S. Hrg. 111–957

FIVE YEARS AFTER THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT: STOPPING TERRORIST TRAVEL

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

OF THE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

DECEMBER 9, 2009

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

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

U.S. GOVERNMENT PRINTING OFFICE
56–149 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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
ROLAND W. BURRIS, Illinois
PAUL G. KIRK, JR., Massachusetts

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
GEORGE V. VOINOVICH, Ohio
JOHN ENSIGN, Nevada
LINDSEY GRAHAM, South Carolina
ROBERT F. BENNETT, Utah

MICHAEL L. ALEXANDER, *Staff Director*
BLAS NUNEZ-NETO, *Professional Staff Member*
NICOLE M. MARTINEZ, *Staff Assistant*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
ROBERT L. STRAYER, *Minority Director for Homeland Security Affairs*
MATTHEW L. HANNA, *Minority CBP Detailee*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*
LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, DECEMBER 9, 2009

ALPHABETICAL LIST OF WITNESSES

APPENDIX

FIVE YEARS AFTER THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT: STOPPING TERRORIST TRAVEL

WEDNESDAY, DECEMBER 9, 2009

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

The Committee met, pursuant to notice, at 9:35 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Burris, Collins, Voinovich, and Ensign.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good morning. We note the absence of two of our witnesses. This is not a protest to the hearing. But Senator Collins and I do note for the second time that there are Department of Homeland Security (DHS) witnesses having trouble finding their way through the traffic to get here. We gave Secretary Napolitano a very hard time when it happened to her earlier, and we will not hesitate to give it to Mr. Beers and Mr. Heyman.

Anyway, we are glad you are here. We are going to proceed with our opening statements, but we gather that the two others are very much on the way.

Today's hearing is part of our oversight responsibility and begins a series now 5 years after the Intelligence Reform and Terrorism Prevention Act (IRTPA) was adopted, the so-called 9/11 Commission legislation. And in this hearing we are going to focus on a very important part of our comprehensive homeland security framework, architecture, which is: How are we doing at stopping terrorists from entering our country? This obviously is a most important homeland security responsibility that faces our government in the aftermath of September 11, 2001.

We are going to hear testimony today from four key government officials who are on the front lines of our country's efforts to achieve this mission. Their jobs are daunting, they are complex, and the consequence of a single mistake is a pressure I know they continually live with and that should weigh really on all of us in the government as we try to do a better job at protecting our people in an age of terrorists who are willing to attack us here at home.

After having made that statement, I must say, in terms of letting our guard down, why I and others are so concerned about the security breach at the Transportation Security Administration (TSA) that was discovered over this past weekend. As you all know, I am sure, a highly sensitive screening manual was posted online, apparently for months, without being properly redacted. This was a serious breach because the manual includes information that could help terrorists to defeat and circumvent the TSA inspection process. This is actually quite relevant to what we are here to discuss today. In this age of freely flowing information, we simply have to have adequate safeguards in place to ensure that terrorists are not being given any advantages as they plot against us. So we will await with real interest and, I say, impatience the TSA review of how this possibly could have happened and how they are intending not just to make sure it does not happen again, but how they are intending to mitigate the potential adverse consequences of this mistake.

The 19 hijackers who attacked our country on September 11, 2001, traveled to the United States with visas, some obtained fraudulently, but most obtained legally. Two of the terrorists were at that time illegal because they had overstayed their visas. The arrests this fall of a number of people charged with planning terrorist attacks in the United States: Najibullah Zazi, Betim Kaziu, Michael Finton, and Hosam Smadi, and the arrest of David Headley, who was more involved in plots against foreign targets, but from the United States, are the most recent reminders that terrorists are still crossing our borders legally—in Headley's case in and out—living among us, and plotting to attack us or, in Headley's case, our allies.

This Committee takes very seriously our obligation to ensure that the Executive Branch is tackling head on the challenges posed by violent Islamist extremists to our homeland security, and fulfilling that responsibility certainly begins with doing everything we can to keep terrorists from ever entering the United States.

There really have been quite a remarkable number of additional laws and programs put in place to achieve this goal since September 11, 2001. A lot of them, I am proud to say, are the result of legislation that began in this Committee but was passed, of course, by the full Congress and signed by the President. The 9/11 Commission legislation was one of those, the 2004 legislation, then the follow-on 2007 legislation.

I think rather than going on at length about all the programs that have been established—U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT), the Terrorist Screening Center, the National Counterterrorism Center itself, the efforts we are making to establish the US–VISIT program, depending a lot on fingerprints—has really been a remarkable achievement, but I have concerns about some of the questions that it raises. And it is no substitute for a biometric exit system. The implementation of a biometric entry system at all of our Nation's ports really has been a centerpiece of the screening system, quite remarkable, but we still, as I say, do not have the biometric exit system in place despite numerous congressional mandates, and that is a concern that we will pursue today.

VerDate Nov 24 2008 12:33 Apr 29, 2011 Jkt 056149 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 P:\DOCS\56149.TXT SAFFAIRS PsN: PAT

I would say bottom line that I think we are a lot safer than we were on September 11, 2001, and we are doing a lot better from the initial point of contact, which is the consular interview abroad where people apply to come in, to all of the various databases that people are screened on when they get on a plane to come here, to the biometric entry system and to our improvements at the exit system as well, we are doing much better. But we have to do yet better than this, and, of course, as we see in error of judgment made by TSA over the weekend, and in some sense what may be some errors of judgment in the case of Major Nidal Hasan in Fort Hood—we do not know that conclusively, but it feels like that—the consequences are really catastrophic.

So this is the pressure that we live under. This is the time in which we have this responsibility. But the four of you, I think, and the agencies and the people you represent have done a tremendous job to bring us to a position much better than we were at on September 11, 2001. We want to explore with you today how we can help you and how you can do better at improving our systems for stopping terrorists who enter the country in a time of rapidly changing technology and clear and persistent attempts by the terrorist organizations as reflected in the run of cases we have had this year, particularly homegrown terrorists coming and going, to attack our country again.

This Committee will be vigilant in the months ahead, in this 5-year review of post-September 11, 2001, legislation to ensure that the Federal Government continues to strengthen these systems, and today's hearing I think is an expression of our commitment to do that.

So I thank all the witnesses for being here, and I am happy now to call on Senator Collins for her opening statement.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman. Five years ago, this Committee authored the most significant reform of our Nation's intelligence community since the Second World War. Today, we recognize that this is no time to rest, no reason to pause, in our efforts to protect our country from terrorist attacks.

Earlier this week, we received a chilling reminder of how a lapse in security can pose a serious threat to our homeland. As the Chairman has indicated, a version of TSA's aviation security manual was posted on the Internet for anyone to access and read. As former Assistant Secretary of the Department of Homeland Security Stewart Baker has said, the manual will become a textbook for those seeking to penetrate aviation security, and he described the leak as serious.

Terrorists continually change their strategies and mutate their forms of attack. We know, however, that their aim remains constant, and that is, to harm our Nation and our citizens.

The 9/11 Commission noted that as many as 15 of the 19 hijackers might have been intercepted by border authorities if procedures had been in place to link previously accumulated information to their names. Several of the hijackers had been cited in intelligence agency files for terrorist links. Existing but untapped data on travel patterns, bogus visa applications, and fraudulent passport infor-

mation could have focused attention on some of these terrorists. And that is why this Committee has focused so relentlessly on the issue of terrorist travel during the past several years.

Following the attacks on our country, the Federal Government took initial steps to deploy systems and procedures to help ensure that terrorists would not again slip undetected across our borders. The Intelligence Reform and Terrorism Prevention Act of 2004, which Senator Lieberman and I co-authored, expanded and strengthened many of these initiatives and implemented other recommendations of the 9/11 Commission. We can look back at a great deal of progress that has been made since that time.

One of these successes is a biometric system for screening foreign nationals seeking to enter the United States. The State Department now collects fingerprints of foreign nationals who apply for visas at U.S. embassies and consulates across the world. They compare them to databases containing fingerprints of potential terrorists and immigration violators. Those fingerprints are now checked at U.S. ports of entry by DHS to confirm that the individual arriving into our country is the same individual who was approved for the visa abroad.

Another important accomplishment has been the creation of a consolidated terrorist watchlist based on terrorism-related information from all parts of the intelligence community as well as the Federal Bureau of Investigation (FBI). The consolidated list allows the names of individuals to be quickly checked to identify terrorism connections. The Intelligence Reform Act required that passengers on international flights to the United States and flights within the United States be checked against this watchlist.

The Government Accountability Office (GAO) has recommended that DHS develop guidelines for the private sector to use the terrorist watchlist to screen their employees. These guidelines, however, have yet to be issued. The owners and operators of our critical infrastructure should be permitted to screen their employees against the terrorist watchlist on a voluntary basis, as long as appropriate civil liberties protections are in place. It is notable that Najibullah Zazi, who plotted the recent terrorist attacks in New York, was an airport shuttle driver at the Denver Airport. That means that he had access to critical infrastructure.

