved as post-9/11 reforms were instituted and is now performed by the Terrorist Screening Center (TSC). All records added to the Terrorist Screening Database are checked against the Department's Consolidated Consular Database (CCD) to determine if there are matching visa records. Matches are sent electronically from the TSC to the Department of State to flag cases for visa revocation. In almost all such cases, visas are revoked. In addition, we have widely disseminated our data to other agencies that may wish to learn whether a subject of interest has a U.S. visa. Cases for revocation consideration are forwarded to us by DHS/Customs and Border Protection's (CBP) National Targeting Center (NTC) and other entities. Almost every day, we receive requests to review and, if warranted, revoke visas for potential travelers for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours per day/7 days per week to work these issues. Many of these requests are urgent because the person is about to board a plane. The State Department then uses its authority to prudentially revoke the visa.

Since the Presidentially-ordered Security Review, there have been changes in the thresholds for adding individuals to the Terrorist Screening Database, No-Fly, and Selectee lists. The number of revocations has increased substantially as a result. This revocation work is processed electronically in the Department. As soon as information is established to support a revocation, an entry showing the visa revocation is added electronically to the Department of State's lookout system and shared in real time with the DHS lookout systems used for border screening.

In addition to these changes, the Department is reviewing the procedures and criteria used in the field to revoke visas and will issue new instructions to our officers. Revocation recommendations will be added as an element of reporting through the Visas Viper channel. We will be reiterating our guidance on use of the broad discretionary authority of visa officers to deny visas on security and other grounds. Instruction in appropriate use of this authority has been a fundamental part of officer training for several years.

The State Department has broad and flexible authority to revoke visas and we use that authority widely to protect our borders. Since 2001, we have revoked 51,000 visas for a variety of reasons, including over 1,700 for suspected links to terrorism. We have been actively using this authority as we perform internal scrubs of our data with watch list information provided by partner agencies. For example, we are re-examining information in our CLASS database on individuals with potential connections to terrorist activity or support for such activity. We are reviewing all previous Visas Viper submissions as well as cases that other agencies are bringing to our attention from the No-Fly and Selectee lists, as well as other sources. In these reviews, we have identified cases for revocation and we have also confirmed that substantial numbers of individuals in these classes hold no visas and of those few who did, many were revoked prior to the current review. We recognize the gravity of the threat we face and are working intensely with our colleagues from other agencies to ensure that when the U.S. Government obtains information that a person may pose a threat to our security, that person does not hold a visa.

We will use revocation authority prior to interagency consultation in circumstances where we believe there is an immediate threat. Revocation is an important tool in our border security arsenal. At the same time, expeditious coordination with our National security partners is not to be underestimated. There have been numerous cases where our unilateral and uncoordinated revocation would have disrupted important investigations that were underway by one of our National security partners. They had the individual under investigation and our revocation action would have disclosed the U.S. Government's interest in the individual and ended our colleagues' ability to quietly pursue the case and identify terrorists' plans and co-conspirators.

In addition to revocation efforts, consular officers refused 1,885,017 visas in fiscal year 2009. We now are renewing guidance to our officers on their discretionary authority to refuse visas under section 214(b) of the Immigration and Nationality Act with specific reference to cases that raise security concerns. No visa is issued without it being run through security checks against our partners' data. And we screen applicants' fingerprints against U.S. databases as well.

The Department has a close and productive partnership with DHS, which has authority for visa policy. Over the past 7 years both agencies significantly increased resources, improved procedures, and upgraded systems devoted to supporting the

visa function. DHS receives all of the information collected by the Department of State during the visa process. DHS has broad access to our entire CCD, containing 136 million records related to both immigrant and nonimmigrant visas and covering visa actions of the last 13 years. Special extracts of data are supplied to elements within DHS, including the Visa Security Units of Immigration and Customs Enforcement (ICE). These extracts have been tailored to the specific requirements of those units. We are working closely with ICE Visa Security Units established abroad and with domestic elements of DHS, such as CBP's National Targeting Center.

We gave DHS access to U.S. passport records, used by CBP to confirm the identity of citizens returning to the United States. We developed new card-type travel documents that work with the automated systems CBP installed at the U.S. land borders. We are collecting more information electronically and earlier in the process. Expanded data collection done in advance of travel will give DHS and partner agencies richer information and more time for analysis.

We make all of our visa information available to other involved agencies, and we specifically designed our systems to facilitate comprehensive data sharing. We give other agencies immediate access to over 13 years of visa data, and they use this access extensively. In November 2009, more than 16,000 employees of DHS, the Department of Defense (DOD), the FBI and Commerce made 920,000 queries on visa records. We embrace a layered approach to border security screening and are fully supportive of the DHS Visa Security Program.

The Department of State is at the forefront of interagency cooperation and data sharing to improve border security, and we embarked on initiatives that will position us to meet future challenges while taking into consideration our partner agencies and their specific needs and requirements. We are implementing a new generation of visa processing systems that will further integrate information gathered from domestic and overseas activities. We are restructuring our information technology architecture to accommodate the unprecedented scale of information we collect and to keep us agile and adaptable in an age of intensive and growing requirements for data and data sharing.

We proactively expanded biometric screening programs and spared no effort to integrate this expansion into existing overseas facilities. In partnership with DHS and the FBI, we established the largest biometric screening process on the globe. We were a pioneer in the use of facial recognition techniques and remain a leader in operational use of this technology. In 2009 we expanded use of facial recognition from a selected segment of visa applications to all visa applications. We now are expanding our use of this technology beyond visa records. We are testing use of iris recognition technology in visa screening, making use of both identity and derogatory information collected by DOD. These efforts require intense on-going cooperation from other agencies. We successfully forged and continue to foster partnerships that recognize the need to supply accurate and speedy screening in a 24/7 global environment. As we implement process and policy changes, we are always striving to add value in both border security and in operational results. Both dimensions are important in supporting the visa process.

The Department of State is an integral player on the border security team. We are the first line of defense. Our global presence, foreign policy mission, and personnel structure give us singular advantages in executing the visa function throughout the world. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. National interests. The issuance and refusal of visas has a direct impact on foreign relations. Visa policy quickly can become a significant bilateral problem that harms U.S. interests if handled without consideration of foreign policy impacts. The conduct of U.S. visa policy has a direct and significant impact on the treatment of U.S. citizens abroad. The Department of State is in a position to anticipate and weigh those possibilities.

We developed and implemented intensive screening processes requiring personal interviews, employing analytic interview techniques, incorporating multiple biometric checks, all built around a sophisticated global information technology network. This frontline of border security has visa offices present in virtually every country of the world. They are staffed by highly trained and multi-lingual personnel of the Department of State. These officials are dedicated to a career of worldwide service and provide the cultural awareness, knowledge, and objectivity to ensure that the visa function remains the frontline of border security.

In addition, we have 145 officers and 540 locally employed staff devoted specifically to fraud prevention and document security, including fraud prevention officers at overseas posts. We have a large Fraud Prevention Programs office in Washington, DC that works very closely with the Bureau of Diplomatic Security, and we have fraud screening operations using sophisticated database checks at both the Ken-

tucky Consular Center and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging applications and applicants who lack credibility, who present fraudulent documents, or who give us false information adds a valuable dimension to our visa process.

The Bureau of Diplomatic Security adds an important law enforcement element to the Department's visa procedures. There are now 50 Assistant Regional Security Officer Investigators abroad specifically devoted to maintaining the integrity of the process. They are complemented by officers working domestically on both visa and passport matters. These Diplomatic Security officers staff a unit within the Bureau of Consular Affairs that monitors overseas visa activities to detect risks and vulnerabilities. These highly trained law enforcement professionals add another dimension to our border security efforts.

The multi-agency team effort on border security, based upon broadly shared information, provides a solid foundation. At the same time we remain fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information. We have and we will continue to automate processes to reduce the possibility of human error. We fully recognize that we were not perfect in our reporting in connection with the attempted terrorist attack on Flight 253. We are working and will continue to work not only to address that mistake but to continually enhance our border security screening capabilities and the contributions we make to the interagency effort.

We believe that U.S. interests in legitimate travel, trade promotion, and educational exchange are not in conflict with our border security agenda and, in fact, further that agenda in the long term. Our long-term interests are served by continuing the flow of commerce and ideas that are the foundations of prosperity and security. Acquainting people with American culture and perspectives remains the surest way to reduce misperceptions about the United States. Fostering academic and professional exchange keeps our universities and research institutions at the forefront of scientific and technological change. We believe the United States must meet both goals to guarantee our long-term security.

We are facing an evolving threat. The tools we use to address this threat must be sophisticated and agile. Information obtained from these tools must be comprehensive and accurate. Our criteria for taking action must be clear and coordinated. The team we use for this mission must be the best. The Department of State has spent years developing the tools and personnel needed to properly execute the visa function overseas and remains fully committed to continuing to fulfill its essential role on the border security team.

Chairman THOMPSON. Thank you for your testimony.

I now recognize Director Leiter to summarize his statement for 5 minutes.

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

Mr. LEITER. Chairman Thompson, Ranking Member King, Members of the committee, thank you for holding this hearing on the events of Christmas day.

Let me start with the most crystal-clear assertion I can make. Omar Farouk Abdulmutallab should not have boarded that plane bound for the United States on Christmas day. The counterterrorism system failed, and I along with other leaders have told the President—I tell you, I am telling the American people—we are determined to do better.

I have also pledged to the President, along with the DNI, a fresh and penetrating look at the human and technical factors that we think contributed to this failure and try to determine ways that we can improve our performance. The President has tasked me with two specific responsibilities—one, a methodology of pursuing follow-up actions for all threats and threads as we detect them, and second, a dedicated capability at NCTC to enhance watch list records.

In addition, I am, of course, working with the DNI, with Leon Panetta, with Bob Mueller and other members of the IC to work on intelligence community-specific improvements.

I would like to briefly summarize the events of Christmas day from our perspective and what went wrong. I want to start by debunking something that has become conventional wisdom, that this is a failure just like 9/11. As the President has said, this was not, like 2001, a failure to collect or share intelligence. Rather, it was a failure to connect, integrate, and understand the intelligence.

Now, one is not necessarily a lead to the more tragic consequences than the other, but the differences in those failures obviously lead to a different set of reforms that might be necessary.

Although the National Counterterrorism Center and the intelligence community have long warned, going back to 2008, 2009, about the threat posed by al-Qaeda in Yemen, we did not correlate the specific information that would have kept Abdulmutallab off that flight.

We did highlight the growing threat of al-Qaeda in Yemen. We also focused on targets in Yemen, but in the fall of 2009 we increased the need to talk about the possibility of al-Qaeda from Yemen targeting the United States. We also in fact analyzed the information that al-Qaeda was working with an individual who, only again after the fact, did we know to be Abdulmutallab.

Finally, the intelligence community also warned repeatedly of the type of explosive device that was ultimately used by Abdulmutallab and the ways in which that device could be used to undermine U.S. aviation screening. But again, despite having identified these overall streams, we failed to make the last final connection, what I would refer to as the last tactical mile here, linking Abdulmutallab's identity to the plot that was in train.

We indeed had the information that came from his father that he was concerned about his son going to Yemen, coming under the influence of religious extremists, and that he was not going to return home. We also had streams of information from other intelligence channels that provide the pieces of the story. We had a partial name, an indicator of a Nigerian, but there was no single piece of intelligence that brought that together, nor did we at NCTC or elsewhere in the intelligence community do that in our analysis.

As a result, although Mr. Abdulmutallab was identified with respect to terrorists and placed in the Terrorist Identities Datamart Environment, he was not watchlisted based on the information that was associated with him, nor was the placed on the No-Fly or Selectee list.

Had all the information the United States had available at the time that link together, his name would have been watchlisted and thus on the visa screening list and the border inspection list. Whether he would have been placed on the No-Fly and Selectee list, based on the existing standards, would have been determined by the strength of our analytic judgment. As I have already said, I believe, one of the clear lessons we have learned is a need to reexamine the standards for inclusion on these various watch lists.

Finally, and I hope I have made clear I have no desire to try to make excuses for what we did not do, because there are things that we didn't do well and we didn't do right. I do want to give you at

least a bit of context about the context in which this failure occurred.

Every day the National Counterterrorism Center receives literally thousands of pieces of intelligence related to CT—more than 5,000 a day; well over 5,000. We review well over 5,000 names each day. Each day more than 350 individuals are actually placed on the watch list.

Now, in hindsight we can say with a high degree of confidence that Abdulmutallab was plotting with AQAP. Although we obviously have to do better, we have to recognize that in my view there is no single silver bullet, and that is especially true as this terror threat we face becomes more multi-dimensional and more dispersed away from traditional areas of promoting terrorism.

So while watchlisting and intelligence are critical tools in this fight, I would echo the Chairman's statement of the need for a layered approach to counterterrorism, which includes technology, international screening and cooperation and the like.

Now, very quickly, I would like to outline the ways in which we are improving the system already. As I have noted, the President has assigned to the interagency to review the standards for inclusion on the watch lists, including the No-Fly Selectee list. This has been done.

In addition, we have immediately moved additional resources to focusing on Yemen and other al-Qaeda affiliates that we believe pose a threat to U.S. homeland security.

Third, we are trying to move away from a names-based system of pursuing these threats, ensuring that our analysts have the time and resources to pursue the small tidbits of information so they can in fact associate that with individuals and ensure proper watchlisting.

Finally, as I also noted at the outset, under the President's direction we are expanding and deepening our allocation of responsibility for specific follow-up actions for a wide range of threats, not just those that appear to be high-priority threats in the beginning.

With that, Mr. Chairman, I very much look forward to working with this committee and fielding your questions as we work on this together.

[The statement of Mr. Leiter follows:]

PREPARED STATEMENT OF MICHAEL E. LEITER

27 JANUARY 2010

Chairman Thompson, Ranking Member King, and Members of the Committee on Homeland Security: 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 Jane Holl Lute, Deputy Secretary of Homeland Security and Patrick Kennedy, Under Secretary of State for Management.

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-Qaeda 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-Qaeda 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 watch list.

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

- Immediately reaffirm and clarify roles and responsibilities of the counterterrorism analytic components of the IC in synchronizing, correlating, and analyzing all sources of intelligence related to terrorism.
- Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.
- Take further steps to enhance the rigor and raise the standard of tradecraft of intelligence analysis, especially analysis designed to uncover and prevent terrorist plots.
- Ensure resources are properly aligned with issues highlighted in strategic warning analysis.

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

- Establish and resource appropriately a process to prioritize and to pursue thoroughly and exhaustively terrorism threat threads, to include the identification of appropriate follow-up action by the intelligence, law enforcement, and homeland security communities.
- Establish a dedicated capability responsible for enhancing record information on possible terrorist in the Terrorist Identities Datamart Environment for watchlisting purposes.

THE EVENTS LEADING UP TO THE CHRISTMAS DAY ATTACK

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

Although NCTC and the intelligence community had long warned of the threat posed by al-Qaeda 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 promul-

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

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

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

Chairman THOMPSON. Thank you very much.

I thank all the witnesses for their testimony.

I remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

To each one of the panelists, since this occurrence on December 25, has any personnel action or disciplinary action taken place in your Department relative to this incident?

Ms. LUTE. In the Department of Homeland Security, Mr. Chairman, the personnel actions that have been taken have related to intensified training, intensified deployment, but there have been no disciplinary actions that have taken place.