The Federal Government also has yet to establish a mechanism to screen mass transit workers, such as those who drive subway trains and buses, against the terrorist watchlist. This was required in the 2007 homeland security law. But although 28 months have passed, no regulations have been issued by DHS. Think about it. Every day these employees have in their hands many lives, and a simple check against the watchlist, such as that already required for hazardous materials drivers, ferry captains, and airline pilots, might prevent a needless loss of lives.

This Committee also authored the legislation in 2007 that strengthened the Visa Waiver Program, and I look forward to hearing more about that as well.

As Senator Lieberman has indicated, the Federal Government has worked hard and the countless Federal employees are diligent in trying to prevent terrorists from coming across our borders to do us harm and to prevent them from traveling and working within

our country. But as the incident with TSA reminds us, even what appeared to be an innocent posting to help Federal contractors can have serious consequences for our security. We need to do more to improve our procedures and to guard against security lapses such as this one.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins, for your opening statement.

Mr. Beers and Mr. Heyman, we gave you a hard time about being late before you arrived so I need not repeat it, but we welcome you. And Senator Collins and I have amply filled the time before your arrival.

Thanks very much for being here. We are taking a 5-year look now at all the things that we have done, the systems we have created to stop terrorists from being able to enter here, and to make sure that those who cause us trouble are noted on the way out as well. So we are happy to welcome you back as our first witness, Rand Beers, Under Secretary, National Protection and Programs Directorate (NPPD) at DHS.

TESTIMONY OF HON. RAND BEERS,[1] UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BEERS. Thank you, Chairman Lieberman and Ranking Member Collins. It is an honor for me and David Heyman and the partners in this effort from the FBI and the State Department to discuss the progress that we have made.

We know, and fully agree with what you have said, that terrorists definitely plan and are attempting to carry out attacks on our homeland, and that it is our responsibility to do everything that we can to deny them the access. At the National Protection and Programs Directorate, we are responsible for identifying the human threats to our country through our US–VISIT program. US–VISIT plays a vital role in helping the Federal Government identify people who pose a threat before they are admitted to the United States, preferably, or if they are here, after they have entered the country.

Our capabilities I think have come a long way in a few short years. Before US–VISIT, State Department and Customs and Border Protection (CBP) had to rely on travel documents, documents that could be easily forged, to determine whether or not a visa should be granted or a person should be admitted to the United States. Today, I think using biometrics, we can verify international traveler identities to make fraud almost impossible, stripping terrorists and criminals of anonymity, one of their most valuable assets.

With the power to uncover a person's true identity and immigration and criminal history, we have been able to deny approximately 9,000 impostors at our ports of entry in the last 5 years as well as identify a number of others who were required to pass through secondary screening to determine their travel history.

[1] The prepared statement of Mr. Beers appears in the Appendix on page 42.

The four US–VISIT agencies basically lacked coordinated data systems, and there was no real way to exchange information easily or check one another's records before making a decision to grant a visa, admit someone to the United States, or grant some other immigration benefit. I think the Intelligence Reform and Terrorism Prevention Act called on us to fully integrate the systems of Immigrationa nd Customs Enforcement (ICE), CBP, and U.S. Citizenship and Immigration Services (USCIS) as well as the State Department and the Justice Department to enable information sharing in a timely fashion.

Today, US–VISIT makes biometric-based information sharing between these agencies possible by providing a single source of information on criminals, immigration violators, and known or suspected terrorists. Every day, 30,000 authorized Federal, State, and local government agency users can query US–VISIT data and get a response quickly in order to help them determine, identify, mitigate, and eliminate security risks.

And, finally, before US–VISIT, ICE officers lacked timely and accurate information about visa overstays, and while this system is not perfect, as I am sure we will discuss today, US–VISIT does analyze and match entry and exit records, identifies hundreds of credible leads each week on people who have overstayed their visas, and those leads are forwarded to ICE, who can then determine what appropriate action that they might take.

So, together, these steps I think have made our efforts to prevent terrorist travel more collaborative, more streamlined, and more effective than ever before. Let me give you one example of the power of this system of improved screening and information sharing and how it is helping us to catch dangerous people.

In 2007, a man applied for a visa at a U.S. embassy. When the State Department checked his fingerprints, in the database there was no negative information about this person, and he was granted a visa. Three days later, US–VISIT received from Interpol information about the criminal history of this individual. This updated data was then run against the existing database system and identified this person who had already been granted a visa. And that visa was then subsequently denied as we passed that information to the State Department.

The point of making this example is to show you that this is not a system that is a one-time-fire-and-forget kind of system. It is a system that is updated on a regular basis and then run against the existing database. It is dynamic. New information is constantly run against the old to make sure that we did not miss somebody that we could identify as a person of interest and ensure that appropriate action was taken in a timely fashion.

So this individual is but one of thousands of people who we have prevented from entering the United States, and yet we know that our success is not complete and that we have more work to be done.

So as part of our ongoing effort, we will continue to innovate with new systems. We will continue to ensure that coordination among the various actors in the Federal Government is effective, and we will continue to work abroad with other countries to get

VerDate Nov 24 2008 12:33 Apr 29, 2011 Jkt 056149 PO 00000 Frm 00010 Fmt 6633 Sfmt 6633 P:\DOCS\56149.TXT SAFFAIRS PsN: PAT

others to also begin to use biometric identification as part of the international system.

So thank you both for having us here today, and know that we are dedicated to protecting the United States. Thank you very much.

Chairman LIEBERMAN. Thanks, Mr. Beers. That anecdote was both interesting and encouraging.

Our second witness is the Hon. Janice Jacobs, Assistant Secretary for Consular Affairs, Department of State. Again, for those in the room, those watching, this is a system that begins way over there, and for most people—but not all, of course—the initial point of contact is a consular officer at the State Department. Thanks for being here.

TESTIMONY OF HON. JANICE L. JACOBS,[1] ASSISTANT SECRETARY FOR CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE

Ms. JACOBS. Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, it is a distinct honor to appear before you today. I appreciate the opportunity to share with you the many accomplishments of my colleagues in the Bureau of Consular Affairs in our continuing efforts to strengthen the security of U.S. borders through the vigilant adjudication of both U.S. passports and visas while maintaining America's traditional openness to legitimate travelers.

Through enhanced training, technology, and data sharing, today's consular officers can more readily distinguish between high- and low-risk travelers, concentrating their efforts on those requiring more scrutiny while facilitating legitimate travel, travel that enhances the U.S. economy and promotes mutual exchange and understanding.

I can state with certainty that in my 20-year Foreign Service career I have not seen a transformation more dramatic than the one that the Bureau of Consular Affairs undertook after the terrorist attacks of September 11, 2001. First as Deputy Assistant Secretary for Visas and now as Assistant Secretary, I have been personally involved in implementing the enormous changes that are detailed in my written testimony. I share the responsibility for our twin goals of open doors and secure borders with my esteemed colleagues at this table. Our close and fruitful cooperation is evidenced through unprecedented data sharing and interagency coordination.

In my written testimony, I outline five pillars of how we stop terrorist travel. We rely on technological advances, biometric innovations, personal interviews, data sharing, and training.

The first pillar, technological advances, relies on comprehensive databases such as the Consular Lookout and Support System (CLASS), and the Consular Consolidated Database (CCD). CLASS is a database which is updated continuously. Because of improved data sharing, CLASS has grown more than 400 percent with almost 70 percent of records coming from other agencies. CCD allows Foreign Service posts, the Department, and our partner agencies

[1] The prepared statement of Ms. Jacobs appears in the Appendix on page 51.

and offices to view information about visa applicants within confidentiality provisions of the Immigration and Nationality Act.

We will soon deploy a global system for conducting and tracking consular fraud investigations. A new electronic platform, now deployed overseas, will provide consular and fraud officers the opportunity to analyze data in advance of the interview, enhancing their ability to make decisions. And security advisory opinions (SAO) are now processed electronically, thus facilitating the processing of nearly 2 million SAO requests since September 11, 2001.

The second pillar is the use of biometrics. In fiscal year 2009, fingerprints of more than 6.7 million visa applicants were screened against DHS's Automated Biometric Identification System (IDENT), and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) databases. Our partnership with DHS allows Customs and Border Protection officers at ports of entry to verify the identity of travelers by checking against fingerprints collected during visa interviews at overseas posts.

We also screen visa applicants against a watchlist of photos of known and suspected terrorists obtained from the FBI's Terrorist Screening Center. Facial recognition screening has proven to be another effective way to reveal impostors.

The third pillar relies on one of the most significant changes in consular practice after September 11, 2001: A reemphasis on the personal interview. The interview is an opportunity for consular officers to determine the credibility of an applicant and the applicant's travel plans and the stated purpose of the visit to the United States.

The fourth pillar demonstrates how we rely increasingly on our partners to enhance our ability to make the right decisions when adjudicating visa and passport applications through data sharing. For example, the Bureau of Consular Affairs, working with DHS, has provided visa adjudicating posts overseas with access to DHS's Arrival/Departure Information System (ADIS), thus giving consular officers more information about an applicant's travel history.

And, finally, the fifth pillar is training. The Department of State is committed to providing the highest level of training to our consular officers. Over the past 6 years, the Department has lengthened and substantially improved the basic consular course required of all officers in consular positions and continually reviews course content for further enhancement. The Department also continually updates the hands-on anti-fraud technologies curriculum.

Allow me to add a brief note about the safety of U.S. passports. Since 2005, we have been issuing state-of-the-art passport documents with advanced technological features to foil the efforts of counterfeiters. We are also doing everything in our power to ensure that passports and passport cards are issued only to U.S. citizens who are legitimately entitled to them. We have greatly enhanced our fraud prevention efforts over the past year. In coordination with the Bureau of Diplomatic Security, we launched unannounced testing of the processes and procedures for passport acceptance and adjudication.

Distinguished Members of the Committee, I believe that we have made significant improvements since the attacks of September 11, 2001. At the same time, we are constantly looking for ways to do

better. Please be assured that the Bureau of Consular Affairs will continue its close cooperation with our partners to find ways to keep this country safe while keeping our borders open to legitimate visitors. We believe the record of the past 8 years shows that we can make advances in both spheres, and we are dedicated to implementing the best possible solutions to further these goals.

Thank you again for the opportunity to be here. I appreciate the Committee's continued interest in our work and have enjoyed the chance to share some of the many accomplishes we have had over the past several years, and I am pleased to take your questions.

Chairman LIEBERMAN. Thanks very much, Ms. Jacobs.

Now we will go to David Heyman, Assistant Secretary of Policy at the Department of Homeland Security.

TESTIMONY OF HON. DAVID F. HEYMAN,[1] ASSISTANT SECRETARY FOR POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HEYMAN. Good morning. Thank you, Mr. Chairman, Senator Collins, and distinguished Members. Thank you for the opportunity to be here today and to appear before you.

I want to echo Under Secretary Rand Beers, my colleagues, the Chairman, and the Senator's commitment to keeping this Nation safe, secure, and resilient, and the appreciation that this Committee has done to do so.

Today I want to discuss three key areas in which the U.S. Department of Homeland Security plays a central role in disrupting and denying terrorist travel: Identification of known and suspected terrorists as well as other individuals who pose a threat to national security; screening of travelers and those seeking immigration benefits; and, finally, securing and verifying travel documents to prevent people from illicitly traveling to the United States.

Let me start by putting the challenge of thwarting terrorist travel in context. To begin with, people are not born as terrorists, nor are extremists necessarily violent. But there are key paths along the way in which individuals turn to violence and terrorism to include recruitment, radicalization, indoctrination, planning, and terrorist action at the end. This process can occur in safe havens, in foreign countries, and even within our own borders. The U.S. Government deploys a number of strategies to counter terrorism, including collaborating with our foreign partners, cutting off terrorists' financial resources, intercepting terrorist communications, targeting terrorist leadership, and countering efforts of recruitment, among others.

But to paraphrase the 9/11 Commission and the Chairman's opening statement, targeting terrorist travel is perhaps one of the most powerful weapons we have to counter the ability of terrorists to operate.

As evidenced by recent events, the United States and its allies have made significant progress in our attempts to frustrate terrorists' ability to communicate, to plan, to finance, and—the focus of this hearing—to travel to conduct operations. Focusing on these four areas allows multiple opportunities to interdict.

[1] The prepared statement of Mr. Heyman appears in the Appendix on page 79.

Those who seek to engage in terrorist activity rely on access to travel networks. Terrorists do travel in order to identify and engage in surveillance of potential targets, to plan their attacks, to train on tactics and operations, to collect funds and documents, and to communicate with other operatives. Every step along this way, however, presents a vulnerability to would-be attackers who must come out of the shadows and interact with the traveling public and our officers at ports of entry and abroad.

What we have learned over the past few years is that border security and preventing terrorist travel is more than drawing a line in the sand and more than just preventing terrorist travel. It is the exercise of our authorities associated with border security and the fact that this can be a powerful resource to identify and thwart terrorist operations at the earliest opportunity.

At DHS we have a number of ways in which we seek to limit and constrain terrorist travel, many of which are accomplished before a terrorist even boards a plane. First, we must know who poses a potential threat, and to identify those travelers who present a risk, we rely on the intelligence community, law enforcement, our border security specialists, and our international partners. These groups help both to populate the watchlist that is managed by the Terrorist Screening Center and understand the techniques used by high-risk travelers to blend into the rest of the traveling public.

Data of known and suspected terrorists is then made available to DHS to screen through our system, such as the Traveler Enforcement Compliance System (TECS), through the Automated Targeting System, and US–VISIT's IDENT. Entities such as CBP's National Targeting Center, the Terrorist Screening Center, Human Smuggling and Trafficking Center, and the National Counterterrorism Center (NCTC) collaborate to ensure coordinated evaluation and response to potential encounters.

Second, we must be able to expedite the entry of the vast numbers of legitimate travelers while restricting the movement of terrorists and other malicious actors. Our knowledge of who is associated with terrorism and the practices terrorist travelers adopt is applied through a multi-layered, end-to-end screening process. This is a process we have developed over the last two decades.

The first layer of that process begins well before departure, with programs such as CBP's Global Entry, with our Electronic System for Travel Authorization (ESTA), that, like the visa adjudication process, provides the DHS the ability to identify potential risks during the planning stage through checks of the applicants against watchlists, criminal history, and other derogatory information.

The second layer is through the advanced receipt of passenger information, reservation data, and manifest information. That enables us to identify likely terrorists and criminals during their movements and coordinate our response.

Finally, the third layer, at our ports of entry our officers are able to identify people who may be attempting to use fraudulent documents.

Each of these steps reinforces the ones before it, allowing us to deny travel prior to departure, target travelers for additional inspection, and prevent entry at arrival, and/or prevent an individual

from remaining in the United States if they are not authorized to do so.

Finally, no amount of watchlisting and screening will help us identify terrorist travelers if they are able to travel on an assumed identity with fraudulently obtained or fake documents. As a result, we need to ensure the security of the documents that we require for travel and an accurate accounting of documents that have been validated due to loss or theft.

Through the Visa Waiver Program and the International Civil Aviation Organization (ICAO), we have worked to develop global standards for the current generation of electronic passports, incorporating biometric data that reduces fraud. Through US–VISIT and other programs, we can verify that the presenter of the document is the same person to whom it was issued and who we have possibly seen before. And with Interpol, we have worked to promote increased use of the Stolen and Lost Travel Document database, a global repository of approximately 20 million records of invalid passports and identity documents. Today, we use this system in most of our border screening programs and every month identify cases of fraud that would have otherwise been undetectable.

I submit my full statement for the record, but let me close by summarizing that by enhancing the security of travel documents, screening persons in advance of travel, identifying known and suspected terrorists as well as other inadmissible travelers, and denying them entry into the United States, we can limit terrorist travel. We can constrain their operations. This is one of a number of tools protecting America against terrorist attacks.

I thank the Chairman, thank you, Senator Collins and Members, and I look forward to your questions.

Chairman LIEBERMAN. Thank you, Mr. Heyman. I look forward to posing some questions to you.

Finally, we have Timothy Healy, Director of the Terrorist Screening Center at the FBI. It is good to see you again. Please proceed.

TESTIMONY OF TIMOTHY J. HEALY,[1] DIRECTOR, TERRORIST SCREENING CENTER, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. HEALY. Thank you. Chairman Lieberman, Ranking Member Collins, and Members of the Committee, thank you for the opportunity to talk about the Terrorist Screening Center (TSC) and its role in combating terrorist travel.

Over the past 6 years, the TSC has become a powerful tool to fight terrorism and integrate the law enforcement and intelligence communities by consolidating terrorist information into a single Terrorist Watchlist. We are continuing to move forward to enhance our partners' ability to combat terrorism by improving the U.S. Government's approach to terrorist screening and safeguarding civil liberties in the process. Our interagency watchlisting and screening efforts have matured into a true information-sharing success. With your continued support, we hope to improve upon our initiatives to provide critical terrorist identity information to our domestic and foreign partners for terrorist screening purposes. Let

[1] The prepared statement of Mr. Healy appears in the Appendix on page 89.

me begin by telling you about where we are at today and where we want to be in the future.

Established in 2003, the TSC is a multi-agency center that connects the law enforcement communities with the intelligence community. We strive to maintain the highest-quality data concerning known or suspected terrorists to aid in the identification process. We ensure the timely dissemination of that terrorist data and that prompt notification is made when a known or suspected terrorist has been identified through the screening process. We ensure that privacy is protected and civil liberties are safeguarded.

The identities contained in the Terrorist Watchlist originate from credible information developed by our intelligence and law enforcement partners.

TSC accepts nominations into the Terrorist Watchlist when they satisfy two requirements. First, the biographical information associated with a nomination must contain sufficient identifying data so that the person being screened can be matched to or disassociated from the watchlisted terrorist. Second, the facts and circumstances pertaining to the nomination must meet "reasonable suspicion" which requires "articulable" facts which, taken together with rational inferences, reasonably warrant a determination that the individual is known or suspected to be a terrorist.

Most of the individuals on the Terrorist Watchlist are not U.S. citizens, but they are living abroad. The Terrorist Watchlist is made up of approximately 400,000 people ranging from suicide bombers to financiers. A small portion of the list is exported to TSA to create the no-fly list. In order to be placed on the no-fly list, a known or suspected terrorist must present a threat to civil aviation or national security. Consequently, the no-fly list is a very small subset of the Terrorist Watchlist. It contains approximately 3,400 people; of those approximately 170 are U.S. citizens.