Chairman THOMPSON. So there are no disciplinary——

Mr. KENNEDY. No disciplinary actions, sir.

Mr. LEITER. We are currently reviewing all the personnel. We have made no final decisions.

Chairman THOMPSON. If you will, at whatever point you complete that review, would you provide the committee that which the law allows so we can review it?

Mr. LEITER. Absolutely, Mr. Chairman.

Chairman THOMPSON. So my understanding is, even though this was an unfortunate situation, nobody has been disciplined. We understand the President took responsibility, and that is good, but the question in the minds of a lot of us is, is that good enough?

Now, my next question to each one of you is if that situation occurred today, would it be any different?

Mr. KENNEDY. On the State Department, it would be different, Mr. Chairman. We had a process that had been worked out with the interagency community, and we have discovered that we did not have sufficient checkmarks in. There was no requirement in our previous rule grid when we reported on the Visas Viper, meaning somebody coming into an American embassy and saying we have concerns about a third party.

We reported that immediately, but we did not have in that process a checkmark that this individual had a U.S. visa. I cannot tell

you why that wasn't included. I can tell you probably because we had already passed to the law enforcement intelligence community the list of everyone who gets a visa on a daily basis.

We have now added that to our process, so any person who comes in the embassy and makes a report of terrorist concern, not only to report that individual in our Visas Viper message to the community, but we add then this person has a United States visa, and we have also enhanced the name-checking capability in that system to make sure that if there is a misspelling——

Chairman THOMPSON. Okay. So, all right, so he has a visa. So what does that do?

Mr. KENNEDY. What?

Chairman THOMPSON. In the process. Does it revoke the visa? Does it——

Mr. KENNEDY. As I mentioned in my statement, Mr. Chairman, if we unilaterally revoked a visa, and there was the case recently up, we have a request from a law enforcement agency to not revoke the visa. We came across information. We said, "This is a dangerous person." We were ready to revoke the visa. We then went to the community and said, "Should we revoke this visa?"

One of the members—and we would be glad to give you that in private—said, "Please, do not revoke this visa. We have eyes on this person. We are following this person who has the visa for the purpose of trying to roll up an entire network, not just stop one person."

So we will revoke the visa of any individual who is a threat to the United States, but we do take one preliminary step. We ask our law enforcement and intelligence community partners, "Do you have eyes on this person and do you want us to let this person proceed under your surveillance so that you may potentially break a larger plot?"

Chairman THOMPSON. I think that the point that I am trying to get at is is this just another box you are checking, or is there some security value to adding that box to the list?

Mr. KENNEDY. Yes. The intelligence and law enforcement community tell us that they believe in certain cases that there is a higher value of them following this person so they can find his or her co-conspirators and roll up an entire plot against the United States, rather than simply knock out one soldier in that effort.

Chairman THOMPSON. Mr. Leiter.

Mr. LEITER. I would offer four ways in which I think the process would work differently today, Mr. Chairman. First, actually beginning in July 2008, right after Mr. Abdulmutallab obtained his visa, NCTC began working with State Department in reviewing visa applications in a new and more advanced way.

The way in which we now review that visa, and I can't go into it in the open session, would have detected a connection with Mr. Abdulmutallab, which would have stamped an automatic warning to State Department, DHS, FBI and other intelligence community components. So first of all, he might not have even gotten the visa in the first place.

Second, anyone who has a visa that goes on the watch list, the default is if that visa is revoked, they also become a no-fly to en-

sure that if someone shows up with the visa, if there is some confusion there, they are also a no-fly. That is the second step.

Third, we have dedicated teams that don't have any responsibility for producing intelligence, but simply for following up on these small leads. I believe those teams would increase the likelihood we would tap.

Fourth, we have, as an interagency way, reviewed already the standards for placement on No-Fly. Although those standards have not yet been formally adjusted, they are being interpreted in a manner which allows us to more broadly apply those practically.

Chairman THOMPSON. Thank you.

I yield to the Ranking Member for questions.

Mr. KING. Thank you, Mr. Chairman.

I guess this would go to Mr. Leiter and Deputy Secretary Lute. The President first spoke to the Nation on this on Monday, December 28, I believe. It was 3 days after the event. During that time I assume most of this information was available to the intelligence community, whoever was briefing the President. Yet when he spoke that day, 3 days after, he referred to Abdulmutallab as an isolated extremist.

Do you know who was responsible for clearing that statement, when obviously he was not an isolated extremist? He was part of al-Qaeda in the Arabian Peninsula. We had this series of information on him. Now, the President seemed to correct that the next day. Why did the President go forward and use that term? Who is responsible for briefing him? Who is responsible for clearing that statement?

Mr. LEITER. Congressman, I frankly can't speak to the White House interactions and who prepared that for the President and who briefed him on that. I simply don't know. I would say that on the night, on Christmas night, we advised the White House. I think the White House, we said that we believe this was an attempted terrorist attack.

I will also add that during this entire look back, an on-going investigation, as you know, different pieces of information have come forward, which have made it more and more clear, I think, each day of his connections to al-Qaeda in the Arabian Peninsula.

Mr. KING. Secretary Lute.

Ms. LUTE. Congressman, I would echo what Director Leiter has said. I was equally not involved in the deliberations within the White House to inform the President.

I can also say, as Director Leiter has said, that from the moment we became aware of this incident, there was an extremely intensive effort to identify as many facts about this individual as we possibly could, including reaching out to international partners who held some elements of information. That work was intensive over those several——

Mr. KING. Because this interrupts my time, I want to interrupt. Again, I am just concerned why 3 days later, with all this information available, the President said "isolated extremist." Was it John Brennan who briefed him? Was it Leon Panetta?

I mean it would seem to me that in a situation like this, there should be one point person, who goes in and tells the President, who coordinates everything. Who is that coordinator? Do you know?

Who would have allowed him to say "isolated extremist" when he was not isolated?

Mr. LEITER. Congressman, I know that the National Counterterrorism Center and others were providing intelligence to the White House on an on-going basis. I simply don't know how those statements were produced.

Mr. KING. Okay.

Secretary Lute and Mr. Leiter, would, you know, either yourselves or anyone in the intelligence community who would now say that Abdulmutallab should be un-Mirandized at this stage? Because, obviously, Director Blair seems to believe it was a mistake to have him put into the criminal justice system. At this stage, is anyone willing to recommend he be taken out of the criminal justice system and put into the military tribunal system?

Ms. LUTE. Congressman, what I can say from the Department of Homeland Security's perspective and in hindsight—there is a lot of hindsight going on—we are focused on those aspects of this for which the Department had key responsibility. The decisions regarding the Mirandizing of Abdulmutallab are appropriately directed to the Justice Department.

Mr. KING. Okay. My understanding was the Secretary of Homeland Security is a member of the President's task force on interrogation, and that supported the creation of the HIG. I am wondering does the Department have a position of whether or not at this stage, not doing Monday morning quarterbacking, right now as of Wednesday, January 27, do you believe that you should be taken out of the criminal justice system and put into the military tribunal system?

Ms. LUTE. Congressman, I am not party of all of the conversations that have gone in this individual. I am not prepared——

Mr. KING. Director Leiter.

Mr. LEITER. Congressman, I think it is critically important that we try to get in as much information from him as we can. I think now, several weeks after the arrest and Mirandizing, it is not at all clear to me, and I am not close enough to know whether or not it would be productive or counterproductive, given the current FBI investigation, to do that.

Mr. KING. Secretary Lute, it has been reported in the press that CBP was waiting in Detroit to question the terrorist when he came off the plane. If that is true, wouldn't that have been sufficient information to contact the Netherlands and at least ask them to do a secondary inspection?

Ms. LUTE. Congressman, what CBP had was consistent with our long-standing practice of examining issues related to admissibility, and——

Mr. KING. Okay, but looking at it now—we are going toward the future again—I am not trying to Monday morning quarterback, but looking toward the future, having that information, if there is enough information to question a person coming off, is it that difficult to ask another government to give him a secondary inspection?

Ms. LUTE. We in fact have changed our practice.

Mr. KING. We have. Okay.

Ms. LUTE. That kind of information will be pushed forward.

Mr. KING. Let me ask Director Leiter and Secretary Lute: People have said the system failed, but what really was the system failure? Wasn't it judgments that failed? Obviously, we always have to adapt the system. But it seems to me the system provided enough information that, if it were properly interpreted, this would not have happened. Did the system actually fail, or are we talking about judgment mistakes?

Again, I am not trying to Monday morning quarterback. But I think rather than just say the system failed, one person accepts the responsibility, shouldn't we be—as the Chairman seemed to be indicating, and I agree—looking for individuals who did make judgment mistakes?

Mr. LEITER. Congressman, I think there are potentially some instances where there was a protocol to be followed, and someone didn't follow the protocol. That is one category of failure.

The second category of failing is did you connect these two pieces of data? I frankly think that that second category is a lot harder to identify and clearly say you made a mistake. We want analysts to do that. But whether or not they actually could, and piece that all together, given the resources, the workload they are facing, I think it is much more difficult to say that that was a clear failure.

I believe the phrase "systemic failure" was meant to suggest that there are a series of failings in different pieces of the system, not that the entire system itself is broken.

Mr. KING. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

The Chair now recognizes the gentlelady from California for 5 minutes. Ms. Harman.

Ms. HARMAN. Thank you, Mr. Chairman.

I would like to welcome our witnesses, but comment on the absence of Secretary Napolitano. This is the committee with primary jurisdiction over the Department of Homeland Security. She is the Secretary of Homeland Security. She is in Washington, DC.

She was invited to testify at this very important hearing, and she should have been here, Deputy Secretary Lute. I understand that you were prepared and you had accepted our invitation, but I am very personally disappointed that she isn't here.

I also want to note for the record that I was briefed following the Christmas bomb plot within a few days. I was first in my district, and then I was on a family vacation, but Secretary Napolitano did call me after she spoke to the Chairman. I am quite aware that she had first spoken to him. I also exchanged e-mails and had numerous calls with Mr. Leiter, who was first in Washington, DC, during the event and then subsequently on a short family vacation himself. I know he was hard at work.

Mr. KING. Would you just yield for 2 seconds? Just to say nobody on this side received those briefings, which I think is wrong. It has always been bipartisan.

Ms. HARMAN. I agree with you, Mr. King, that there should be bipartisan briefings. You know that I agree with that.

I also want to note that in recent years there have been many intelligence community successes. The Zazi plot, the Headley plot and others are examples of success, and there had been many intelligence community sacrifices, particularly the loss recently of seven

CIA personnel at the Forward Operating Base Chapman in Afghanistan. Obviously, all of us know this and want to salute again today the hard-working women and men of the intelligence community.

But despite all those successes and the risks that they take, the Christmas day problem does represent a failure. Two of you, Mr. Kennedy and Mr. Leiter, have stepped up and taken responsibility, as has Mr. Brennan, and I applaud you for doing that. I applaud the fact that you have all pledged that you would do better.

Doing better is not optional. A hundred percent security can never be achieved, but surely we can do better. At least to me, listening to all of this and based on my long experience with the Intelligence Reform Act and other efforts to try to better, I think that doing better is not about laundry lists. It is about leadership.

Only through leadership will our system of layered security become more agile and responsive. Let us understand that the enemy that is seeking to harm us is agile and responsive. Whatever it is that we now decide to do, they will try to figure out a way to get around it. So our system of collection, analysis, visa approval, watchlisting and other things should get better. But only through strong leadership will that better system stay agile and responsive.

Let me just add one thing as the tag end. This I commend the Department of Homeland Security for doing very well, and that is preparing, not scaring the public. There is a new tone. I applaud that. Let us remember that the successful layer of security on Christmas day was a prepared public on that airplane.

So, finally, let me make one other point. There is testimony submitted for the record of this hearing by the ACLU, and I have read that testimony, and I think it is extremely thoughtful. It reminds me that one piece of unfinished business since the Intelligence Reform Act of 2004 is the formation of a privacy and civil liberties commission that was supposed to oversee new practices to keep our country safer.

I wrote a letter to the President in October with Senator Susan Collins of Maine, and the White House has never responded to our letter. Insofar as I know, nothing has been done. I think that this is unfortunate and will prevent us from assuring the public that we are enacting better practices consistent with our Constitution.

But my one question, because time is running out, is to each of you. What are you personally going to do to assert leadership in the near- and medium-term to make certain that the people under your supervision remain agile and responsive against an evolving threat by a learning organization?

Ms. LUTE. Congresswoman, perhaps I will begin. You and I know each other well. I take very seriously the responsibilities of leadership, and I underscore responsibility. I personally traveled to 12 countries in 12 days with colleagues from the Department of Homeland Security to bring a message of leadership from the United States to our international partners with whom we have to work very closely to raise the standard of aviation security.

I personally spoke with the IAB officer on the ground in Amsterdam to understand from his perspective what more can we do to change the system and to improve our ability to prevent a future event as occurred on Christmas day.

The Secretary equally has personally made aviation security a cornerstone event of our efforts going forward in this, along with other parts of the Department, who take very seriously its leadership role to help create a homeland where the American way of life can thrive. This is something we take extremely seriously.

Mr. KENNEDY. Ma'am, the Secretary of State is incredibly involved in this, and she has charged me, and I think that I would offer in the brief time I have two points, but there are others.

The first, we need to continually increase our software capability to take disjointed pieces of material and bring them to get together. The second thing we need to do is and I have to make sure that is happening, and I think that we also have to make sure that we remain and improve our lash-up with the National security and the law enforcement community, because we are on the frontline.

But while we are on the frontlines, if we don't have the backstopping that is the best that we can lash up, then we would fail again. That is my pledge to make sure those happen.

Mr. LEITER. Congresswoman, I have spent a tremendous amount of time since December 25 with my workforce, my analysts, my watch listers, my watch standards, and made clear to them many things. One, I have to enable them to be able to do the job. If they need something, they have to come to me, so I am making sure that lines of communication are more open than ever.

So one of the things I first said to them is I want to know from every one of them how do we do our job better. I did an open e-mail to my entire organization. I probably got 200 responses of what they think needs to be done.

The second thing I said to them in a way relates back to what the Chairman asked. I told all of them you have to ask yourself whether or not you can keep doing it, because this is high pressure. It is high stakes. You are going to get beat up in the public realm. You have to make sure that you can commit yourself 100 percent to this every single day. There is no embarrassment if they can't. We have to make sure that we have a well-honed team that really stays on this.

Finally, the last thing I would say I am doing—I am not generally noted to be an especially patient person, but whatever patience I have shown in the past in terms of trying to negotiate or massage interagency agreement to obtain data or to provide cooperation, frankly, I am done with it. I am going to ask once politely, and after that I am bringing to the White House and Director Blair and saying this has to be done. If it can't be done, I can't guarantee you the security that I think you and the American people deserve.

Could I add one thing, Mr. Chairman? I just want to note on the record I endorse wholeheartedly the information that this committee needs to make a decision. You have my commitment from NCTC—I hope we have illustrated that in the past—to provide you that completely and on a nonpartisan basis the information you need to do your oversight correctly.

Chairman THOMPSON. Thank you.

The gentleman from Indiana for 5 minutes, Mr. Souder.

Mr. SOUDER. Thank you, Mr. Chairman.

First, Mr. Kennedy, I would appreciate for the record if you would—you said since 2001 you revoked 51,000 visas and 1,700 for suspected links to terrorism—could you give us a by-year number of visas revoked and number for suspected terrorism?