The screening process leverages thousands of our law enforcement officers and other government partners to help identify, detect, and deter terrorists. Terrorist screening occurs throughout the world at our embassies, at our ports of entry, during police stops, during special events, when HAZMAT licenses are issued, or when guns are purchased.

Terrorist screening occurs when processing passports or visa applications or citizenship and immigration applications.

Our Tactical Operations Center operates 24 hours a day and receives approximately 150 calls per day. Of those, approximately 30 to 40 percent are positive matches to the Terrorist Watchlist. All positive matches are forwarded to the FBI Counterterrorism Center for the appropriate law enforcement response. Additionally, we improve our Terrorist Watchlist by updating existing records using the information discovered during the encounters.

In conjunction with the Department of State, we have completed bilateral agreements with 17 foreign governments and have independently provided screening support for certain international events such as the World Games. Over the past 2 years, our outreach teams have coordinated with all 72 State and local fusion centers, and we also provide terrorist-related encounter information online.

TSC notifies fusion centers when encounters occur within their area of responsibility. The TSC was recognized for its innovative information-sharing initiative at the 2009 National Fusion Center Conference.

As we move forward, our watchlisting efforts must be predicated upon four basic operational concepts: Maintenance of the highest quality of terrorist identity data, timely dissemination of that terrorist identity data, responsive information sharing, and safeguarding civil liberties.

Once a known or suspected terrorist is identified and included in the Terrorist Watchlist, we must ensure the timely dissemination of that terrorist data to our screening partners.

U.S. Customs and Border Protection uses the Terrorist Watchlist at all 327 ports of entry. Law enforcement agencies use the Terrorist Watchlist when they conduct their normal police checks. The TSA uses the Terrorist Watchlist when they coordinate the screening of all commercial air passenger travel. The Department of State uses the Terrorist Watchlist to screen aliens seeking visas and U.S. persons applying for passports.

The TSC led the interagency initiative to develop an effective interagency redress process and maintains a separate unit dedicated to resolving redress matters. Working closely with our interagency partners, we standardize the interagency Watchlist Redress Procedures and provide travelers with an opportunity to receive a timely, fair, and accurate review of their redress concerns. A traveler who believes they were inconvenienced as a result of screening can submit a redress complaint through the DHS Traveler Redress Inquiry Program (DHS TRIP). The complaint is reviewed by the agency that received it and referred to the TSC Redress Unit after it has been determined that it has a connection to the Terrorist Watchlist. Of note, 0.7 or less than 1 percent of the DHS TRIP complaints actually have some connection to the Terrorist Watchlist. We review all available information and work with the nominating agency to determine if the Terrorist Watchlist status should be modified. The TSC neither confirms nor denies an individual being on the watchlist. We do, however, assure the inquiring entity that we have examined all applicable Terrorist Watchlist records to ensure they contain current and accurate information and we have taken all reasonable measures to reduce any future misidentification.

We have also established protocols to aid the individual who continuously gets misidentified because their name is similar to the watchlist. To provide relief in these situations, our TSC CBP employees issue what is called a Primary Lookout Override so that the individual will not be inconvenienced during future screening attempts.

Our ongoing commitment to high-quality terrorist identity data, to the timely dissemination of that information, and to share that information once we have encounters occur is our ultimate goal. Our watchlisting and screening enterprise would not be where it is at today without the superb collaborative efforts between the TSC, the FBI, DHS, Department of State, Department of Defense, the NCTC, and members of the intelligence community.

Chairman Lieberman, Ranking Member Collins, I look forward to answering any questions you may have.

Chairman LIEBERMAN. Thanks very much, Mr. Healy. I must say, if I may paraphrase what Ms. Jacobs said, in her years in Federal service, she has not seen so dramatic a transformation as they have in the Consular Affairs section. I think it is generally true across the board. It has been quite an impressive upgrade and also the establishment of a series of what I would call filters, but really they are much more than that, particularly using modern information technology. So I think we have come a long way.

Let me begin my questioning with you, Ms. Jacobs, because as we said, you are at the beginning of the process. I think one of the most important provisions of the terrorism prevention legislation that we passed in 2004 was the requirement that all individuals undergo a personal interview when applying for a visa. No matter how advanced and seamless our border screening technology becomes, these automated databases were obviously created to catch people that we already have reason to suspect. They cannot help us discover the terrorist who has never come in contact with one of our intelligence or law enforcement agencies. Only a trained and motivated consular officer is able to identify that terrorist who has never made himself or herself known.

So I wanted to ask you, in the course of their interviews, consular officers obviously come across a wide variety of travel documents, not always from the country to which they are posted. What mechanisms are currently in place to help consular officers identify fraudulent documents?

Ms. JACOBS. Thank you, Mr. Chairman. We have, in fact, put in place since September 11, 2001 a very robust anti-fraud training program whereby officers who are going out in the field to do their first consular assignment start with the basic consular course, where they get training in fraud prevention and detection. Once they are overseas at a post, that training continues. We have an orientation program for all of our officers that teaches them what genuine documents look like from that particular country, but also they are given online tools and other databases that they can check in order to confirm the legitimacy of travel documents or documents from other countries.

The officers in the field, and the Foreign Service nationals who work alongside them, really are true experts in determining whether a document is fraudulent or not. They can look, touch, feel documents. They know a wide range of documents that are issued in that particular country. But, again, we have tools available online where there are entire libraries of samples of documents from other countries. We use the Edison online tool database in order to verify the authenticity of documents.

So I am very comfortable in saying that we have given officers the training and the tools that they need, and we also really stress interviewing techniques, the ability when you are talking to someone to even look for facial expressions to see if someone is telling you the truth.

I think with all of that put together that the officers are much more able today than they were perhaps in the past to pick up on

VerDate Nov 24 2008 12:33 Apr 29, 2011 Jkt 056149 PO 00000 Frm 00018 Fmt 6633 Sfmt 6633 P:\DOCS\56149.TXT SAFFAIRS PsN: PAT

clues, on irregularities, either in what someone is saying or in the documents that are presented.

Chairman LIEBERMAN. Yes, and obviously this is very important, just to stress the point that I made in offering this question. We have got this biometric system, fingerprint system, for entry into the country, but for somebody who is not in a fingerprint database, obviously the accuracy of the reader documents is critically important.

Tell me a little more about the consular case management system that you referred to in your testimony and how that is different from what happens today and, if in any way, how it will improve the consular interview process.

Ms. JACOBS. We have had basically individual tracking systems available at different posts for tracking fraud cases. What we are going to be deploying in the future is a system that will be available to everyone. It will be in our consolidated database whereby people will be able to look at the fraud cases that are being handled at any post around the world. We will be able to check on trends. We will be able to see if we have visa shoppers, people going from post to post, whether we are being told the same thing as was said at another post.

It will give us a much better feel for the amount of fraud that we are encountering and, as I said, some analytical tools in order for us to be able to detect trends that might be occurring.

We are very excited about this. We are seeing all kinds of different uses, both on the visa side and passport side, and we think that once this is in place, our ability to detect fraud will be enhanced even further.

Chairman LIEBERMAN. That is good.

Under Secretary Beers, I wanted to ask you if you would talk a little bit about the advantages of a biometric exit system. In other words, do you think one is needed? And what would its benefit be as opposed to a biographical system for law enforcement, including DHS?

Mr. BEERS. Thank you, Senator, for the question. We have been looking at this really for some time now. I think with respect to the biometric system over the biographic system, the real issue to make it most effective is to ensure, in fact, that all people who are exiting the country who are in some kind of a visa or immigration status, in fact, do check out with the country. The current system, which is biographically based, does not have that degree of certitude with respect to the checkout. The options that we are looking at all have as an element the assurance that people cannot exit the country in that visa status by air or sea without actually checking out. So that will increase our certainty about individuals and whether or not they are in status with respect to the time frame that their visa was available for or their entry would allow them to be in this country.

It also allows us, because it is biometric, to also check effectively as to whether or not any activities that occurred after their entry into the country—for example, criminal activity—was known and recorded and whether or not there was, in fact, some criminal action which was incomplete with respect to that. So in the pilot study that we have run, we actually picked up some individuals

who are wanted in this country who were trying to leave the country because of that. So I think it is an additional degree of assurance.

Having said that, as you well know, sir, this is only one portion of the way that people can exit this country, but, by and large, the people who come in by air go out by air. And so it will definitely increase our assurance over that.

But let me just add as a final point, we do currently have a system designed to detect overstays. It is not perfect, but it is also in existence, and it does refer cases on a regular basis to ICE for taking further action. And a number of overstays have been arrested as a result of this system. But biometrics I think we believe would enhance this overall system.

Chairman LIEBERMAN. Can you give us, even in broad terms, any timeline for deploying a biometric system, for instance, at airports?

Mr. BEERS. Yes, sir. We are in the final stages of a recommendation to the Secretary of Homeland Security for the system to be selected from among the various options that we tried and some that have been put together as a result of that test, but which were not actually tested. And my expectation is that she will be reviewing this in the course of either this month or the next month. We will then share that with you all and with others. It is not going to be a free system under any circumstances, and we will have to provide you, as I promised Senator Voinovich, among others, an actual budget amount that would be forwarded. Then we would go into rulemaking, and my expectation is that actual implementation would probably not begin in this fiscal year, although we will try, if it is possible, with some test points to do that.

Chairman LIEBERMAN. Well, that is actually good news. Obviously, we wish it would have happened earlier, but you are on a timeline now that will take us to deployment of a biometric exit system at airports if not in this fiscal year, then presumably early in the next one. Then at another time I would be interested in hearing about what you think the challenges are to deploying a biometric system at land points of exit.

Mr. BEERS. That is a much longer conversation, sir.

Chairman LIEBERMAN. It is. We will come back to that. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Beers, I have a copy of the TSA Aviation Security Manual that was posted on the Internet, and every single page of this manual has at the top of it "Sensitive Security Information." At the bottom of the cover page, it says "Warning: This record contains sensitive security information that is controlled. No part of this record may be disclosed to people without a need to know without the written permission of either the head of TSA or the Secretary of Transportation." It goes on to say that "Unauthorized release may result in civil penalties."

So how did this happen?

Mr. BEERS. Let me start, because we both have spent the morning—and, quite frankly, that is why we were late—in being able to answer the expected questions that you all quite legitimately would pose about this.

The first point I want to make is there is no question that this was inappropriately posted on this Web site and that the protections that were supposed to have been put in place were not adequate. And this, I think, represents a breach of all of the protocols that you just noted in indicating the nature, Sensitive Security Information (SSI), do not disclose, etc. All of those I think are correct. As a result of this—but let me make two other points first.

The first thing is that this document that you are referring to is a document which was for supervisors. It was not for front-line screeners. So the actual screening procedures that a transportation security officer (TSO), would actually use at a screening point are not in that document.

The second thing is it is an older document. It is six versions ago in terms of that. That does not mean that it is not an inappropriate release of the document, as you quite correctly said.

Senator COLLINS. But are you saying that this has substantially changed in the last year and a half? Because that is not my understanding.

Mr. BEERS. Mr. Heyman, I, and the Secretary all talked to the Acting Administrator of TSA. The document has changed since then. I am not using that as an excuse to say that this is not a problem. But the other part of it, quite honestly, is that the actual screening procedures are not in that document, and that is the procedures that individual transportation security officers actually use at the checkpoints. So that is, I think, an important distinction to make about this particular document.

Senator COLLINS. But let me tell you what is in the document, and since this document is widely available now and has been discussed in the press, I do not believe I am revealing anything that is not already out there. And, Mr. Heyman, I will address this issue to you.

There is a whole section in this document on credentials, on the IDs that are used by the Central Intelligence Agency (CIA), that are used by the U.S. Marshals, that are used by the Bureau of Alcohol, Tobacco, and Firearms. There are pictures of the actual IDs and of the badges.

I would say to my colleagues that there is a page with a picture of what an ID for a U.S. Senator looks like. And, ironically, in the airport this weekend, I had the screener look at my ID and check the manual.

So this is important. If we are talking about making sure that people who would do us harm do not have the ability to falsify documents, we have given them a textbook on how to do so in this manual because we have showed them exactly what documents look like for individuals who are likely to receive less screening because they have these documents, because they are law enforcement officials, for example. So there is a lot of sensitive information in here.

Have you notified the agencies whose credentials are included in this document to tell them that the information is out there and that now their credentials may be vulnerable to being counterfeited?

Mr. HEYMAN. Thank you, Senator, and I suppose I should thank Under Secretary Beers for the opportunity to answer this question.

Let me just echo Under Secretary Beers' comments. This is entirely unacceptable. There is no one at the Department who has any opinion to the contrary on this, and you bring up what are the next steps on this.

First of all, there is a full investigation that is underway. In the last 48 hours, we have removed the information from the Web site. The practice of posting SSI documents in whole or part has been suspended pending further review. The Acting Administrator yesterday designated all operational standard operating procedures to be designated in whole as SSI. And the appropriate persons have been put on administrative leave pending the review.

We also need to recognize that it is axiomatic to security, and particularly to aviation security, that we have a defense in-depth and a layer defense that no single security measure is the entirety of our security measures. As Under Secretary Beers has made clear, this is one of a number of manuals for securing the checkpoints, and it is also important to note that while terrorists change their tactics, we change our tactics, too, on security. That is why there are six versions of this document. That is not to say that we change our secure documents as you have indicated on a regular basis, but in the interim, we have actually already put in place interim security measures that are being deployed enterprise-wide, and we have, in fact, as you have asked, notified not just those who may be interested stakeholders in the unauthorized release of this information, but also other stakeholders who we work with on a day-to-day basis.

Senator COLLINS. Are you conducting a damage assessment, such as would happen in other parts of the intelligence community when there is a breach like this?

Mr. HEYMAN. Yes. There is a review of the actual incident. There is an Inspector General (IG) review going on there. And we are looking at what the implications are to security.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks very much, Senator Collins.

So do I understand that, therefore, you will be considering perhaps even reengineering parts of the systems to close any of the vulnerabilities that may have been exposed by this breach?

Mr. HEYMAN. We are going to let the review give us the indication of where we should go.

Mr. BEERS. But in particular on the issue of identification, there are additional augmented layers with respect to those exempted categories to ensure that there is a second official—or that TSA Acting Administrator Gail Rossides has put in place a second official who will ensure that to the extent that we can identify fraudulent documentation—and we do spend a lot of time looking at fraudulent documentation, including official identification, to make sure that we are having a second look, to make sure that those kinds of exposures, in fact, have a second layer, as Mr. Heyman indicated, in terms of our protected interests.

Chairman LIEBERMAN. OK, I appreciate it. I think those remembering that line from the 9/11 Commission that the events of September 11, 2001, happened because of a failure of imagination, I think at these moments we have to imagine—and I am sure you will—what a terrorist group thinking about getting into the United

States would do with information that has been released now and, therefore, what we can do to alter procedures or create second layers to block that from happening. Does that make sense?

Mr. HEYMAN. Absolutely. Yes, sir.

Chairman LIEBERMAN. Thanks. Next in order of arrival is Senator Burris.

OPENING STATEMENT OF SENATOR BURRIS

Senator BURRIS. Thank you, Mr. Chairman.

I do not think I heard a definitive answer to Senator Collins' question. Were the other agencies notified about the badges and the imprint in the document? Have you all made contact with them to reference those specific badges or identification for these various law enforcement persons? Yes or no.

Mr. HEYMAN. Yes.

Senator BURRIS. Thank you.

Let me change the subject a little bit because in terms of the whole move of trying to protect our borders and to secure the travel to and from our country, we just passed legislation here called the Tourist Act to try to encourage tourists to come to the United States because we are losing so much money because more Americans are going abroad than visitors are coming here. But have we noticed any impact on tourism as a result of our seeking to have the no-fly list, the screening, the fingerprinting, and this process? Has anyone done any type of a study as to how it is affecting tourism coming into America?

Ms. JACOBS. Thank you, Senator. The Department of Commerce actually does keep track of the number of foreign visitors coming to the United States in any given year, and there is no question about the fact that immediately after September 11, 2001, I think for a variety of reasons, not simply because of new screening procedures, there was a drop in the number of people coming to the United States.

For our part in Consular Affairs, after September 11, 2001, we knew that we had to really focus on security, but at the same time, we also were well aware of the need to continue to allow legitimate visitors into the United States. And so we set about trying to strike the proper balance between what we often call secure borders and open doors.

We have made a number of efforts to facilitate the travel of students and exchange visitors, for example, and I would note that in the most recent report published by the Institute of International Education, the number of foreign students in the United States increased by 8 percent last year.

We have also tried to facilitate business travel because we have heard loud and clear from the U.S. business community that they felt that somehow——

Senator BURRIS. I understand business travel is down.

Ms. JACOBS. Business travel, I think, is down this year from last year. A lot of people attribute that to the global economy.

Senator BURRIS. But have there been any studies attributing that to the increased requirements, of getting a visa to come from the consulate or trying to get into the country? Do the businessmen want to be bothered with fingerprinting and all of these screening

processes that they have to go through? Have any studies been done in that regard?

Ms. JACOBS. I am not sure that there have been any sort of scientific studies. Certainly we have heard anecdotally of people who say that they do not want to come because they believe it is too hard. We have done an awful lot of outreach overseas and also here in the United States to various——

Senator BURRIS. Well, that will create a problem for this promotional legislation that we just passed. We are now putting funds into saying come back to America, bring us your euros or whatever the currencies are, because we are having an economic problem with travel. So that would be the Commerce Department that would have to promote this kind of thing in cooperation with the State Department? Or which agency?

Ms. JACOBS. Well, the Department of Commerce, of course, helps the tourism industry here, so it tries to promote travel and tourism. We certainly try to get the word out that our borders are still open, our country is still welcoming of legitimate visitors here to the United States.

I really do think, sir, that it is a function of the global economy right now. That is why we are seeing a drop in the numbers. I think once a recovery is underway, we are going to see those numbers come back.

Senator BURRIS. Let us hope so, anyway.