But, secondly, I know my friend from New York kept making a point about Monday morning quarterbacking. As a Hoosier, when you have Peyton Manning as your quarterback, you don't have to do Monday morning quarterbacking. That is important here, because it is the person in charge, and the people in charge. When they fail is when we do Monday morning quarterbacking.

It is not the agent who didn't have the information who messed up here, that as you see these people at the airports as you go around the world, there were signals from the top to back off of profiling, don't focus as much, agents not focusing as much on capturing people as moving them through, not putting things together.

I have some basic questions that we learned before, and I was very disturbed at some of the briefing. My understanding is in public record that we didn't know he paid cash, because we don't collect the information on cash, because 20 percent or some percentage of people who do foreign travel pay by cash and that that wasn't in his—we didn't know he paid cash. That is public record. Is that true?

Mr. LEITER. I think it is true that we did not know he paid cash. One note, I would say, Mr. Souder. I think you are right. Roughly 20 percent of global passengers pay cash. That proportion, from the region he came from in Africa, is vastly higher, so frankly, a cash payment for a ticket from where he bought his ticket really would not raise any suspicion.

Mr. SOUDER. We also didn't know that the British had him on a no-fly list. Is that correct? That is publicly reported.

Mr. LEITER. The British did not have him on a counterterrorism no-fly list. The British had——

Mr. SOUDER. But they had him on a no-fly list.

Mr. LEITER. He did not have a visa——

Mr. SOUDER. He didn't have a visa, so he couldn't fly.

Mr. LEITER [continuing]. For criminal purposes.

Mr. SOUDER. So the question is, and this is what I would ask you, in any type of basic tracking or intelligence, in narcotics and that type of thing, you build a system. When a business is trying to figure out risk of something, they build a system.

The cash would not be relevant in normal, but the cash becomes relevant if the father said this, and you knew you were watching something from there, and you are tracking a ticket. Then all of a sudden the cash is relevant. The fact that he didn't have a visa was not relevant, because it wasn't relevant to terrorism. But the fact that he was a liar on his visa form suddenly becomes relevant, once you know that the father called, and he bought cash in that.

In other words there is a point system. My understanding is you don't have a point system. Is that true?

Mr. LEITER. Congressman——

Mr. SOUDER. In other words there is no way to pyramid the information.

Mr. LEITER. Congressman, I don't think that is quite true, but I don't want to quibble with your point, because I think you are exactly right. Those individually——

Mr. SOUDER. Irrelevant things, yes.

Mr. LEITER [continuing]. Inoffensive bits of data add up to a larger picture. I will say that over the past several years, as we have tried to "accumulate data" so all of that data can be shared and analyzed together, one of the consistent challenges we have faced at the National Counterterrorism Center is these bits of data that aren't terrorism information, but could add to that picture.

That has been one of the most significant obstacles we have faced in making sure all that information can be effectively analyzed.

Mr. SOUDER. But would you not agree that there are things where you are building a broad picture, and there are things that are specifically relevant to getting on an airplane? In other words I know early on until they somewhat improved the system, that one time going through the Washington airport, six of the seven people in secondary where members of Congress. Why? We got out early. We bought e-tickets. We paid cash.

That those are logical things you watch for in an airplane, and they build that, but you might not need them in your full terrorism bank. Do you have any ability to separate when you are getting on an airplane, when you are getting at something else from kind of this general pool? Otherwise, you will have so much information that will be indecipherable.

Mr. LEITER. On that, Congressman, I would really defer to Deputy Secretary Lute on their screening——

Mr. SOUDER. Then let me tie a question with that, that we worked hard in the very original bill to make sure that Homeland Security was going to be at as many posts where they were doing visas and as many posts at airports. You had 50 deployments. Are you asking for more?

In other words the whole point of port security in airports is not to kind of arrest them after they have blown everything up. It is to get it before it gets here. Are you asking and requesting more overseas deployments? Are you going to get this kind of information where they can say, okay, this is airplane specific, this is harbor specific, as opposed to just general?

There may be something—for example, somebody's shipping orders. That may be relevant in a port, but not relevant to the total counterterrorism center.

Ms. LUTE. Congressman, on each of these lines we are doing more. As you know, the Department of Homeland Security has no authority abroad. But we do have programs where we have people deployed for precisely this purpose. These are limited programs. We have expanded them as Congress has given us the resources to do so. We will expand them again. We have expanded them in the wake of this episode.

Mr. Chairman, if I could just make one thing very clear about the Secretary's leadership and your presence today, as you know, she had planned—there was international travel that conflicted with this hearing today. I was offered in part because I went abroad immediately at her direction with my colleagues to raise some of the issues that you are raising about the kind of informa-

tion that we are collecting, about the kind of technology that we can deploy, about the weaknesses that exist in the system and how we can work collectively to raise that bar.

Mr. Chairman, with your staff it was coordinated and agreed that that I would appear for that reason.

Mr. SOUDER. With all due respect, it isn't true that you have no authority abroad. You have the right to reject their entry into the United States.

Ms. LUTE. Absolutely right, Congressman. There is no question. We do—we can——

Mr. SOUDER. A container doesn't have to come in. A person doesn't have to come in. We have that authority.

Ms. LUTE. That is correct. But to your point about additional information, we have made that change in Homeland Security, taking information that previously under our pre-existing protocols was related to admissibility and not putting it in the service of making flying determinations.

Chairman THOMPSON. Thank you.

Time has expired.

The Chair now recognizes Mr. DiFazio for 5 minutes.

Mr. DEFAZIO. Thank you, Mr. Chairman.

Ms. Lute, you know, we wouldn't have any imaging technology capability today if it hadn't been for Kip Hawley. You know, I have been a fan of this since I was first exposed to it about 8 years ago. I kept bumping up against that "Oh, my God, we are going to see people's skin or bodies or images" or whatever.

Kip Hawley, you know, after a number of failed administrators, really focused on this. He pushed it through. I kept saying, "Isn't it just the way you get software? It doesn't have to be your body. It can—" and Kip finally got that done.

So the point I am making here is we need a TSA administrator. I am going to ask this question, which I asked Ms. Napolitano last spring. Can't you just get it out of the way and allow the people in the TSA to unionize? It will not impinge, unlike some wacko Republicans think, on National security. Just get that out of the way so that won't be the thing that stalls the new TSA administrator.

She said she wanted to wait for an administrator to get it done. You can't wait. She needs to make the decision, get it done, give them those rights and get that off the table, and then the next administrator can just deal with security issues and their history and background, and not this specious issue. That is just a message I wish you would deliver to her, because she said here, you know, to me quite some time ago she was wanting to move this forward, but she wanted to wait for the administrator. Can't wait. Get it done.

Point No. 2, you know, the imaging technology is good. It may or may not have worked in this case, but it has to be mated with something that does vapor detection. Are we full out there working on vapor detection or trace detection? You know, I mean dogs are great, but, you know, we need, you know, maybe, you know, either we need a heck of a lot of dogs or, you know, we need some technology that is more dependable than those puffer machines.

Ms. LUTE. You are absolutely right, Congressman. This technology does represent an improvement in our overall capabilities, but it is only one part of a layered system. Other technology has

to be brought to bear as well, as well as improved processes, improved information gathering across the board.

We are working very closely and have established a high-level working group with the Department of Energy and the National labs to look precisely not only at are we using existing technology to best effect, but what are the promising new technologies that we can then add to these multiple layers to ensure the best safety and defense possible?

Mr. DEFAZIO. Okay.

To anybody, are all—I hate these stupid names; I don't know, the Terrorist Identities Datamart entire and, you know, whatever, TIDE? Are all the people on the TIDE list now selectees? I don't see why they wouldn't be. It is an insignificant number of daily passengers compared to the number of people who fly daily. It would not be in an imposition. Are they now also selectees?

Mr. LEITER. Congressman, they are not, although I must say I very much appreciate your sentiment. Frankly, from my perspective as the director of NCTC, it is no skin off of my back if they all were.

Mr. DEFAZIO. There are 500,000 of them. They are worldwide. There are 3 million-something people fly a day. You know, I mean it would add significantly to the burden. Does Homeland Security object to this?

Ms. LUTE. Homeland Security has no objection to that, to any measures that enhance the security of the traveling public.

Mr. DEFAZIO. Do you think that would enhance security, that anybody who is on the TIDE list is a selectee?

Ms. LUTE. Rather than going——

Mr. DEFAZIO. Yes or no. I am running out of time.

Ms. LUTE. If any—it takes——

Mr. DEFAZIO. You don't know.

Ms. LUTE [continuing]. It takes layers of defenses—

Mr. DEFAZIO. Okay. All right. So you are sort of no.

Mr. LEITER[continuing]. Respectfully.

Mr. DEFAZIO. Yes, yes.

Mr. LEITER. Again, I respect your views, and I am happy to do it, but the pressure on NCTC, on DHS over the past 8 years has never been in that direction.

Mr. DEFAZIO. All right.

Mr. LEITER. It has always been in the exact opposite direction. So I just want to recognize this is a very changed——

Mr. DEFAZIO. I understand, but, you know, Congress acted, and we pushed, and we have in place now an appeal system. So if somebody is on that list, like John Lewis from Georgia, our colleague, or, you know, former Senator Kennedy, others who get on the list, you know, there is an appeals process. You can get off the list.

But why not err on the side of caution? Anybody on that list becomes a selectee. They at least get that slightly higher level of screening. They have some interaction with a, you know, with an officer, you know. I just think that to me, and again, it would be a very, very, very infinitesimal percentage addition to the daily workload.

Mr. LEITER. Congressman, I agree in many ways——

Mr. DEFAZIO. Okay.

Mr. LEITER [continuing]. But would note it would be about a 40 or 50 times increase in the number of selectees we have today.

Mr. DEFAZIO. Yes, but I don't think so on a daily basis. It is 500,000 people on the list. How many of them fly on a daily basis, you know, when there are 3 million people a day flying? I mean I just don't think it would be.

Mr. LEITER. But we currently have 14,000 on the Selectee that would increase them 40 to 50——

Mr. DEFAZIO. Yes, but I know it would increase the list that much, but in terms of daily workload, it would be nowhere near that.

One other quick question to State. You talked about you have the authority to immediately revoke a visa. You know, but you want to communicate. Then you said, but if it was urgent, you would act.

Have you ever had a recommendation the other way to you, that you revoke a visa that you didn't revoke?

Okay. Thank you.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you.

Thank you very much. We have been told that some votes will happen, and I have been fairly lenient with time. But in the interest of giving every Member an opportunity to ask questions, we will strictly adhere to the time.

The gentleman from Alabama, Mr. Rogers, for 5 minutes.

Mr. ROGERS. Thank you, Mr. Chairman.

As everybody on this committee knows, for many years I have been a vigorous advocate of canines' use and remain that way, and I want to talk mostly about that.

Before I do, I want to visit the subject that my colleague from Oregon brought up about the administrator who was proposed. The administration didn't propose him until September. I mean they had been in office 8 months, so if this was such a priority with the administration, he should have been proposed earlier.

Secondly, you did raise the issue that I care about. That is canine use. Right after this Christmas day bombing, Secretary Napolitano in her remarks—White House press conference—listed three or four items that the Department was going to turn to to enhance our security layer system, and one of them was enhanced canine use.

I sent her a letter since then, expressing again, as I have in this hearing and in other venues, my concern that we aren't utilizing that asset enough. I know for a fact that TSA only uses 750 canines. These are very inexpensive, very effective means of technology.

You have stated in your statement, the written statement, in two different places that you have increased your use of canine detection dogs, explosive dogs, in our transportation hubs. Can you tell me where and how many and what your plan is on that asset?

Ms. LUTE. In this open setting, Congressman, I am not going to detail any of the specific security measures that we have taken, but we believe that canines are an important part of the multi-layered defenses that we have been talking about. We look to use them to

the greatest extent possible. We know their value. We are convinced of it, and we are going to expand our use.

Mr. ROGERS. Okay. But you haven't significantly expanded them since the Christmas day bombing.

Ms. LUTE. But we have in fact expanded them. But the details of that in this setting I am not prepared to explain.

Mr. ROGERS. That is fine. I do want to get back with you in a more private setting, but I want to address a new technology.

Currently, the Amtrak, the Capitol Police and the Federal Protective Service all use a new type of canine explosive detection dog called a vapor wake dog. What it is is when somebody walks by, the dog detects the vapors in their wake. We all leave a wake when we walk by. Explosives in particular leave the smell, the odor, there for 15 minutes in that wake. So when it comes to transportation hubs like airports, bus stations, subways, whatever, the dog doesn't have to smell the person directly. It can just step by when the person walks by.

All these entities use it, but TSA does not use it. The Capitol Police, as I said, uses it. The Secret Service is now looking at it. They are going to probably start using it. Why has TSA been so reluctant to use that technology?

Ms. LUTE. Congressman, we focus on layered defense, as we have been discussing here this morning, and we are examining all aspects of layers, including the increased use of canines. As I mentioned, the Secretary has made very clear her determination that we look at promising new technologies, techniques, canines, leave no stone unturned to increase the security of the traveling public.

Mr. ROGERS. Well, they are used extensively in Europe. One of the things I was hoping that Secretary Napolitano would do during her trip to Europe—and I thought about it when she announced it—was I am hoping that as a part of the agreements that we worked out with our allies around the world, that for planes that are destined to the United States, that we can at a minimum deploy dogs, canines to those airports to be at the gate of any plane that is leaving for the United States to make sure that at least those passengers are screened with that layer of security that we have some control over.

If they want to let people get on the planes going elsewhere, that is their business, but if it is coming to this country, I want to make sure they are screened with every tool that we have got in our toolbox. A frustration that I have got is we are spending billions a year on bells and whistles, and we have a very simple technology that works, and we aren't using it anywhere close to the level that we should be using it. So I would ask you if you are going to make this a priority is to go forward and in the near future.

Ms. LUTE. Yes, sir. As the Secretary did make clear to her European colleagues when they met together on this issue at her request, there are number of measures that need to be taken. This is not a business-as-usual environment that we are in, and it takes the collaboration of all of us to be able to assure the traveling public that we are doing ever we can to keep them safe, including measures such as you have outlined.

Mr. ROGERS. Great. Thank you very much.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

The Chairman now recognizes Representative Cleaver for 5 minutes.

Mr. CLEAVER. Thank you, Mr. Chairman.

Ms. Lute, you addressed this already to some degree, and I am not sure how much you can discuss this issue here publicly, but you had mentioned that you and the Secretary had traveled abroad in hopes of working out some cooperative agreements with our allies in this fight against terror.

One of the questions that maybe you can answer here, and I would be interested in hearing, you know, some of the more detailed information in the right setting, proper setting, but is there any willingness abroad to support what we are trying to do in terms of aviation safety for other countries to contribute financially to enhance technological measures, I mean? Or are we the only Western nation that is engaged in spending a lot of money in trying to increase the technology or create more sophisticated technology?

Ms. LUTE. Congressman, this was an extremely intensive trip. My many years in the Army prepared me well for the conditions under which we were traveling.

The dialogue with our international partners could not have been more supportive. They recognize almost universally that this is not a U.S. problem. This is not a Dutch problem. This is not a Nigerian problem. This is an international problem that the responsible governments of the world must come together to address. Again, they all agree that in the area of information gathering and sharing, we need to do better, and we can.

In the area of technology, we are not deploying existing technologies to best effect, and there are new and promising technologies. We are not the only ones with an investment in technology and reliance. It is one of the multiple layers of defense that we have in place.