Mr. Healy, you named several agencies involved in this whole screening process, and I was listening to you as you gave the various agencies. It appears to me that there is just a bureaucratic boondoggle with agencies involved in this whole process. Could you give a list of all the agencies that are checked—Homeland Security, the State Department, the FBI, and then Homeland Security has about three or four different agencies involved, and then all that information is supposed to come into your database, the TSC, to check this person and get back to whoever is sending the information in to you. Please give me kind of a rundown of how this will work with all these various agencies involved.

Mr. HEALY. Yes, Senator. Let me describe kind of how the process works, if I could.

Senator BURRIS. Sure.

Mr. HEALY. There are members of the intelligence agency that would include the FBI and the CIA; and there are members of law enforcement. If they have identified a known or suspected terrorist, this is how the process works. They have a vetting process that they go through. So if they identify somebody, they have their normal process that they go through. They vet that name. If it is an international terrorist, as an example, it would go then to the National Counterterrorism Center. The National Counterterrorism Center would vet that name as well. There is a process that they go through. There is a minimum derogatory information that they would go through, that they would look at, that I described, and I have it in much more detail in the written testimony. So NCTC will vet it a second time.

After NCTC has looked at it and vetted it a second time, it goes to the Terrorist Screening Center where it is vetted a third time. So once it gets vetted at that point, it gets entered into the Ter-

rorist Screening Center database. Once it is entered into the Terrorist Screening Center database, what we did was to be able—because of Homeland Security Presidential Directive (HSPD–6)—to be ready to be available to screening partners, we think a look at what existing databases they had.

So what we do is we export it out to a database called NCIC, National Crime Information Center, that makes it available to all State and local police officers. We export it out to Department of State's system. We export it out to DHS's system. And so when they encounter an individual, they do their normal process, and then it will pop up that this individual has been watchlisted.

When they see that, there is a process that they go through where they will eventually contact the Terrorist Screening Center to verify whether or not this individual is, in fact, the person. Once we have done that, then we notify the FBI for the operational response.

So I know it sounds like a spaghetti soup of different agencies, but it actually works very effectively in terms of the process.

Now, we have multiple agencies that work at the Terrorist Screening Center, from TSA, Department of Homeland Security, Customs and Border Protection, ICE, and the FBI.

Senator BURRIS. So you are saying all those agencies are working right there in one location. You do not have to send data back and forth to a central location in that agency, but the agencies are right on site.

Mr. HEALY. Yes, sir. This screening process works at the Terrorist Screening Center, and all these components are at the Terrorist Screening Center. The screening process occurs right there.

Senator BURRIS. That makes sense.

Mr. HEALY. It comes into the TSC. It goes out of the TSC. When encounters occur, you have basically all the subject matter experts there to work the process, to identify the individual and make sure that it gets out to the appropriate law enforcement agency for the appropriate response.

Senator BURRIS. Mr. Chairman, I see my time has expired, but I have to go and preside. I wonder if I may take a couple more minutes. Is that permissible?

Chairman LIEBERMAN. It is OK with me, and Senator Ensign, your colleague who is next, has graciously——

Senator BURRIS. Thank you, Senator, because I am concerned about a couple of friends who have been on a list, and they cannot get their names off the list. Who handles this list? When they go through the airport, their names are on the list, and they turn them around, and they go through this process every time they travel. It has not happened in the last few months, but I have talked with one of the young ladies who is a tall, very good-looking blonde. She looks as American as apple pie, but her name evidently is a name that is not common. I will not say her name for her own protection, but she has trouble every time she goes to an airport to travel, and she travels a lot. What is the story with that?

Mr. HEALY. Senator, I think I can try to help you there. I was in a unique position because when I got to the Terrorist Screening Center, I was there during the early stages that we started up, and

then I left for a period of time, having different assignments within the FBI, and then I came back.

One of the things that I noted when I came back was the redress process, and it was the first thing that they briefed me on. The redress process during the early stages of the TSC was actually kind of a dream, and what it allows us to do, in cooperation with the Department of Homeland Security, is allow the individual that feels that they have been watchlisted an avenue to go through. They go through the DHS TRIP program, the Traveler Redress Inquiry Program, and they submit their name, and then that component will vet it to determine whether or not this person is on the watchlist. And the DHS TRIP program will work with that innocent traveler to facilitate their travel.

Senator BURRIS. But does it go all through the system? Because I know that one time she was going to New York and she was trying to exit New York, and her name was in New York. And it was just a shock to her that—I guess the list is there because she had supposedly been cleared 2 or 3 months ago from some other airport, but the name had not been removed.

Mr. HEALY. Well, the traveler redress process, when DHS vets that, and if it has some connection with our watchlist, it will get vetted to us. I have a redress component unit that goes through that name. What they do is they look and they work with the case agent—if this person is legitimately watchlisted, they will work with the case agent to see, is there any way that we could downgrade this person.

Senator BURRIS. Do the names stay on the list?

Mr. HEYMAN. Senator, the TRIP program was intended to be a one-stop shop so that individuals could go and not have to go out to all of these different agencies that are doing the security review. It is now available on the Web site, and your friend or colleague can go there. It is adjudicated by all of the agencies involved, but you only have to go to one place, enter your information, and it will be passed on. The Web site is www.dhs.gov/TRIP.

Senator BURRIS. I hope that she——

Mr. HEYMAN. That she is listening.

Senator BURRIS. Yes. Thank you very much, and thank you, Mr. Chairman. And I do have to leave. I appreciate the extra time.

Chairman LIEBERMAN. Thanks, Senator Burris. Good questions.

Senator Ensign, thanks for being here. Good morning.

OPENING STATEMENT OF SENATOR ENSIGN

Senator ENSIGN. Good morning. Thank you, Mr. Chairman, for holding this hearing. I come from the State of Nevada, and tourism is very important to my State, but also a lot of people do not realize how important it is to the entire country. If you combine it all together, it is either the No. 1 or No. 2 most important industry as far as from an economic standpoint for the United States. So it is critical in some of the work that is being done here to make sure that we have tourism being taken care of, that we have balance between security and making it easier for people to come here.

Having said that, what Senator Collins talked about with this TSA document, that gets back to tourism as well. If people do not

feel safe, they do not travel. As we saw after September 11, 2001, it is psychological. And this is an incredibly serious matter.

Now, Mr. Beers, you mentioned that this is an old document. But these particular documents that we use, our identifications, these are current. These are not old ones. This one actually says January 2007 to 2009. That is the one that we are using right now. And so I do not think that this is something that we should just dismiss. I realize that maybe some parts of the document may have been reworked, but there is a lot in there that is probably still being used.

How high up did the authorization have to go before this was leaked? Did it go up to political appointees? Or were these just career people who leaked the documents? Mr. Heyman.

Mr. HEYMAN. This was not leaked. It was inappropriately put up on the Web site.

Senator ENSIGN. Who authorized it?

Mr. HEYMAN. This was done in the Security Office, I believe.

Senator ENSIGN. How high up did the authorization have to go before it was allowed?

Mr. HEYMAN. I would have to get back to you on that.[1]

Senator ENSIGN. I think that is really important. And not only the people who put it on the site, you said that these people were put on administrative leave. I think Mr. Beers is the one who said that. Were the people who authorized it also put on administrative leave? You said you do not know who authorized it.

Mr. HEYMAN. Again, we would have to get back to you. We are doing the review right now.

Senator ENSIGN. OK. But you made the statement that they were put on——

Mr. HEYMAN. People who were involved in this have been put on administrative leave. That is the information we got from the TSA Acting Director this morning before we came over here.

Senator ENSIGN. OK. Let us make sure you get back to us to find out whether the people who authorized it were also put on administrative leave. We do not want to just have a scapegoat out there. The people who authorized this need to be held responsible as well. I consider this a very serious breach.

You mentioned that a review is going on. Do we have a timeline on the review?

Mr. HEYMAN. No, I do not have that for you.

Senator ENSIGN. OK. Do we know when we will have a timeline? Is it months? Is it weeks?

Mr. HEYMAN. No. They have been moving very quickly on this. There are two reviews. There is the Inspector General review as well as the Office of Investigations review.

Senator ENSIGN. OK. If you could get back to us on how long you think it is going to take to complete the review process.

Mr. HEYMAN. Sure, happy to.[2]

Senator ENSIGN. Obviously, there are several aspects of the review. I realize that. But as far as at least give us the various timelines when people could be held accountable as well as when

[1] Responses to the questions asked by Senator Ensign appear in the Appendix on page 117.
[2] Responses to the question asked by Senator Ensign appear in the Appendix on page 118.

the review process—what Senator Lieberman talked about, where some of the policies would be changed and evaluate whether or not—how many things need to be changed. That is something, whether it is in a classified forum or whatever, that we as members of the Senate should certainly be able to have access to.

Mr. Chairman, that is the reason I attended today. I wanted to make a couple of points on this because I do think it is so serious a matter, that is seems too often that people are not thinking through things or whatever on our security. I agree with you, before September 11, 2001, was people did not think things were going to happen. We have not had a terrorist attack here in a long time, so people may be a little lax with security and things like that. I know that is normal human nature. That cannot be allowed in the world that we live in today, so this is a very important matter and needs to be looked at very carefully.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Of course, I agree with you, Senator Ensign. I appreciate your line of questioning and what you have just said. Maybe we will do one more round as we have questions.

I wanted to ask you some questions coming from this very troubling case of the American citizen, known as David Headley, charged in Federal court with six counts of conspiracy to bomb public places in India, to murder and maim persons in India and Denmark, to provide material support to foreign terrorist plots, to provide material support to Lashkar-e-Taiba (LeT), a Pakistan-based terrorist group affiliated with al-Qaeda, and six counts of aiding and abetting murder of U.S. citizens in India.

He is alleged to have made five trips from Chicago, where he was living, to Mumbai from 2006 to 2008 to conduct pre-attack planning and surveillance for LeT on many of the targets that were struck in the November 2008 Mumbai attacks. Because Headley is a U.S. citizen, his travel, at least based on that, based on entry and exit, did not raise suspicions, although it may have in other ways, I understand. He was able to use the United States as a base of operations. In the briefings that I have had on this, without revealing anything classified, it seems, I gather, that he was not involved in any plots related to targets in the United States, although one wonders whether that would have been the case for an extended period of time, but that he was using this as a base from which to plan attacks outside of the United States.

It just leads me to ask—and this is a difficult order, with everything else we are doing and trained to do—to what extent should a case such as this one lead us to think about broadening the screens that we have in an attempt to detect and disrupt American citizens or residents who are traveling overseas to carry out terrorist attacks and how one might do that?

Mr. BEERS. Mr. Heyman, do you want to start?

Mr. HEYMAN. Sure. Look, these cases are significant, a number of cases recently, and I think we see that individuals and, in the specific, U.S. citizens are, in fact, sympathetic to al-Qaeda, to its affiliates, to the ideology, and as such, we can no longer assume that Americans are not involved in terrorism. As indicated by the recent indictments, we see also the nexus of travel in those who

may get further indoctrinated abroad or perhaps trained or otherwise.

We will continue to pursue the programs that we have been pursuing to these days that I think have been effective. That is to say, continuing to engage with communities through our links to State and local partners, we need to do that. I think we need to continue working with our colleagues in the FBI and the intelligence community to be able to identify threats. Travel in and of itself is not necessarily an indicator.

Chairman LIEBERMAN. Yes, that is the challenge, right?

Mr. HEYMAN. Yes. And so I think those are the kinds of things that we continue to pursue so that we can help law enforcement at the earliest time identify those who may be participating in these kinds of activities. And I know you said you had——

Mr. BEERS. We certainly have a constant review of those procedures going on, and they have been changing. And while I do not want to talk about——

Chairman LIEBERMAN. Which procedures do you mean?

Mr. BEERS. The procedures that DHS, in our responsibility for monitoring travel in and out of the United States or in the United States by air, has modified procedures based on information from the intelligence community in order to try to stay current with what we know to be the case and anticipatory in terms of trying to think out of the box in order to do that.

The actual information, as you well know, sir, about the possibility of Americans or Westerners being trained in Pakistan has been out publicly based on the Director of National Intelligence's statement of, I believe 2 years ago.

Chairman LIEBERMAN. Correct.

Mr. BEERS. And that information obviously was made available to us, including in classified forums, and so we have looked at ways to try to make sure that we are ahead of the curve on this. But going beyond that, obviously we get into classified information.

Chairman LIEBERMAN. It is difficult. Is there a role to be played here in sharing information on potential terrorist travel with other nations? Mr. Heyman.

Mr. HEYMAN. Yes, there is a role, and we actually do collaborate, cooperate, and share information with partner nations, and there are definitely opportunities to do more of that. In the recent arrest in the Netherlands with the Somali, that was in close cooperation with the Dutch Government.

Chairman LIEBERMAN. Good. Let me ask you two questions that come from the Headley case for me. One, it has been reported that Headley changed his name. One parent was Pakistani, one parent was American. His original name was Daood Gilani, and he changed it to David Headley, allegedly to reduce scrutiny by immigration and customs officials while traveling.

I wonder, as this is a test case, what can be done to try to block this kind of name change being used as a way to avoid being on a watchlist or being picked up by some other terrorist blockage system. You get my point. To what extent can an individual like this make it harder for him to be picked up by changing his name, in this case to an American- or English-sounding name?

Mr. HEALY. Chairman, it is difficult because, first of all, I am in a difficult position about commenting on a particular case.

Chairman LIEBERMAN. Yes, understood.

Mr. HEALY. But I find challenges in my particular position because it is truly a balancing act. It is a balancing act between safeguarding civil liberties and protecting the American people. And the best we can do is just keep driving the intelligence and keep working the intelligence as much as we possibly can to get the information.

I do not know how else you could do it.

Chairman LIEBERMAN. Does anyone else have a response on that?

Mr. HEYMAN. I agree with Tim Healy that this is a challenge. Those who are seeking to do harm are constantly hearing what we are doing, watching what we are doing, and adapting to that. So changing names may be one thing. Changing secure documents—attempting to change documents, changing even biometrics, people do that. So we have to constantly be working to try to counter that through technology, through procedures, but also through additional layers so that we are not just resting on one thing, one security solution.

Chairman LIEBERMAN. Yes. I think without making too much of a point of it, even though the Headley case presents challenges to the system or questions about it, the fact is that through quite remarkable work across law enforcement and intelligence, he was identified and was stopped. And, of course, though he traveled legally in and out of the country, we do have records, of course, of every time he traveled in and out, which are part of the case that has now been built against him.

With the indulgence of my colleagues, I want to ask you another question. This is a fact case, and I remember it was presented to us as a worry by one of your predecessors in the last Administration at the Department of Homeland Security, and this is something I know people worry about. This is the dual passport issue. Someone with Pakistani and United Kingdom passports travels to Pakistan with his Pakistani documents, and then comes to the United States with his British passport, and we do not have any record that he traveled to Pakistan. I do not know if that is a question without an answer, but I pose it to you because I remember that as a practical fear based on the presence of all the training camps and centers of world terrorism in the Pakistan-Afghanistan area now particularly.

Mr. BEERS. Sir, that continues to be a concern. I was last in London in November and had a 2-hour dialogue with a variety of British officials on this particular issue. It is one in which we are looking to work out procedures, and I cannot tell you we have worked them out yet, but we are absolutely aware of this and looking at whether or not there are ways within our systems to be able to catch that, because you are absolutely right. If the person left the United Kingdom under one passport and came back under another passport, being a dual citizen, that would be caught by the United Kingdom. But the travel under a Pakistani passport is not necessarily under the current system going to raise an alert. But they

are looking at that system, and I think we all have to be cognizant of that.

Chairman LIEBERMAN. Well, I am encouraged that you are raising the question. It is not easy to solve, but I appreciate that you are on it. Thank you. Senator Collins.

Senator COLLINS. Thank you.

Ms. Jacobs, to follow up on the question that Senator Lieberman just raised, I want to ask you about the status of the implementation of the stronger security requirements for the Visa Waiver Program that were enacted as part of the 2007 homeland security law. As you are well aware, the reason we are concerned about the visa waiver countries is their citizens are not required to be interviewed by the State Department officials overseas and submit to other background checks. So we have been seeking agreements with countries so that they share more information with us on potential terrorists, and that is required in order to be a member of the Visa Waiver Program.

Now, it is my understanding that there are 35 countries currently participating in the Visa Waiver Program. could you tell us how many of the 35 are currently providing us with the enhanced information called for under the 2007 law?

Ms. JACOBS. Thank you, Senator. I believe in my written testimony I refer to agreements with some 17 countries at this point, and we would be very pleased at the State Department, in conjunction with my colleagues here at the table, to come give you a closed briefing on how this process works and how we are going about trying to get countries to sign these agreements.

I will say that sometimes it is a challenge because of the different laws that countries have, especially regarding privacy. It can be difficult for them to sometimes sign these agreements. But I want you to know that the State Department along with TSC and other colleagues, are very actively involved in trying to get more of these agreements.

I would add that we were very happy to see the enhanced security measures that were put in place for the Visa Waiver Program in the 2007 law. We do believe that this has increased the security of the program. I think it has also really been a good motivating factor for other countries to increase law enforcement cooperation, sharing of data, so I think it has been a very good thing overall.

Senator COLLINS. Just to clarify, I think in your statement you say that the State Department and the TSC have agreements with 17 countries, but of those, only 13 are Visa Waiver Program countries. So it is my understanding that only 13 of the 35 countries that are Visa Waiver Program countries are participating. That really concerns me. That does not strike me as a very good sign that 2 years later we still do not have agreements with that many countries.

Ms. JACOBS. We continue working with all of the visa waiver countries trying to encourage them to sign these agreement. As I said, for some of them it is difficult because of their laws and the privacy laws and procedures that they have in place. But you can be assured that we will continue working with all of the VWP countries and other countries to try to get this data.

I will say that they are sharing some data, for example, on lost and stolen passports. They are now sharing that data with Interpol, which is a very big step. We now have a centralized way of checking for lost and stolen passports. But we will continue to work on these other data-sharing agreements.

Mr. HEYMAN. In fact, all 35 countries are sharing lost and stolen passport data now.