Equally, there is a recognition that this global system, as we saw on Christmas day, with an access to any part of this system, you potentially have access to the entire system, so we all need to come together, and they recognize those responsibilities. The Secretary is leading a series of regional dialogues leading to a major conference on this issue so that concrete actions can be taken in the information sharing, technology, and system strengthening.

Mr. CLEAVER. I have no other questions, Mr. Chairman. Thank you.

Chairman THOMPSON. Thank you very much.

The Chairman now recognizes Mr. McCaul for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman.

This was clearly a failure in intelligence. I think all the witnesses have agreed to that. The President of the United States has as well. It is more than a failure to connect the dots, as we talk about so much. It is a failure to identify dots or specific threat information coming in and acting upon it appropriately.

We had the Christmas bomber's father going to the embassy, warning us about his son. The State Department issued a cable that basically stated that and sent it to law enforcement, and I as-

sume to the NCTC, stating that information had posted just that Farouk may be involved in Yemeni-based extremists.

I think Members of Congress and the American people don't understand why with that type of information and Director Leiter with specific intelligence coming in through the IC, the intelligence community, why that wasn't linked together, No. 1, and why it wasn't acted upon to ensure that this man never got on this airplane in the first place.

I think we agree that this visa should have been revoked immediately, given the information. I can't get into the classified information that you are privy to, but it was specific. What happened here?

Mr. LEITER. Congressman, some action was taken, but as you have identified, as I have talked, we would say it was obviously not sufficient, which was his name was entered into the Terrorist Identities Datamart Environment, but that didn't have automatic repercussions in terms of screening, visa revocation, or stopping him from boarding the plane.

The other intelligence simply wasn't identified and associated with this individual. I can tell you that there was concern on the intelligence community's part about potential attack by al-Qaeda in Yemen, and we were concerned even about the timing of that. What we didn't connect was the individual's name or where that attack would occur. That was our failure.

Mr. MCCAUL. Was that because it was misspelled—the name was misspelled? I mean to me, you know, if you type my name into Google, for instance, M-C-C-A-U-L, they will say, did you mean M-C-C-A-L-L. and so do you not have a similar type of capability?

Mr. LEITER. Actually, the misspelling did not affect NCTC in any way. It did affect, as I understand it, and I will defer to Under Secretary Kennedy on this, from our perspective when his name was sent in, we actually put the spelling in both ways. The technology we use, it wouldn't have made a difference.

Mr. MCCAUL. Did you not have the cable that the State Department sent?

Mr. LEITER. We did, and we inserted the spelling based on a number of things.

Mr. MCCAUL. Yet you made the decision not to revoke the visa, given that information?

Mr. LEITER. I don't have the authority to revoke a visa. That is an authority——

Mr. MCCAUL. Right. Can't you call Secretary Kennedy and say, "You know, I think we have got a problem here. We ought to think about revoking this visa."

Mr. LEITER. The intelligence community can, frankly. That normally doesn't occur, if the nomination itself comes from the State Department, because——

Mr. MCCAUL. Well, I think there needs to be a lot better coordination going on here between these two entities.

Mr. Kennedy, why, given the information that you had, why wasn't the visa revoked?

Mr. KENNEDY. Sir, as I mentioned earlier, when we get any information, when anyone appears at an American embassy and say that they have doubts about someone, we immediately generate

what is called a Visas Viper message. We send that to the entire law enforcement and intelligence——

Mr. MCCAUL. My time is running out. I understand the process, but you had this information, and you didn't revoke the visa.

Mr. KENNEDY. Because——

Mr. MCCAUL. I mean the cable I just read——

Mr. KENNEDY. Right.

Mr. MCCAUL [continuing]. Makes it pretty clear that this man is associated with extremists in Yemen. You didn't revoke his visa.

Mr. KENNEDY. What it was, sir, his father said he was associated with this, and so we then asked the intelligence and law enforcement community if they had any other information. I don't want to take much of your time. I would be glad to visit with you afterwards.

Mr. MCCAUL. Well, I think the father is a very credible source. This isn't some anonymous person coming in saying this.

Mr. KENNEDY. We have people coming in, sir, to American embassies every day, attacking their relatives.

Mr. MCCAUL. Well, let me just—my time—this was a failure extraordinaire, and I sure hope it never happens again.

Deputy Secretary Lute, the last of my remaining time, they have identified a vulnerability in our system. I am very concerned about future flights now. The system didn't work. The screening—you know, they are always a simple genius, you know. They use chemical explosives, which would be detected through X-ray, but not through the magnetometer.

I know we are focusing on the 16 countries of interest in terms of pat-downs and more enhanced screening, but I am concerned about still the majority of the airports out there where we are still vulnerable. They could still use this technique and get chemical explosives through the magnetometer. What is the Department of Homeland Security doing about that?

Ms. LUTE. Congressman, we are not just focused on those 16 places that you have identified. We are focused on aviation security globally and the traveling public, to ensure their safety.

People have talked about silver bullets. We don't look for silver bullets in Homeland Security. We know it takes a layer, multiple measures of layers, not just by us, but by our international partners, and it takes constant vigilance.

We have made some adjustments internally now to take the information that we get, push it forward where we have teams on the ground or to authorities in airlines where we don't have specific teams. We are looking to expand our teams as well. This is not a business-as-usual response. No one will be satisfied——

Mr. MCCAUL. But my point is there are still many airports vulnerable to the same technique deployed by this terrorist.

Chairman THOMPSON. The gentleman's time has expired.

The gentleman from Pennsylvania, Mr. Carney, for 5 minutes.

Mr. CARNEY. Thank you, Mr. Chairman.

I have to echo the sentiments of a number of our colleagues today, who I am very dismayed that the Secretary herself is in here. I mean it is probably fair to ask where the hell is Secretary Napolitano for this hearing, to be quite honest.

I understand, Deputy Secretary Lute, that you are prepared and that is great, but she was invited. She needs to be here to address something of this magnitude. My first question is why was her first response to the public that the system worked?

Ms. LUTE. Congressman, if I could, and I clarified before, the Secretary had international travel that was originally conflicted. We coordinated with the Chairman's office. She has been in regular talks with the Chairman, other Members of this committee. She dispatched me with my colleagues around the world to work aggressively with international partners, part of the reason my appearance here was coordinated and agreed.

What the Secretary has made clear in her initial response, she was responding to in the environment of what are we doing to address this concern now? How are responding to the information that we would have to ensure that there are no other flights that are subjected to any danger or that pose any threat to the American public?

Mr. CARNEY. I want to shift gears slightly here. You and I, last time we spoke, I believe, was New Year's Eve. That is right. How is the QHSR coming? Are we further down the road? Are we going to see it soon? Frankly, does the QHSR lay out a sort of chain of command that would obviate some of the issues we are talking about today?

Ms. LUTE. We did speak late New Year's Eve, in fact. The QHSR from our perspective is concluded. It is with the White House right now, ensuring final interagency coordination prior to release. As I mentioned to you, we are on schedule that I discussed with you.

We look for the QHSR, together with the bottom-up review of the Department and a number of other measures that we are taking internally to clarify roles and responsibilities in what is a significant enterprise for this country—that is, homeland security.

We believe that the QHSR lays this out in a clear fashion, the roles and responsibilities of other Members, other parts of the Federal Government, State, local, law enforcement. It is an enterprise to ensure that this homeland is a place where the American values, aspirations, and way of life can thrive.

Mr. CARNEY. Okay. Thanks. Just one more question, and you didn't answer my second question, my first comment. Do you know why the Secretary said the system worked in her first reaction?

Ms. LUTE. Congressman, as she has made clear, she was responding to a series of questions that were also related to what are you doing in response to this information? What are we doing now to ensure that the traveling public is safe—planes in the air, airlines? What information are we pushing out?

Mr. CARNEY. Thank you.

Mr. Leiter, I just have a couple of moments left. By the way, sir, I respect you enormously and what you bring to the table, and I really want to know from your perspective, was there a single point of failure, a double point of failure, multiple points of failure in the Christmas day attack?

Mr. LEITER. Multiple.

Mr. CARNEY. Multiple.

Mr. LEITER. Yes.

I am trying to save you time, Congressman.

Mr. CARNEY. We will have a chance at some more questions, Mr. Chairman?

Chairman THOMPSON. Well, we can, or we can submit them for the record and get a response.

Mr. CARNEY. Okay.

Chairman THOMPSON. Multiple probably could go a long time.

Mr. LEITER. Congressman, if you would like me to expand, I always can, but I was——

Mr. CARNEY. Well, no, no, as the Chairman of the Oversight Investigation Subcommittee, I think maybe we will have you come in and chat with us a little bit. I will appreciate that.

No more questions, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

I don't want the committee to be misled. I have talked with the Secretary 2 days ago. We did not talk about her non-attendance or attendance at this hearing. Staff did communicate based on a directive we received that the Secretary would not be here, and we worked on Deputy Secretary Lute's presence.

That changed. At a minimum, based on that change, somebody could have communicated back to the committee one way or the other that we told you we weren't going to be here, we are here now, but we still can't come because of some other things. That is the courtesy I think the committee still deserves, and it does not require comment.

The gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman.

Mr. Leiter, based on your testimony, your written testimony and also your testimony that you gave last week before the Senate, it appears you believe that the Federal Government did in fact collect the dots, but did not recognize the linkages between those pieces of information. Is that a fair assessment of your statement, your position?

Mr. LEITER. Yes, definitely.

Mr. DENT. Isn't it true that the NCTC is designed to be a major, if not the premier intelligence fusion and analysis center?

Mr. LEITER. We have the statutory responsibility to be the primary analytic center for counterterrorism, and we along with the CIA have primary responsibility on it.

Mr. DENT. Thank you.

I also understand that the Intel Authorization Act of 2010 that passed the House Permanent Select Committee on Intelligence, but was not considered on the House floor, included sharp decreases in staffing levels for the Office of Director of National Intelligence. Isn't it true that your staffing at the National Counterterrorism Center is included in those DNI staffing levels and could have been very negatively impacted?

Mr. LEITER. Congressman, that is correct. As Director Blair noted, I believe, last week, my discussions with him in December were about how I was going to absorb cuts of up to 20 percent of my personnel areas to include analytic and watchlisting personnel.

Mr. DENT. So then do you have enough analysts to connect these dots?

Mr. LEITER. Well, believe me, it is a very, very small silver lining and not a silver lining I really wanted, but those initial cuts have

now been canceled for us. We have been working with the DNI and the——

Mr. DENT. So you do have enough analysts?

Mr. LEITER. No. I have already discussed with the DNI, and he has discussed with the Office of Management and Budget the need for additional analysts and individuals to work on watchlisting. So we enhanced those watchlisting records, so the right people are on the No-Fly list, the Selectee list. Right now I don't have enough people to do that.

Mr. DENT. So you are saying, then, additional analysts, and not fewer analysts, as HPSI proposed, that would help you accomplish your intelligence fusion mission?

Mr. LEITER. Yes, but I do want to make clear I don't look at this as this great opportunity to grow.

Mr. DENT. I understand.

Mr. LEITER. I look at it as the realization that we can't do the mission as expected, and we weren't doing as well as we did because of the assets we didn't have and the assets we were potentially losing.

Mr. DENT. Thank you, sir.

To Deputy Secretary Lute, I understand that while at the Schiphol Airport in Amsterdam, they have these full body imagers, as you know. They were not used at the checkpoints for the flights bound for the United States on Christmas day. In fact, within the United States we have only 40 of these machines at about 19 airports.

While I know that you can not guarantee protection, particularly when you are relying on human interpretation of an image, do you believe that the whole body imager would have had a better chance of detecting or identifying Abdulmutallab's explosive device than the current technologies employed at airports?

Ms. LUTE. Congressman, we believe it represents an improvement over our current capabilities, but again, it is only part of a layered system.

Mr. DENT. Understood. In order to address privacy concerns, some of the local vendors have developed these so-called auto detection software for their whole body imaging equipment with the goal of getting the TSA image observer out of the process. This auto detection technology, I am told, is currently being tested over in Schiphol and in Amsterdam.

Is the TSA, the Transportation Security Lab, or the S&T director examining this auto detection technology? If so, when can we expect to see some preliminary results?

Ms. LUTE. We are examining all aspects of advanced imaging technology, whole body imaging. We are aware of some of the technologies that exist out there, and we are also engaging in dialogue with our international partners like the Dutch to see what they have, what they are using. We believe this is an enhancement.

We take the privacy concerns very seriously. There are a number of measures in place with respect to whole body imaging now, the dislocation of the observer, the non-retention of image. But we believe that this is an area where we don't want to settle for just existing technology, but also want to explore most promising new.

But we also don't want this to take forever. We want to put tools in the hands of screeners now to enhance security.

Mr. DENT. Good. Then I hope you will certainly communicate with our friends in the Senate that stripped the amendment that was placed in the TSA authorization by the House that would restrict the use of these whole body imagers.

Finally, there appears to be a debate on which advanced technology system is better—backscatter radiation or the millimeter wave technology. Have you done an analysis on the health and safety of both of those types of systems? Did you identify any risks in multiple daily exposures?

Ms. LUTE. So, Congressman, I am aware that there are differences. I am not a scientist. Our science and technology folks, together with the Department of Energy and the National labs, are working with TSA on this and other technologies as part of a layered defense.

Mr. DENT. Could somebody report back to us? Could somebody send a report back to us, which is the better technology?

Ms. LUTE. Yes.

Mr. DENT. Thank you.

I yield back.

Chairman THOMPSON. Thank you.

We will get the gentleman's question answered by the Department. Be happy to.

The gentlelady from Ohio for 5 minutes, Ms. Kilroy.

Turn your microphone on.

Ms. KILROY [continuing]. The responsibility for failing within their respective organization. I think coming before this committee is part of that acknowledgment of responsibility and the oversight that it ruled as given to this body and to the United States Congress.

I think it is critically important that once we acknowledge the errors, that we also provide a plan or hear from you your plan to fix, to correct the problem, to make sure that people aren't becoming complacent in the years since 9/11 and protect the flying public. I thank those of you who made very clear statements in your testimony, as you did, Director Leiter, about that level of responsibility.

The more I hear about the Christmas bomber, the more I am amazed at how he got on the plane. That continues today to really stun me, that given the level of information, granted in different parts of the system, that there was sufficient information that, at least to me, it seems that he should not have been allowed onto that plane.

I keep learning things through hearings, through briefings, and through public news reports, that news reporters managed to get some information that had not been shared with the committee in prior briefings. But there was sufficient information, apparently, for him to be tagged for questioning when he got off the plane. I don't understand, I guess, why the Customs and Border Protection was the agency that was charged with questioning him when he got off the plane.

Ms. LUTE. Congresswoman, that is we have standing protocols that have been in place in this case since 2006 related to admissibility issue questions. The Customs and Border Protection persons

were prepared on the basis of that information to question him when he arrived.

We have changed that process. We now take that kind of information and push it forward to a pre-boarding opportunity that individuals be questioned before they get on planes, precisely because we recognize now that there is important information that can help us understand whether or not an individual poses a threat to aviation security, and so we have changed that process.

Ms. KILROY. Well, I appreciate that things have moved forward and people will be getting questioned ahead of the process.

But when you have this incident that has occurred—and thank God that actions were taken that all passengers and crew were able to get off that plane safely—but once you have this person, who has attempted this atrocious act, when and who, what agency should be involved in taking custody of that person? Who is trained to interrogate a terrorist? Who has ultimate authority in the chain of command in this type of situation?

Ms. LUTE. I can only speak to the part about the information that we had regarding admissibility. No one is satisfied that this individual got on this plane with this material. It should never have happened, and we have to do everything we can so it doesn't happen again.

We are taking the information we have about admissibility. He was at no time identified as a No-Fly or Selectee, which would have triggered certain actions prior to his boarding.

Ms. KILROY. I understand that, but he took actions on the plane. Everybody on the plane was aware of that. People on the ground were aware of that. So are Customs and Border Patrol agents trained in the science of interrogating a terrorist that has been taken into custody?

Ms. LUTE. He was handed over to the Department of Justice and the FBI.

Ms. KILROY. So the reports that I read that Customs and Border Protection interrogated him for an hour before he was turned over to the FBI—you are saying that would be incorrect, then?

Ms. LUTE. No. Customs and Border Protection had him upon presentation for entry, and he was handed over to law enforcement officials.

Mr. LEITER. Congresswoman, if I—I got it.

Ms. KILROY. Yes.

Mr. LEITER. He was initially arrested by the Customs and Border Protection officers, who were there at the airport. Immediately upon being removed from the aircraft, he was immediately turned over to the Federal Bureau of Investigation.

Ms. KILROY. I also want to endorse the line of questioning that Congressman Rogers led with respect to the use of canines, because I think that they have amazing abilities to detect, and they are very observant of body language as well as their use of different senses.

With respect to the changes in the visa process, have there been any changes in the length of visas that are going to be offered, allowed to people so they could come to this country?

Mr. KENNEDY. Mr. Chairman, should I answer the question?

Chairman THOMPSON. The gentleman will answer the question.

Mr. KENNEDY. I will be glad to see the Congresswoman and come visit with her and discuss that or submit an answer for the record, whichever you prefer, sir. I am prepared now.

Chairman THOMPSON. You can answer the question now.

Mr. KENNEDY. Ma'am, it really doesn't matter whether a visa has a validity of 1 day or 1 year. If information comes to us on the day after a visa issue or 30 days after or 90 days after, if the intelligence or law enforcement community comes to us and said, "You cleared this person, because there was no record when you cleared them. We now have something new on this person. That is, he or she is a danger to National security," we revoke the visa that day.

Ms. KILROY. Thank you.

Chairman THOMPSON. Thank you.

The gentleman from Georgia for 5 minutes, Mr. Broun.

Mr. BROUN. Thank you, Mr. Chairman. Mr. Chairman, during your opening statement you seemed to blame the Bush administration on this instance on Christmas day. To me there is a whole lot more going on here than just blaming President Bush and his administration, because I think this administration has a lot to blame, too.

Deputy Secretary Lute, I assume that you are just a good soldier and carrying out the orders that you were given by your chain of command. You mentioned attempted attack, and they have actually—before your testimony, you just talked about that during your discussion about the Secretary not being here.

I am incensed, frankly, that she is not here. Even the foreign visit was to brief people in Europe, and she ought to be here briefing these people in this committee who have responsibility to ensure the safety of the American public.

Also, the Secretary said that the system worked, which is hogwash. The Chairman asked if there was any disciplinary action being taken, and all of you all said no. Frankly, I am incensed by that, and I think the President of the United States should ask for the resignation of Secretary Napolitano and get somebody there who is not in la-la land. Frankly, I think she is in la-la land.

I don't know who else in your Department is, but whoever he is, they need to go, because the safety of the American people absolutely is critical on having good leadership at the top. I don't think we have that here in this country.

So I am incensed. I think other Members of this committee are incensed that the Secretary won't take her time to come here and face this committee. I hope the President will take disciplinary action and get rid of her and get rid of anybody else in your-all's Department who are in denial, frankly, about the seriousness of this.

In the United States Marine Corps, I was taught to know your enemy. I have heard testimony from some other of the members of this panel. They seem to get it. But I don't think the Department of Homeland Security, and I am not sure the President and his administration, get it.

We are facing not a war on terror. We are facing a war against a group of fascists in this country who hate this Nation, hate everything we stand for, including the freedom, including the freedom we give to women, and they want to destroy this Nation. We must as a Nation start facing the fact that these are Islamic fascist ter-

rorists, who want to use that tactic in a war. Terrorism is only a tactic. We are not fighting terrorism. We need to stop talking about that.

To me the failure here is political correctness gone amok. There are many Members of this committee, principally on the other side, who don't want profiling. We just had a hearing about the undocumented attendees to a State dinner. We have got a lot of undocumented attendees in this Nation that the State Department allows to come into this country, and some that are documented.

We need to change the whole philosophy of how we are trying to protect this Nation. I don't think we are doing a proper job. Frankly, I am incensed. I hope the President will start paying attention to what is going on here and will stop this inane thought of not profiling people that are entities that we know hate our Nation and will do what is necessary to protect the American public and keep this Nation safe.

Mr. PASCRELL. Will the gentleman yield?

Mr. BROUN. No, I won't.

Mr. PASCRELL. You won't yield?

Mr. BROUN. No, I won't.

Mr. PASCRELL. Okay.

Mr. BROUN. Because I have got just a minute left, and so I want——

Mr. PASCRELL. I will just say it later, so it doesn't matter.

Mr. BROUN. But it is absolutely critical that this administration take serious our enemy. America needs to know its enemy. It is radical—it is a bunch of radical folks all over the world, who want to destroy it. They are going to continue to attack us.

Whole body imaging is not going to prevent, and even the canines are not going to prevent, bombings. There is no way unless we search every body cavity on every person who wants to come into this Nation.

But we know one of the big, glaring, flashing dots is radical Islam. We have got to start focusing upon that. There is absolutely no question about that. Our people are going to die. Those who are worshiping at the altar of political correctness are going to—that worshiping at the altar of political correctness and not profiling our enemies is going to result in killing American citizens.

With that, Mr. Chairman, I yield back. My time is up.

Chairman THOMPSON. Thank you very much.

The gentleman's time has expired.

We have two votes scheduled, and we expect to return in about 25 minutes. The committee stands in recess.

[Recess.]

Chairman THOMPSON. We would like to reconvene the recessed meeting.

We now will begin questioning with the gentlelady from Nevada, Ms. Titus.

Ms. TITUS. Thank you very much, Mr. Chairman. I do have a couple of questions. I would like to start with Mr. Leiter.

On several points in your written testimony, maybe not so much in your oral testimony, you note that the intelligence community possessed strategic intelligence regarding al-Qaeda in the Arabian Peninsula, and you note that they had—and I put this in quotes—

"had the intention of taking action against the U.S. prior to the failed attack on December 25, but we did not direct more resources against them nor insist that the watch list criteria be adjusted prior to the event."

You also note that the NCTC and intelligence community had long warned of the threat posed by this group in the Arabian Peninsula. But it appears that despite your intelligence on this and your concern about it expressed here, that the necessary steps weren't taken to prevent this.

So I want to ask you who was receiving your reports about this intelligence? Why do you think they didn't respond to it in the appropriate way?

Mr. LEITER. Congresswoman, I think everything you said is correct in terms of encapsulating my statement. All of the intelligence we write goes to a broad array of consumers ranging from the President to the members of the Cabinet, deputy secretaries and the like.

I wouldn't say, though, that nothing was done. It is that the things that were done turned out not to have been ones that stopped this threat. There was forceful action taken on a number of fronts to try to disrupt various threats from al-Qaeda in Yemen. What it didn't do is detect this thread or stop this particular individual.

Now, steps were taken. Why do I think that we didn't shift enough focus onto this individual? I do think that al-Qaeda in the Arabian Peninsula, although we saw a desire and a possibility to strike the homeland, I don't think we fully realized the speed with which they had moved and actually put that desire into action.

Ms. TITUS. Well, I would ask you going forward, which is the important thing, do you think we are putting enough resources and enough attention on this growing threat in the Arabian Peninsula?

Mr. LEITER. I think we have begun to move those resources. I still don't believe we have all the resources we need. I would also add that I remain particularly concerned, as I have testified before this committee and others previously, I remain particularly concerned not just about Yemen, but also in Somalia and the flow of Americans of largely Somali descent to Somalia. I think that poses a similar threat. Although Yemen is the subject of today's hearing, we have to remain very, very focused again on Somalia and, of course, on Afghanistan and Pakistan.

Ms. TITUS. Do you feel like the people who are higher up, all this group that you report to, are taking your warnings seriously?

Mr. LEITER. I think without a doubt. I believe the President's immediate direction on shipping resources, Director Blair's intervention here to make sure we have the resources, and the rest of the intelligence community, I think we have.

Ms. TITUS. Well, we need to. There is no question about that.

Mr. LEITER. I agree with you wholeheartedly.

Ms. TITUS. Just one other quick question for Ms. Lute. I would ask you—now, we have put so much focus on the international flights, because this incident was an international flight, but we can't forget that 9/11 involved domestic flight. We are not ignoring them or letting them go by the wayside as we now suddenly focus on Schiphol, are we?

Ms. LUTE. Absolutely right, Congresswoman. We are not neglecting any part of the aviation security systems, nor are we neglecting our land and sea borders, as we have this particular focus on air. We have a number of measures in place across the board to enhance our vigilance, increase our information gathering and sharing, as we have been discussing, working with technology in this multi-layer defense domestically as well as internationally.

Ms. TITUS. Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you very much.

The gentlelady from Michigan, Mrs. Miller, for 5 minutes.

Mrs. MILLER. Thank you very much, Mr. Chairman.

You know, there have been lots of questions from my colleagues about the process and the failures of our protocol, et cetera. Many people have commented about the absence of Secretary Napolitano, and I would associate myself with those remarks.

However, I will also say that it is stunning to me that Attorney General Holder or nobody from the Department of Justice is here to talk to this committee and to testify to this committee. I would respectfully request that at some point he does testify before this committee.

Our responsibility is to have oversight, and I want to focus, I think, on what has happened since the attempted act of war, because that is what it was. It wasn't a criminal act. It was an act of war by a terrorist, an enemy combatant. I was stunned that this terrorist was not turned over to the military.

Again, I am just incredibly dismayed no one from the DOJ is here. Yet, it was they, under the direction of Attorney General Holder, that made this decision to turn this terrorist over to the FBI, and not as an enemy combatant. He made the decision. I believe that the attorney general is creating a culture at the Department of Justice that fosters an ideology of approaching this war on terror like a simple police action.

I will cite a couple examples of why I say that, because I do believe it is dangerous to our security, and I am very concerned about it. We know, for instance, that before becoming the attorney general, Eric Holder and his law firm represented accused terrorists that were in the custody of the military, and he urged their release to the civilian justice system. That includes Jose Padilla. They were very proud about giving free pro bono legal service to 17 Yemeni and one Pakistani, who currently are at Gitmo.

We know that he and President Obama have placed many of these attorneys in high-ranking positions at the Justice Department—again, attorneys that provided free, top-flight legal assistance to enemy detainees.

I mean my husband's an attorney. I know a lot of attorneys. You might have pro bono work for a child abuse case, domestic violence case. This is what they decided they wanted to give free legal advice to: Enemy detainees.

We also know that the attorney general has stonewalled Senator Grassley, who is attempting to discover who these high-ranking Justice officials are and what their role is in making these decisions.

We know that the attorney general has been a huge advocate to close Gitmo and to bring these detainees to the United States. We

know that the attorney general has made the decision to bring KSM and others implicated in the 9/11 conspiracy to New York City for trial without consulting any security officials in New York or other high-ranking officials in the military or intelligence communities.

Our Ranking Member mentioned that he had not consulted them—actually, I think it was on the Jim Lehrer Show, where he said he consulted his wife and his brother before he made that decision. So I have concern with that.

We also know that in this instance the attorney general did not share, in the instance of the Christmas day bomber, that he did not share the intelligence gleaned from the Christmas day bomber with the military or intelligence officials before giving the Miranda rights to this terrorist.

I know the President has said that no one is accountable, or that no one will be held accountable, no single person, but I believe that President Obama must hold Attorney General Eric Holder responsible for the loss of additional intelligence that would have been gained to protect our citizens from future attack.

He has been rather flippant, I would say, in saying that he is not afraid of Khalid Sheikh Mohammed being given a platform to spout his anti-American rants in our justice system. He says we have nothing to fear from giving terrorists constitutional rights and access to our court. I disagree.

I am the only Member of this committee from the Detroit area, and this incident may have faded in the front of many papers, newspapers, and media across our Nation, but I will tell you in Detroit we are looking every single day at this terrorist, this enemy combatant, an act of war against America, who was treated at the University of Michigan Burn Center, which is probably the best burn center in the entire world, and not only given one free court-appointed, taxpayer-funded attorney, he has three—three—attorneys.

We are looking every day at what is happening at the Federal building in the city of Detroit, all of the expense that is being taken on by the Detroit Police Department at a time they can't afford that kind of expense, and other security officials, just to make sure that we have no incident there.

The first thing this guy hears when he gets off the airplane is, "You have the right to remain silent." Here is your great justice system that we are having here in America. It makes me crazy.

In the absence of anyone from the Department of Justice, let me just ask Director Leiter. Do you think that Attorney General Eric Holder's decision to Mirandize this guy denied us the opportunity to garner very valuable information? Do you think that if we got a terrorist in Afghanistan or Yemen or in theater and we only interrogated him for 50 minutes, that that would be adequate?

Mr. LEITER. Congresswoman, I will try to answer, of course. I mean I am not from the Department of Justice. One thing I do want to correct, though. I don't believe it is correct that the information that was garnered during those initial 50 minutes of interrogation was not shared with the intelligence community or with the Department of Defense. I say that, because I was on the video teleconference that evening, and——

Mrs. MILLER. If you could, just a moment. I recognize he did share the information, but he did not share the information that he was going to Mirandize this, and that was my point. Nobody was asked about that. That was Attorney General Eric Holder's decision, apparently.

Mr. LEITER. I apologize, Congresswoman. I understood. I just did want to make clear that the information that they garnered was immediately shared with the intelligence community. It was put to action. I think there was information that was garnered from that initial 50 minutes of interrogation that has been quite valuable.

Mrs. MILLER. Well, my time has expired, so I would just simply say that, Mr. Chairman, we are facing a new type of enemy who doesn't consider the battlefield to be just in Yemen or in theater. The battlefield that day was Seat 19A on that Northwest flight, and these are enemy combatants. I think it is dangerous for America to treat them as civil criminals. Thank you.

Chairman THOMPSON. Thank you very much.

For the record, as you know, the Minority has an opportunity to request a witness, and it could have very well been the Minority's option to request Attorney General Holder for this hearing, and they did not.

The Chairman recognizes the gentlelady from New York, Ms. Clarke, for 5 minutes.

Ms. CLARKE. Thank you. Thank you very much, Mr. Chairman.

Let me just say that as a New Yorker, I know that it is possible that we have under previous administrations tried individuals who seek to do us harm—terrorists, if you will—in civilian courts and been very successful there. So, you know, I think that this is an issue we can go back and forth with.

But I think that we have to also make sure that in doing so we don't manifest through our conversations just the outcomes that we are seeking to prevent. That is encouraging others, by labeling enemy combatants, to become enemy combatants.

I think that we have the power and an expertise in our Nation to address all of these concerns, and that is why we are here today to encourage one another to use those talents and expertise to do what needs to be done to protect the American people. Certainly, as we review our failures and our mistakes, we learn from them to strengthen ourselves as a Nation, to do what has to be done to protect the American people.

So having said that, my concern has to do with our ability to manage these databases. I have felt all along since, really, hearing from constituents in my constituency that they have had a very hard time getting off these lists, that we were building a quagmire. I say that, because at a certain point the list becomes the proverbial trying to find the needle in a haystack, when you are not purging it, when you are not moving people through the cleared list.

So I am just concerned that as we build out this data infrastructure to be able to find individuals, to communicate in real-time about individuals that we may have on one list, but may not be on another, that the time that it takes to scan, to data input, because it is my understanding that particularly in the TIDE database, that there are people with similar names in addition to the actual

name. I am sure once you sort of plug in a name, you are going to get a list of names.

I want to raise the question with each of you about how we refine our capacity through data maintenance and gathering to be able to do that type of ID in real-time. The GAO has found that agencies involved in screening international visitors to the United States do not screen individuals against all records in the watch list.

Can we say that the system has become too cumbersome for accuracy of screening to become more difficult over time? I would like to get that response from each of you.

Ms. LUTE. Congresswoman, perhaps I will begin, and then Director Leiter may want to add to it.

There is an enormous amount of data being gathered. It is one of the tools that we use for aviation screening, and we use it for other purposes as well. We are constantly refining our processes to ensure that we have the accurate information of an individual that is in these databases.

One of the issues that I raised in my conversations with international colleagues, and the Secretary certainly emphasized as well, is creating a standard for passenger name records so that we have as much information as we possibly can about individuals. Are they who they say they are, and are they fulfilling the intent they declare?

We do and have created a sort of one-stop for de-confliction when people find themselves on a database erroneously. It is called the Travelers Redress Information Program. It is not yet a perfect system, and we acknowledge that, but we are working very hard to address it.

Mr. LEITER. Congresswoman, believe me, I am very sympathetic to your concerns, because I have the responsibility to get through all of this data and make sure it is clean. We want it as clean a system as we could have. I will note a couple of things.

First, I think it is important to note that United States persons make up a very small percentage of our high database, very small percentage. In fact, you can only be in our database if you are the subject of an active FBI investigation. Within 24 hours of that investigation being closed, you are purged. I think we have a very good record for meeting that standard. So I think that is point No. 1.

Point No. 2, are there simply better ways of doing this? There undoubtedly are. Any names-based screening system has inherent weaknesses. It requires not just a name, but you also want additional data about that person if you can, whether it is a birth date or a passport number.

The next step, really, is moving towards greater integration of biometrics. Under Secretary Kennedy has already noted some of those advances that we have made. I think both at the initial screening when someone is getting on an aircraft, but certainly when they are getting a visa, when they arrive at a port of entry, the integrated use of biometrics, which is there already, is extremely helpful.

It has to be expanded. There is a significant resource tail, and there is also a significant civil liberties concern that have to be addressed as we do this. But we know that is the right way to go.

Chairman THOMPSON. Thank you very much.

The Chairman now recognizes for 5 minutes, Mr. Olson.

Mr. OLSON. Thank you very much, Mr. Chairman.

Before I get started on my line of questioning, I would like to identify myself with my colleague from Michigan's remark on the decision to use the criminal justice system of our country instead of the military justice system to prosecute this individual.

Very briefly, what I have understood is when he was brought off that aircraft after he had tried to kill all the people aboard that plane, he was taken into custody, was taken to the hospital for medical treatment.

Two FBI agents began asking questions. He was giving them actionable intelligence for at least 50 minutes, intelligence that saves lives. Those agents that were asking those questions—there is an exception to the Miranda rights that if you believe there is imminent information that is going to save lives—there is another bomb on an aircraft or, as we saw unfortunately on September 11, there are other aircraft in the air with bombers like Mr. Abdulmutallab on it—then they have discretion to ask questions. Again, for 50 minutes, by reports, they got actionable intelligence information.

Five hours later, another group, a "clean team," showed up. The first thing they did was read him his Miranda rights. No surprise, he hasn't talked since then. We will never know what information we have lost and what risks and what damage we may put to our country by not interrogating him fully and getting all the information he had to learn about what al-Qaeda's doing in Yemen.

I would like to change tactics here, change the tone of my—I want to talk a little bit about—you know, one thing that I believe is the most information we can have and the quicker we get it, the earlier in the whole process, the better chance we have to thwart it.

As we know Mr. Abdulmuttalab, it seems to be that he got, at least from the information I have had, that his radicalization, his radicalization happened while he was going to school in Great Britain in England. The British intelligence states he is—Islamic student organization in their fight against extremism. Abdullahmatal—I am sorry—Abdulmutallab was the fourth president of an organization like that in Great Britain to be charged with a terrorism-related offense.

My question is is extremism on college campuses something that the intelligence community is focused on, both abroad and here at home?

Mr. LEITER. Congressman, I would be happy to talk about this more in a closed hearing. I will say we have worked very closely with the British as they look at their groups. We have consistently seen connections between terrorists threatening the United States and terrorist activity in the United Kingdom.

One of the things we have done as a response to this is reinvigorate that information sharing to make sure that we have full visibility into whether or not it is the schools or the garage mosques

or simply the splinter groups. I agree with you. We have to make sure this information is shared very quickly.

Mr. OLSON. Have we seen anything here domestically akin to what is going on in Great Britain?

Mr. LEITER. Congressman, we have never seen within the United States nearly the scale, scope, depth of radicalization that we have seen in the United Kingdom. We have pockets of it, and we are concerned with it. I wouldn't associate it with any single environment within the United States.

Mr. OLSON. Thanks for that.

One more question. Maybe I appreciate if it is two sentences across the line in the classification system. But one individual I am concerned about, and I hope I pronounced this right, is Sheikh Anwar al-Awlaki, who had contact, we know, with Mr. Abdulmuttalab, probably in Yemen, probably as part of the, you know, the organization that helped him get trained and certainly can keep him indoctrinated.

Also concerned as a Member from Texas. Apparently, there were e-mail contacts between him and Captain Hasan who, as you know, killed 13 soldiers at Fort Hood. I am just concerned. Do you know of any other? He is using 21st century technology—videos, teleconferencing technology, particularly, you know, of sending that signal to England and Great Britain again. I know I am harping on them, but is there any evidence that he has been doing that home here in our country?

Mr. LEITER. Congressman, I really can. I can't go into great depth here. I will tell you that the intelligence community has been concerned with the activities of Anwar al-Awlaki for some time. He was initially investigated in association with the events of 9/11, when he was an imam in San Diego, later in Northern Virginia.

I can tell you that even well before Major Hasan, but certainly after the events of Fort Hood, NCTC, the FBI and other agencies have been very, very focused on Awlaki, but also other individuals like Awlaki, who are savvy to Western ways, Western technology, modern technology, and their ability to reach into our border through this technology.

Mr. OLSON. I see that I have run out of time. Thank you very much. Stay on him. Thanks.

Chairman THOMPSON. Thank you very much.

The gentleman from New Jersey, Mr. Pascrell.

Mr. PASCRELL. Chairman, thank you.

Mr. Chairman, many of us have stressed one thing as Members of this committee. If there is one thing we have stressed, it is that the bureaucracy itself is as great a threat to our National security as anything else. You heard the bureaucracy today, part of it.

Let me just point out that Congress is not exempt from this criticism. Indeed, this is at least the fourth of different full committees to hold a hearing on the attempted attack of December 25. This strikes me as entirely counterproductive to what we are trying to accomplish.

It seems crystal clear to me that the events of December 25 were allowed to occur, because once again we have failed to connect things in the information that we already had, we already knew

about. Once again, our intelligence agencies failed to communicate with each other. This is a human error, not an electronic error.

We spend a lot of time talking about the state-of-the-art of these machines that are in airports and aren't in airports. We have not told the American people the truth. Many binary explosives are not detectable at this point.

We established a Director of National Intelligence, the DNI, to serve as the head of the intelligence community. It consists of 16 different agencies spread throughout the Federal Government—16. Each of these intelligence agencies have different standards for their personnel—each of them. 9/11 9 years ago—they still have different standards.

I would conclude that you are not going to get the proper relationship amongst these agencies until you have basic standards. In fact, the agency within all of the 16 that has the toughest standards is the CIA. I would begin there.

But we established that position of Director of National Intelligence to finally provide some leadership and guidance over the intelligence community so that we could finally close the gaps in this information sharing. Clearly, we are not there yet.

What troubles me most about this incident was that we allowed this individual to receive a visa in the first place to enter the United States. I think of all those families who have tried to get united and were denied a visa, because they thought if they came to the United States, that they wouldn't go back. Many of those cases were adjudicated correctly. Many of them were not.

We never took steps to revoke his visa before he entered a foreign airport to travel. We already had negative information on this individual. Not only had the State Department spoken to his father, but we knew that he traveled to Yemen. For young men to travel from Nigeria to Yemen with no known legitimate purpose—that should raise a number of red flags.

Mr. Leiter, Director Leiter of the National Counterterrorism Center, is often described as the arm of our intelligence community that is responsible for—I hate the phrase, and probably you do, too—connecting the dots on intelligence gathering. Do you agree that is your primary role and responsibility? If so, doesn't that hold you primarily responsible for the failure to connect the dots on the intelligence we already had on this individual?

Mr. LEITER. Absolutely. I said several times, Congressman, NCTC is the primary analytic organization. It was our responsibility to do this. We didn't do that. There was another organization that also had responsibility under the DNI's standards. That didn't occur there either.

Mr. PASCRELL. Do you wonder why some of us have concluded that maybe we have added an extra layer of bureaucracy to the intelligence apparatus that is slowing us down to get to the goal line? Do you wonder why we think that at times? Or do you think that the DNI is absolutely necessary to stop those who wish to bring harm to our families, to our neighborhoods, and to our borders? What are your thoughts? I know you work for them. What are your thoughts?

Mr. LEITER. Congressman, I think the DNI is a useful construct to advance intelligence reform. I do not think that the DNI in this

case, this construct or the layers, was the problem. I mean I think many of the weaknesses you have identified are fair weaknesses. I just don't think they were the issue that caused this failure here today.

Mr. PASCRELL. Do you have the authority you need to work with intelligence across our Federal departments and agencies? Do you have the authority to do that?

Mr. LEITER. Congressman, it is not easy for an——

Mr. PASCRELL. I am not saying it is easy. Believe me, I am not, Mr. Leiter. But my question is very specific.

Mr. LEITER. I do not, nor do I believe the DNI, as currently constructed, has all of the authority necessary to move all of the information in a way that will maximize the likelihood of detecting these plots.

Mr. PASCRELL. Mr. Chairman, I hope that—and I know you were listening, and the Ranking Member, to the last answer. The gentleman has been forthright. I thank him for his service to his country. We have created—my conclusion, not their conclusion—a monster. We will never get the safety of the American citizens as we build these levels of bureaucracy that do not get to the heart of the issue.

I would ask you to go back——

I would ask you to go back, Ms. Lute——

I would ask you to go back, Mr. Kennedy—to look at this bureaucracy as being the systemic problem. This is human error, but maybe it is human error precipitated by the fact that we have created a bureaucratic nightmare so that no one is held accountable. That is why you create bureaucracies, you know.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

The gentleman's time has expired, but we always recognize his leadership.

Mr. Leiter, In light of your question, we are going to ask you to provide us what authority you think you need in order for you to do your job in a manner you deem necessary.

Mr. LEITER. Mr. Chairman, I am happy to do that, and I would work with the DNI. I would add that although I say that, I don't have any particular authorities right now that would quickly ensure that every bit of this data is shared with every other component of the intelligence community.

Chairman THOMPSON. I understand, but you just said in response to the gentleman from New Jersey's question that you don't have it.

Mr. LEITER. Mr. Chairman, I am happy to go back, and we will come back with recommendations to you.

Chairman THOMPSON. Thank you very much.

The gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

I thank the witnesses for appearing today.

I believe, as has been indicated, this was a failure of intelligence, but I would like to make sure that I state that it was not a failure of all intelligence personnel. I say this, because we have many people who risk their lives on a daily basis. Some, by the way, lose

their lives, as was evidenced by the recent event that we need not go into.

Their families—they see these hearings. I don't want their families to assume that I have concluded that all intelligence officers are failures, because I want them to have the morale necessary to do a very difficult job under circumstances that are extremely complicated, and sometimes almost impossible, if not impossible.

I believe that the structural integrity of a plane at 3,000 feet traveling at 500 miles per hour is of paramount importance. It is as important as anything that we deal with. Because the structural integrity of that plane is so important, I want a system that will reveal and allow us to capture the Omar Farouk Abdulmutallab.

But I also want a system that will capture the Abdulmutallab who doesn't pay cash, the Abdulmutallab who doesn't ask for Seat 19A, the Abdulmutallab whose father doesn't turn them in. I want a system that will capture the Abdulmutallab whose religion I am not aware of.

If we focus only on connecting the dots that could have been connected to the exclusion of designing a system that will allow us to capture the Abdulmutallabs who are not obvious, who are not intuitively obvious to the most casual observer, if you will, it would be a mistake.

We must have a system that will reveal the Abdulmutallab who is Anglo-Saxon and has blond hair, because this beast that we have to deal with continually metamorphoses. It becomes something else somewhere else. If we only assume that it will be tomorrow what it is today, we will make today's mistake, and it will impact tomorrow.

So the system that I am looking for is one that will allow us to understand, in my opinion, that the last line of defense is the airport. That is the last line of defense. The American people don't ask us to do the impossible. They do demand, however, that we do all that we can—that we do all that we can.

At some point the excuse that we didn't do all that we could is not going to be enough for the American people. So we have got a duty at these airports to do all that we can. We owe it to the intelligence officers who risk their lives every day to make sure that we do all that we can at the airports, our last line of defense.

A quick question, if I may. Did we know the religion of Richard Reid prior to December 2001?

Mr. LEITER. I don't believe so. I don't think we knew anything——

Mr. GREEN. I think that that answer suffices. The reason I asked is because if we focus on religion and then some other adjectives, we are missing a point here. I want to capture the culprit whose religion may not be the religion du jour for our purposes. This is serious business, and it goes beyond the ability to simply identify that which is superficial, the superficial social analyst who can come in after the fact and connect all of the dots and see how clearly we could have saved the day, had we connected the dots.

So I suppose I had more of a statement than questions for you, because I just absolutely believe that we must not allow ourselves to be trapped by religion and by ethnicity and place of origin. It is bigger than that.

Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman THOMPSON. Thank you very much.

The gentleman's time has expired.

The gentleman from California for 5 minutes, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I appreciate the time. I am sorry I couldn't be here during all of this, but I am divided between three different committees, and we just voted to impeach a Federal judge. I think it is only eight times in history we have done that, so I had to be there for that vote.

Yes, I hope we are not prisoners of wrong impressions either. But I also hope we are not prisoners of PC. We are in a war declared on us by radical jihad, radical Islam. That happens to be a fact. We didn't pick the war. They picked the war. I haven't seen too many Irish Catholic nuns blow themselves up.

Sometimes we do stupid things like having my 6-month-old granddaughter a couple of years ago taken out for a secondary search when they searched her diaper. That kind of stupidity hurts us, I think, even though we do it to make sure that we have some egalitarian approach to this.

Mr. Kennedy, let me ask you something. That is if the State Department had the information about Abdulmutallab from his father prior to issuing a visa, would we have issued a visa?

Mr. KENNEDY. Sir, if we had the information the father had presented before——

Mr. LUNGREN. Yes, that is my question.

Mr. KENNEDY. Yes, sir. What we would have done is we would have not issued the visa. We would have sent in to the intelligence and law enforcement communities a security and advisory opinion, ask them what additional information they had, and then made the decision on the basis of what additional information they provided as well.

Mr. LUNGREN. So if that is the case, why wouldn't we move to revoke the visa if we have that information?

Mr. KENNEDY. Because we sent the request in to the Visas Viper, sir, went into the intelligence and law enforcement community and ask them if they had any additional information on Mr. Mutallab.

Mr. LUNGREN. Does someone have a constitutional right to come to the United States?

Mr. KENNEDY. No, sir.

Mr. LUNGREN. Does someone have some sort of international right to come to the United States?

Mr. KENNEDY. Absolutely not.

Mr. LUNGREN. A visa is a discretionary action by the United States, right?

Mr. KENNEDY. Absolutely, sir.

Mr. LUNGREN. The granting of a visa. So why would you even hesitate about not granting someone a visa if he had that information from the father such as was given by Mr. Abdulmutallab's father?

Mr. KENNEDY. Two reasons, sir. First is context. We turn down almost two million—1.9 million visas a year. So we do not——

Mr. LUNGREN. Okay. I don't care about the other. I am asking you about this specific case. That is why I am asking.

Mr. KENNEDY. No, because, sir, there are people who come into embassies every day, every month, family members, disgruntled business partners, and others who say that so-and-so might be a terrorist. So we have been very carefully analyzing that. We consult with our partners.

Mr. LUNGREN. Okay. I understand that. Let me ask you this, then. So do we have a lot of fathers who have experience such as Mr. Abdulmutallab's father did, who turn their sons in with that kind of information?

Mr. KENNEDY. There have been family members.

Mr. LUNGREN. So there are a lot of them.

Mr. KENNEDY. There have been family members who——

Mr. LUNGREN. You know, I appreciate it. I don't like people getting cute with me. This is very serious business.

Mr. KENNEDY. Absolutely.

Mr. LUNGREN. The American people are asking us. I was just home. People are saying, "How in God's name can you screw up like this?" We have spent billions of dollars trying to do it, and we say, "Well, you know, a father comes in like this with this guy's pedigree. He says that about it. Yes, we got a lot of them." I would argue that you don't get a lot of them, and I would argue that you ought to be a little more serious about this then doing that.

Mr. KENNEDY. Sir, I am——

Mr. LUNGREN. Now, you know, it is easy to be a second, you know, on Monday morning quarterback, but when you tell me that, it bothers me a great deal.

Mr. KENNEDY. If I could just finish my sentence.

Mr. LUNGREN. You can finish your sentence, but we are in a serious question here about people who want to kill us, and you talk to me. It sounds like the State Department is doing things the way they used to do it.

Mr. KENNEDY. No, sir. The second part of my sentence, sir, is that we are reviewing all of our procedures. We regard ourselves as the first line of defense, and we have every intention. We are committed to——

Mr. LUNGREN. Well, you weren't the first line of defense here, were you?

Mr. KENNEDY. I believe we were, sir.

Mr. LUNGREN. This is amazing. I am sorry. It is amazing to me. So you don't—it didn't work the way it should, though, did it?

Mr. KENNEDY. Absolutely not.

Mr. LUNGREN. Okay.

Mr. KENNEDY. I said that in my testimony, sir.

Mr. LUNGREN. So you are reviewing the procedures and criteria. So what would do differently now, if you got this information? Or would you do anything differently, except make sure it went up the line?

Mr. KENNEDY. If he had been a visa applicant, we would have coded that information. We would have sent the inquiry to Washington. We would have asked other people in the intelligence community what——

Mr. LUNGREN. Okay. So he wasn't a visa applicant. He already had a visa.

Mr. KENNEDY. Right.

Mr. LUNGREN. So what change would take place now, if you are confronted with the same information, not applying for a visa, but he has a visa. This information is brought to you at one of the embassies.

Mr. KENNEDY. I would think, as you suggested, sir, we would do all more in-depth review to make sure that the information being presented to us was valid. Then if it was valid, we would move to revoke the visa immediately.

Mr. LUNGREN. Okay. I would just like you to bring one little bit of information back to the State Department. I have an adult daughter who was visiting Gambia the week after Christmas. She thought it might be important for her to go to the embassy to indicate that she was there—American citizen there.

She was told the person that would take that information was sick, and the person who was—or, excuse me, was on vacation—and the person who was supposed to take that person's place was sick. Therefore, she could come back in a week to tell them that she was there. She was leaving in a week.

I just want to tell you she didn't pull anything about being my daughter or anything else. I just happen to think that kind of a response to a simple American citizen going to a country saying, "You know, you might want to know I am here in case anything happens"—not that she thought anything was going to happen in that country, but that was the response she got.

Mr. KENNEDY. That was totally inappropriate and wrong, and I will look into that, sir. We encourage, we request, we have web sites to encourage any American traveler to record their——

Mr. LUNGREN. That is what she did. She was told to come back after she had left.

Mr. KENNEDY. That was an error, and we will look into it. Why? That is not our procedure.

Chairman THOMPSON. The gentleman's time has expired.

The gentlelady from Texas for 5 minutes, Ms. Jackson Lee.

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

To the witnesses, let me thank you.

I think all of us echo the fact that we know that there are men and women on the front line, and we appreciate their service. We also appreciate the leadership of the President of the United States as the Commander-in-Chief. He should be able to expect the highest level of performance of his staff, of his Executive staff, that he should also expect the Congress is a collaborator with him in team homeland security.

Unfortunately, I think that there were enormous challenges and missteps that did not equate to the team working together and playing on the playing field together. I frankly believe that part of it is, of course, some of the missteps of the United States Congress, some of the inability of the executive to listen to the Congress.

My subcommittee, the Subcommittee on Transportation Security and Infrastructure Protection, looked into the question of watch lists. We actually made comments about the burdensome method of that watch list, of how heavy laden it was, how inaccurate it was, to the extent that we had 8-year-olds, so we had an 8-year-old as a witness. Another 8-year-old had been interviewed. It is a simple task to look at that watch list and provide the intelligence

and the staffing to make it a watch list that is credible of the name.

The other broken part of the system is the responsibility still, as I understand it, on airline personnel as people come to counters and their names—they go to the back and check their names—civilians looking at issues that happen to deal with homeland security issues.

We have a problem and a crisis that needs to be fixed. A part of it is that we must acknowledge that we will not have people bearing flags running down airports and saying, "I am a terrorist." Individual operators and actors, franchising of terrorism, seems to be the call of the day, and then taking credit for it one way or the other. We know now that Osama bin Laden has taken credit for the December 25 action.

Many of us, who are not inside the Department, were aware that there was activity going on around the holiday. We know that that is the modus operandi of terrorists. Go when a country is focusing on something else. So my questions go to this whole question of interrelatedness.

Quickly to Secretary Kennedy, are your consul offices—do they have a direct connection to the watch list effort of Deputy Secretary Lute and the counterterrorism efforts of Director Leiter so that the Nigerian consulate person would have had that direct connection?

Chairman THOMPSON. Please use your microphone.

Mr. KENNEDY. My apologies.

We get daily and——

Ms. JACKSON LEE. Can they call back and contact a human being?

Chairman THOMPSON. Madam, well, just, I don't think he finished it.

Ms. JACKSON LEE. I understand, but my question is can they—I hear what he is going to say. The question is——

Chairman THOMPSON. Now, I didn't hear what he was going to say. Just let him answer. You have got plenty of time. I am going to be very nice.

Go ahead, Mr. Kennedy.

Mr. KENNEDY. The law enforcement and Homeland Security and intelligence communities provide us with information every day on new threats. We load that into our database, and that information is available to every embassy and consulate throughout the world.

Ms. JACKSON LEE. Does the consular general have the authority or the ability, or the individual who dealt with the father of the alleged perpetrator in the incident at December 25, to be able to call back on the telephone, on a cable, on an e-mail, or whatever is secure, to ask questions out of the Deputy Secretary Lute area or the counterterrorism area?

Mr. KENNEDY. What they do is they call the visa office at the State Department, which is our central repository and which is in daily contact via all the secure means with both as the National Counterterrorism Center, the Department of Homeland Security, the FBI's Terrorist Screening Center. Yes, ma'am. We are in contact with daily. That is one of the major improvements since 9/11. We are all lashed up as partners——

Ms. JACKSON LEE. But if you are in contact, what does that mean? Does that mean that the person who engaged with the father of the alleged perpetrator had the ability to get on the phone and call and get a quick answer of the person who answered the phone in Washington, DC? I am suspicious. There is an individual here talking about activity of an individual that has a visa.

Was there a direct link for there to be a response by checking live intelligence by way of a direct call to the counterterrorism or direct call to the watch list? Those are in two different areas.

Mr. KENNEDY. Yes, sir. He was not on the watch list. He was not on the Selectee list. The State Department, when the father came in, talked to an embassy officer, who then immediately reported to the consular section that this is the information that was received, and that information was immediately sent to Washington.

Ms. JACKSON LEE. Have you made changes to ensure that information that would describe someone as suspicious can be responded to quickly? Because frankly I believe that all that the father said was enough information for a well-trained official, whether they are State Department or not, that we are living in a different climate and maybe I should do something about it? Have you had a re-training of your staff around the country—around the world, rather?

Mr. KENNEDY. Yes, ma'am. We have sent out revised and updated instructions, and we emphasize that we have added additional information to the immediate report that is sent in—it is called Visas Viper—that notifies the Homeland Security and intelligence and law enforcement communities that the State Department has come into piece of information that may well be important, and here it is.

Ms. JACKSON LEE. Deputy Secretary Lute, if I might, on the watch list, which has been one of the major complaints and a burdensome list that is both, I believe, inaccurate. In many instances it plays into my colleague's comments about profiling for the basis of religion and otherwise, which does nothing to fight the war on terror.

My question is the distinction between the watch list and the No-Fly list. In this instance this person should have definitely been on the No-Fly list, and so my question is what is the strategy for a comprehensive and coordinated watchlisting and screening approach into a prioritized implementation and investment plan that describes the scope, governance principles, outcomes, milestones, training objectives, metrics, cost and schedule of necessary activities as relates to the watch list to be able to move to the No-Fly list?

If I may also raise to Director Leiter so I can have these questions out, which I think is very important. I hope that when we are on notice that an incident is occurring, all hands will be on deck, similar to making sure that embassy personnel, who we have great respect for, are at their desks at appropriate times, because all times of the schedule, if you will, the calendar, people are coming and going. I hope if there is a terrorist act, we have all hands on deck on this information.

Director Leiter, and I would say my question is there has been a lot of discussion about the failure. This was not a failure to con-

nect the dots, but to analyze what we had. It has been said that the intelligence community, to build a more robust analytical capability, specifically what steps are being taken to accommodate this goal in training, system design and technological changes, but more importantly, on the human intelligence and behavioral assessment, which, if you had done that on the gentleman's actions, he would have been on the No-Fly list.

Deputy Secretary Lute.

Ms. LUTE. Yes, ma'am. Thank you. As you know, the Department of Homeland Security does not own or control the watchlisting. Abdulmutallab was neither No-Fly nor Selectee.

But we are working very closely with our colleagues throughout the interagency to identify the kinds of information that is necessary for us to take steps related to ensuring aviation security.

In fact, in the wake of this incident, we will take information such as Under Secretary Kennedy was talking about and put that in the hand of our immigration advisory professionals that are stationed abroad in nine locations so that they can engage in additional questioning and examination of persons who come on that list. That is an important step in the direction of increased security, and we are looking at others as well.

You also mentioned the frustration with the ensuring the accuracy of the list. We share that frustration. It is important that we do have lists on which we rely for ensuring the safety of the traveling public, that these be accurate lists. We are working very intensively to establish an easy way for people to de-conflict information when it is erroneous and to ensure that those lists are the accurate, important tool that we need them to be.

But we also know that we are facing a determined adversary, who is looking to use people who are unknown to any system. In this regard we need to evaluate their activities, travel patterns, and other activities which can tip us off that this person may be dangerous, certainly is worth additional screening and questioning, and working intensively with our interagency colleagues to get better systems in place for those contingencies.

Mr. LEITER. Congresswoman, thank you for the question. I think you are exactly right, that we have to improve the ability of these analysts to understand the characteristics of this information as they are coming in so they get a true feel for when a father walks in, why is the father walking in? Why this report?

We are doing a number of things on this front. Most importantly, we are creating specific teams that are not bound to writing daily intelligence. When they get that bit from the father and dive into it and connect that intelligence in a way, that you do have all the information necessary to make that determination about whether someone should be or should not be on the No-Fly list.

So you also do not get people on the No-Fly list that you don't want on the No-Fly list, because the only way you are going to get the bad guys off the plane is to also ensure that the good guys can get on the plane. Otherwise, the system just becomes unwieldy.

So we have already begun additional training. The Director of National Intelligence is studying how we can advance that training more. We are creating teams to pursue these to ensure that they

have the time and they have the resources to track down these free pieces of information and put them together.

Mr. KENNEDY. Congresswoman, you also asked is the State Department on duty in addition to the embassy people you mentioned. We have somebody responsible that is in our operation centers 7 days a week, 24 hours a day, 365 days a year. If a question comes in from an embassy—it may be in a different time zone—or comes in from our partners in the National security community, that officer knows who to reach out to to get the right information they need immediately.

Ms. JACKSON LEE. Mr. Chairman, may I just say a point on the record?

I thank the witnesses.

The one point that I heard Deputy Secretary Lute say is that Homeland Security does not have ownership of the watch list. I think it speaks to, again, the work we have to do and have been doing to get the synergism so that we have some mutually interrelatedness on trying to help all of these persons and that we can get an understanding everybody has ownership of the watch list, the No-Fly list.

We have got to find a way to weave in our security so that there are no gaps, not putting the fault on these public servants, but there has to be a cleaning up of the cracks in the system that will allow this kind of breach to happen. It has to be a combination, Mr. Chairman, of the Executive working with us as team homeland security, and no distinction between Republicans and Democrats, team homeland security.

I hope in that spirit that we will have the appointee necessary for the running of the Homeland Security Department to move as quickly as possible to be appointed and confirmed on the behalf of the American people. I look forward to working with them.

I thank you, Mr. Chairman, for yielding.

Chairman THOMPSON. Thank you very much.

I want to thank the witnesses for their valuable testimony and the Members for their questions.

Mr. Kennedy, if you would provide the committee with the instructions you referenced Chairwoman Jackson Lee that have been implemented since the December 25 incident with respect to training and other information. Now, if that is classified, just let us know, we will still govern ourselves accordingly.

Mr. KENNEDY. Mr. Chairman, I will be pleased to get that to you, sir. Thank you.

Chairman THOMPSON. Thank you.

Mr. Leiter, you said you want to make sure that good guys get on the plane. There is a good guy here who is a Member of Congress that has an awful difficult time getting on planes. He is Congressman John Lewis in Georgia.

Deputy Secretary Lute, can you look into that and figure out a way how he can not be flagged for secondary screening and other things, because he is in fact John Lewis? Now, there is another John Lewis out there. We still ought to have a system to figure out how to handle this.

Ms. LUTE. Yes, sir, we should. I am on it.

Chairman THOMPSON. Okay. Thank you very much. I am sure he would appreciate it.

Mr. LEITER. Mr. Chairman. Can I make one note on that front?

Chairman THOMPSON. Yes.

Mr. LEITER. Not knowing the facts of Congressman Lewis' case and certainly not accusing him of being a known or suspected terrorist, I do want to flag for the committee—I think it is important to understand—that a desire to have more people on the watch list will inevitably lead to more false positives. We have to accept that, I believe, as a cost.

There is nothing we can do technologically or with the human to eliminate those false positives from occurring—again, not speaking directly to the Congressman's case, but accepting that this will be a byproduct of ensuring that some bad people don't get on the plane.

Chairman THOMPSON. Well, and I understand, but that is going forward. This has been from day 1. So we are not even to the next generation. But, obviously, we assume the inconvenience that adding to the list will bring, but these are different times.

Mr. Kennedy, last question. Can you provide the committee with either, if you know right now or at a later date, how many people we actually have working in the visa office in your shop here in Washington?

Mr. KENNEDY. Mr. Chairman, let me get that for the record. I can get within a swag, but I will submit that for the record, sir.

Chairman THOMPSON. Thank you very much.

Mr. KING. Thank you for the testimony. Thank you for their service. I yield back.

Thank you, Chairman, for the hearing.

Chairman THOMPSON. Thank you.

Before concluding, I remind the witnesses that the Members of the committee may have additional questions for you, and we ask that you respond expeditiously in writing to those questions.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 1:21 p.m., the committee was adjourned.]

# APPENDIX

---

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE OF TEXAS FOR JANE HOLL LUTE, DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

*Question 1.* In response to a recommendation by the 9/11 Commission about improving passenger pre-screening, the Secure Flight program is being implemented so that TSA will be assuming the duty, which now rests with the air carriers, of checking passengers against the No-Fly and Selectee databases. I understand TSA is first implementing Secure Flight domestically, but with there being a significant threat concerning international in-bound flights, how will the Department conduct watch list passenger pre-screening for in-bound flights to the United States? How will this be incorporated with existing CBP programs like the Advanced Passenger Information System?

Answer. DHS is implementing Secure Flight through a phased process. The Transportation Security Administration (TSA) anticipates that Secure Flight deployments for domestic aircraft operators will be completed in spring 2010. TSA has also initiated Secure Flight deployments for foreign aircraft operators and expects to assume watch list matching for all flights, international and domestic, by the end of calendar year 2010.

All aircraft operators, both foreign and domestic, who have not transitioned to Secure Flight are responsible for conducting watch list screening of their passengers against the No-Fly and Selectee lists.

Currently, U.S. Customs and Border Protection (CBP) screens travelers arriving into or departing from the United States against the Terrorist Screening Database (TSDB, the U.S. Government's Terrorist Watch List), including No-Fly and Selectee records. All commercial and private aircraft operators with flights arriving into or departing from the United States are required to transmit passenger manifest information through the Advance Passenger Information System (APIS) to U.S. Customs and Border Protection (CBP). APIS is used for terrorist watchlist screening, law enforcement analytical work, passenger facilitation, and departure monitoring. As part of program alignment, on February 19, 2008, CBP started screening all APIS manifest submissions against the No-Fly and Selectee watch lists with the screening results being provided to the TSA Office of Intelligence (TSA–OI) for resolution. CBP has been working closely with TSA and the airline industry to align the APIS program with TSA Secure Flight watchlist screening. When TSA's Secure Flight Program is fully implemented, the No-Fly and Selectee screening will transition from the APIS system to Secure Flight. CBP will continue to process APIS manifest information for its law enforcement and traveler facilitation mission.

*Question 2.* Ms. Lute, It is my understanding that "Puffer Machines" or Explosive Trace Portal Machines worked great when they were tested in the lab testing but during field testing they had a high breakdown rate caused by dust and dirt entering the machines. I have been told by TSA that there are currently 9 machines currently in the field, but TSA has no intention to field any more because of the breakdown rate. Is any effort being made to revise or improve this technology?

Answer. At this time there are only two deployed Explosive Trace Portals (ETP), one at Gulfport-Biloxi International Airport and one at Phoenix Sky Harbor International Airport, and both are slotted for removal this year. As we deploy Advanced Imaging Technology (AIT) at an airport we remove obsolete equipment at the same time. This minimizes disruption of the airport operations and increases resource and cost efficiencies.

While the ETP devices previously purchased by Transportation Security Administration (TSA) experienced operational performance issues that hindered their effectiveness in the field, TSA and the Department of Homeland Security Science and Technology Directorate continue to evaluate a variety of trace detection technologies.

*Question 3.* Ms. Lute, it is my understanding that every checkpoint in the United States has portable Explosive Trace Technology devices. I realize it is not practical to test every person in every airport with this device because of time limitations, but can TSA increase the amount of passengers randomly selected for the explosive trace technology swab test? Has TSA taken any steps to increase their use?

Answer. To restate your question more accurately, every checkpoint in the United States has tabletop Explosive Trace Technology devices. Explosive Trace Detection (ETD) technology is a critical tool in our ability to stay ahead of evolving threats to aviation security. In fact, the Transportation Security Administration (TSA) has recently expanded the random use of ETD technology at airports Nation-wide as an additional layer of security. Since it will be used on a random basis, passengers should not expect to see the same thing at every airport or each time they travel. TSA will continue to evaluate the numbers of passengers screened and work to maximize the effectiveness of ETD screening as commensurate with resource levels and airport operations.

*Question 4.* Ms. Lute, it is my understanding that a pilot program that was recently completed by TSA called "e-Logbook" would allow TSA to instantly be able to know if a FAM or LEO flying armed is on-board an aircraft. I have been informed this pilot program was a success however, it is my understanding that no funding has been requested yet for this program to go up Nation-wide. I would like to know what the current status is and what plan does TSA have to role out this program Nation-wide?

Answer. The Federal Air Marshal Service (FAMS) has a dedicated system in place to continually track, in real time, Federal Air Marshal (FAM) presence on domestic and international flights.

With regard to the Electronic Logbook (e-Logbook) pilot program, the Transportation Security Administration (TSA) is seeking to establish an automated process for providing situational awareness for other armed law enforcement officers (LEOs) on-board any given aircraft. The e-Logbook pilot program was tested in Washington (Reagan National Airport, Dulles International) and San Francisco and TSA is currently considering a Nation-wide implementation. In the interim, TSA's Transportation Security Operations Center (TSOC) currently tracks State and local armed LEOs on commercial aircraft through a National Law Enforcement Telecommunications System (NLETS) solution implemented last year. Although functional, the NLETS solution relies on manual processes and is limited to State and local LEOs.

Also, on February 1, 2010, TSA began a pilot implementation of an enhanced credential verification procedure for Federal Law Enforcement personnel flying while armed.

The enhanced identification procedures require each Federal LEO flying armed in accordance with 49 C.F.R. § 1544.219 and respective agency policy, to be in possession of a Unique Federal Agency Number (UFAN). The UFAN is an agency-specific alpha-numeric number TSA issues to Federal agencies/entities upon request. The UFAN is known only to TSA and the respective agency/entity. Each agency/entity must ensure its eligible law enforcement personnel are aware of this number to be used in conjunction with the LEOs badge, credential, a secondary form of Government-issued identification, and airline-issued LEO flying armed paperwork. The UFAN number is an additional form of verification and will be requested of the LEO at the LEO checkpoint prior to entry into the boarding area.

*Question 5.* Ms. Lute, it has come to my intention that some flights have both FAMS agents and LEO's flying armed, while other flights have neither. Is the Department taking any steps to create a scheduling system to maximize the use of FAMS with LEO's flying armed?

Answer. The Federal Air Marshal Service (FAMS) provides mission coverage to the Nation's civil aviation system using a concept of operations (CONOPs) that is essentially a threat-based matrix prioritizing scheduled flight coverage well in advance of the flight date. FAMS, on the other hand, can be made available to cover emergent threats when necessary. In order to perform the FAMS' mission, all Federal Air Marshals (FAM) undergo intensive specialized training far exceeding requirements for law enforcement officers (LEOs) flying armed.

With regard to the matter of other armed LEOs, the FAMS has determined that flight schedules from other agencies (Federal, State, and local) are flexible by nature, often booked within days of the flight date (allowing virtually no advance FAMS planning) and are not sufficiently reliable to ensure daily coverage of flights. Overburdening airlines and TSA's Mission Operation Center with additional last moment cancellations/bookings to ensure proper coverage of high priority flights presents operational and logistical challenges best overcome by the FAMS making its own schedule independent of other LEOs traveling on flights.

*Question 6.* Ms. Lute, does the Department plan to hire more FAMS agents? If so, how many?

Answer. The President's fiscal year 2011 budget request does seek to increase the Federal Air Marshal Service funded staffing level. Specifically, the budget request seeks to hire 499 additional FAMS personnel in fiscal year 2011.

*Question 7.* I have recently become aware of "event-driven" as compared to "person-driven" software. As I understand it, "event-driven" software is very efficient and can instantly capture and process extremely large volumes of information. I understand that electronic signals generated by events serve as input into specialized event-driven software. I am told that based on its processing rules with predetermined expectations and constraints, it can intelligently process the information to constantly revaluate individuals' risk profiles, connect the intelligence-revealing dots, and automatically and immediately communicate the derived intelligence or alerts to all the appropriate people that need to know, or need to take action.

I am told that this event-driven software has been successfully used for years in extremely complex manufacturing environments such as Aerospace and Defense, as well as many other challenging industries. The processing of travel and security "events" is apparently no different and I understand that the software can be deployed very quickly. It appears there is a possibility that with this software the "events" leading up to the Christmas day bomber incident would have set off the alarms for everyone, even if the bomber was not on any watch list. How long do you estimate it will take before the American people can be protected by comprehensive "event-driven" software?

Answer. DHS is aware that event-driven systems have proven useful in such large-scale applications as manufacturing, financial and investment management, aircraft and spaceflight, and project management. Common to all these applications is some on-going process, workflow, or lifecycle. For example, a production line; an investment policy based on a series of price or monetary changes; a series of engine thrust, altitude, heading, weather, and fuel (and many other) measurements, which describe the health of an aircraft; or a development cycle for a software design. The "event" refers to a point along the process, workflow, or lifecycle, where an automated decision is made by the system to proceed or to take one of several alternatives. Using our manufacturing or aircraft and spaceflight examples, this could be deciding to insert a new throttle assembly because the old one was ineffective or setting a series of thrusters or making altitude adjustments on the Space Shuttle to ensure a safe re-entry trajectory. For event-driven systems to function, at least three elements are necessary. These are: (1) A constrained set of rules that determine how decisions are made, (2) access to all the data or databases that are necessary to make a decision, and (3) sensors to detect an event or measurements that are continuously made along the process or lifecycle.

In the context of the attempted attack on December 25, 2009, for an individual and an explosive material, a set of rules does exist for deciding what happens if one or the other is detected, therefore the first element for an event-driven system is present and functioning. The second element, access to all data, was incomplete. In the case of the individual, while he used his real identity (e.g., he did not try to use a false passport or another name), DHS screening systems lacked any data indicating that he presented an imminent threat. In particular, he was not on the U.S. Government's terrorist watch list.

Similarly, while DHS had sufficient information to know that the particular substance could be explosive, our foreign partners did not have systems or processes in place to detect it.

In summary, an event-driven system applied to the attempted attack on December 25 would not have functioned because the individual was not watchlisted and because the screening equipment was not sensitive enough to detect the explosive material. Had the individual been watchlisted or had the equipment been sensitive enough to detect the explosive materials, an event-driven system would not have been necessary as the existing information-based and physical screening processes would have prevented him from boarding the aircraft. DHS is working with our counterparts within the U.S. Government and our foreign partners to close these vulnerabilities.

Event-driven systems could prove useful for some homeland security applications. However, should the Department identify event-driven systems as a practical technology solution for air passenger screening, it will take time to integrate into the existing enterprise.

*Question 8.* The findings of the administration's report released Jan 7, 2010, included: "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 "NCTC and CIA personnel who are responsible for watchlisting did not search all available data-

bases to uncover additional derogatory information that could have been correlated with Mr. Abdulmutallab".

My understanding is that most of the analysis is currently a process of manual searches of the various databases.

Could this goal be achieved with automation, through the use of clever technology that can process large volumes of information efficiently and if so, are you currently looking at putting such technology in place?

Answer. The Department of Homeland Security (DHS) is investigating ways to improve searches across the large number of databases in the Department. Even before 25 December, in response to terrorist activity, the Department established a DHS Threat Task Force (DTTF) and provided access to 47 databases to a single co-located team in order to conduct name traces. While this is a step forward and has yielded actionable insights, the greater need is the ability to search across databases at the same time, combining search results. Rather than search each database individually, a federated search would allow us to more quickly make analytic connections.

A cross-database search capability could enable DHS to conduct searches on individual names, submit lists of names for search, and set up alerts which are tripped when new information on individuals of interest arrives. Various statistical and probabilistic algorithms could be used to prioritize the search results based on context and frequency.

DHS is exploring options for a federated search capability. While federating searches across multiple databases is technically feasible, it is challenging when dealing with numerous datasets of different eras and structures, and it must also be done in a manner consistent with DHS information use policies including implementation of the Fair Information Practice Principles. In advance of creating this capability, moreover, the Department will also develop 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 privacy, civil rights and civil liberties, and ensuring DHS can achieve its mission to detect threats to the homeland.

*Question 9.* Does our technology today enable us to assess every single passenger's risk profile, considering all contributing factors, in order to determine his/her specific risk level at any given point in time, and to immediately communicate an elevated risk to the security agencies for extra screening or follow up? If not, are you aware of a technology that could accomplish this?

Answer. For international flights, in addition to screening against the No-Fly and Selectee lists that are part of the Terrorist Screening Database, DHS uses a decisions support tool that compares traveler information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. The primary purpose is to target, identify, and prevent terrorists and terrorists' weapons from entering the country. All individuals entering the country by commercial air and sea carriers are run through this system. Based on results of the targeting systems, DHS will determine appropriate next steps, which include denying boarding, additional screening before departure or upon arrival, denying admission to the United States, or arrest upon arrival.

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON OF MISSISSIPPI FOR MICHAEL E. LEITER, DIRECTOR, NATIONAL COUNTERTERRORISM CENTER

*Question 1.* What disciplinary or other personnel action has your agency taken in response to the events leading up to the failed attack on Flight 253?

Answer. Response was not received at the time of publication.

*Question 2.* Does NCTC have the authority it needs to fulfill its mission to the American people? Specify any additional authorities needed to operate effectively.

Answer. Response was not received at the time of publication.

*Question 3.* Under what circumstances are names removed from the TIDE database? Describe relevant procedures and the time intervals associated with these procedures.

Answer. Response was not received at the time of publication.

QUESTION FROM HONORABLE CHRISTOPHER P. CARNEY OF PENNSYLVANIA FOR MICHAEL E. LEITER, DIRECTOR, NATIONAL COUNTERTERRORISM CENTER

*Question.* Mr. Leiter, at the hearing when asked about how many points of failure occurred within our intelligence and homeland security systems, "Was there a single

point of failure, a double point of failure or multiple points of failure?", you answered "Multiple". Please list these failures and rank them in terms of severity and what needs to be done to fix them.

Answer. Response was not received at the time of publication.

○