Senator COLLINS. Good. Mr. Healy, I want to follow up on the questions that our colleague from Illinois asked you about how an individual who should not be on the terrorist screening list ends up on the watchlist. And it is heartening to me to hear that there is now a single point where an individual can appeal to. However, back in 2007, there was a follow-up audit of the Terrorist Screening Center that was performed by the Inspector General at the Department of Justice that found that, on average, it took the Terrorist Screening Center 67 days to close its review of a redress inquiry.

Now, if you are on the no-fly list and you need to fly for business, 67 days is a pretty long time to try to get your concerns resolved if, in fact, there has been a mistake. Is it still that long on average? Or has progress been made since this audit was issued?

Mr. HEALY. Senator, we have been able to reduce that time frame. Again, we work with our partners, DHS, on that particular process. We actually established a secondary process. We took a look at the number of individuals that we encountered regularly that were properly watchlisted to see if we could help that process as well. We took a look at another process where we looked at individuals who have similar names but that we have encountered numerous times that were not on the watchlist. And so we actually proactively reach out to work that, unknown to the individuals, to make sure that we work with DHS in that process that I described so that they could have no screening issues associated with that.

So it is a challenge. Again, when I first got to the TSC at the very beginning, the redress process was kind of a dream. And when I came back to be associated with it about 10 months ago, it was a dream that became a reality, and that was a lot of work, a lot of cooperative effort between DHS and ourselves, and then a lot of proactive work. The American people do not know, they do not have to necessarily file with the DHS TRIP program. If we get a congressional inquiry, it automatically starts that. If we read something in the paper about an individual that claims they have had a problem, we automatically start that process as well.

So I am excited about how it works, and I am excited about how we were able to do it. But, again, when it finally gets to us, the vast majority of people that think they are on the watchlist typically are not. When you take a look at DHS TRIP, the number of inquiries that they had, they had over 78,000 inquiries of people that thought they were on the watchlist. Of that, there were just over 500 that were actually on the watchlist that got to us. So the numbers just do not work out. They are stopped for a number of reasons not having anything to do with the terrorist watchlist.

But we, together with DHS, work proactively to really try to satisfy them. We take it very seriously. Again, the challenge that I have is protecting the American people, but safeguarding civil liberties. And if I cannot do both, then I have failed.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins.

Senator Voinovich, welcome. We had a conflict of events today where there was an announcement of legislation that I have worked on with Senator Voinovich, Senator Conrad, and Senator Gregg on deficit reduction, and so you represented me there, I am sure quite well, as I have attempted to represent you here. But, anyway, welcome and please proceed.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Mr. Chairman. I pointed out in this session that the two of us cosponsored a bill to create the SAFE Commission and that Senator Conrad and Senator Gregg took that vehicle and tweaked it to have something that is going to be acted upon next year, which is terrific. And I think everyone understands that if we do not get our debt and our budgets taken care of and address our fiscal responsibility, a lot of the things that we are trying to do to secure America, we will not have the money to do.

Chairman LIEBERMAN. Absolutely right.

Senator VOINOVICH. I think Senator Conrad said it well. He said next to our national security, the issue of the debt is the second most important thing we need to deal with right now because people are really questioning our credibility and our credit, and they are very uneasy out there. So I am really pleased that there are 27 sponsors, and we have not even gone out to find others. Maybe we will get something done. It would be wonderful.

Chairman LIEBERMAN. You have been a very persistent and principled leader in this, and I appreciate what you have done. So my goal is to make sure we get this done before you leave the Senate next year.

Senator VOINOVICH. It will make my children and grandchildren very happy.

When we got involved in the Visa Waiver Program (VWP), I was very much involved in that, and I would like you to comment on how that has really resulted in putting the pressure on other participants in the program. Senator Collins made a point about it, that there are 35 countries that participate and only 13 have complied with program requirements. If we had not gone forward with the Visa Waiver Program expansion, would we be as far as we are with these other countries that really are not up to where they ought to be? I mean, these new countries have done a great job. They are almost role models, and I understand that by the end of this year, Greece is finally—in fact, I talked with Prime Minister Papandreou. He is excited that, I guess, the Greeks have finally done what they are supposed to do, and they are going to come on board with the program. But if it had not been for that 2007 VWP legislation, we would not have been in a position to lean on these people.

Could you comment on that at all and how it has helped security, and also, if you might, our public diplomacy?

Mr. HEYMAN. Sure. Thank you, Senator. I know you have been a terrific leader who supports this program, and we thank you for that.

The Visa Waiver Program is an extremely important instrument of institutional cooperation with our allies. From a security perspective, VWP has helped to introduce, expand, and accelerate a host of improved security measures. We talked about them this morning. We have enhanced passport requirements now the standard—not just with visa waiver countries—verifiable standards at airports, aviation security, and in general, greater cooperation with the United States on an array of law enforcement and security issues.

Moreover, as I just mentioned, nearly every VWP country now reports lost and stolen passports to Interpol, and they do that according to Interpol standards. So from a security point of view, this has been a step in a very good direction.

But it is also beyond that. It is my belief that there is the security in the national security sense that we do not talk about in terms of transactions, and that is, by facilitating travel to the United States, the VWP plays a vital role in strengthening the ties between nations, between peoples, and that is something we were talking about earlier in terms of the decline in travel to America. We certainly think that we are now facilitating enhanced security and travel between these nations.

Senator VOINOVICH. Well, it is interesting. I was in Latvia in July, and I met with President Zatlers and some of his folks, and they said that General Mullen was in Latvia, and he would have ordinarily been on the front page of the paper, but it was the same day that they announced that Latvia was going to be participating in the Visa Waiver Program, and that was the front-page story, and President Zatlers also relayed how excited people were that they were going to be able to take advantage of this program, and the same thing was said in Lithuania.

So you would think that because we moved on that legislation now we would try to get other countries to come on board and meet those high standards that have been set. But the question I have—and I know you may not be able to answer it today, and it follows upon what Senator Collins said: What kind of sanctions do you have? Are you in the position where you can say to a country, look, we have given you enough time, you are not doing what you are supposed to do, and, by the way, if you do not do it, we are going to take you off the list? That is tough.

Mr. HEYMAN. That is a tough question, and I think the program has been designed to take a deliberative, continuous assessment of security. We continue to monitor threat situations, immigration activities, border security on a regular basis in these countries, as well as compliance. And there is a requirement that the Department formally review VWP designation status at least every 2 years. These formal reviews evaluate the country's compliance to the security requirements and whether the country poses a significant risk to U.S. interests. So that process is in place, and we do continue to review not only on a day-to-day basis but also with these biennial formal reviews.

Senator VOINOVICH. Well, I have a suggestion that may be inappropriate, but there are Members of Congress that have good relationships with some of these countries. Just maybe a telephone call from us or a visit to them might indicate that we understand that

they are not doing what they are supposed to do, or let them know that we are aware of it. That might be helpful, particularly coming from those of us on the Foreign Relations Committee or the Appropriations Committee.

Mr. Beers, I understand that we are going to hear from you. You answered Senator Lieberman's question about how we are going to handle the biometric air exit situation.

Mr. BEERS. Yes, sir, and I hope to be able to come up and brief you all on the Secretary's decision in the not too distant future. From our last conversation in your office, we did complete the pilot study. It was delivered as required to the Appropriations Committee. It is an indication of how that worked in the two test cases that we ran.

We have since then taken that study, which we actually began before the formal delivery to the Hill because we had the information that we needed in order to begin our own recommendation, to the Secretary. Mr. Heyman and I are running that process. We have had several meetings, including one just recently. I think we are at the last stage of presenting the Secretary with the options. When she decides, I will come up, as I promised you, and brief you.

I told Senator Collins the same thing, but you know it even better—it is going to cost money, and we thank you for the additional funds that you saw fit to add to our ability to use, at least in the initial stage, those funds to get this program started. And as I told the Senator, that will be helpful. We would hopefully both come up here and talk with you about the process, about the funding requirements, go through with the rulemaking that will be necessary in order to undertake this, and begin I think by the beginning of next fiscal year, at least with the first stages of that program. Hopefully, we will be able to do it sooner, but I do not want to make a promise that I do not think we can keep. But we will keep you, and the full Committee, of course, fully informed in terms of where we are in that process.

Senator VOINOVICH. Can I follow up?

Chairman LIEBERMAN. Senator Voinovich, go ahead and take whatever time you need because we had a colloquy that took from your time.

Senator VOINOVICH. We did put some money in the homeland security budget for that, and I was assured that it was enough to get you started. But I want to make it clear to you that I need to know how much money you do need.

Mr. BEERS. Sir, you have made that abundantly clear. There is no doubt about that. [Laughter.]

Senator VOINOVICH. I have got one more shot next year. That is good. I hope we can move on it.

Senator Lieberman, one of the problems we have got here is that the law says that if we do not have this new process put in place for biomatric air exit, no new countries can come in unless they have a visa refusal rate of less than 3 percent, turned down. And so there may be countries that are not now signed up who can't get in to the program. How many countries do you have that are trying to get in the program now?

Mr. HEYMAN. We have 35 Visa Waiver Program countries.

Senator VOINOVICH. Yes, but what I am saying is you have got a bunch of people, I know, like the Croatians and others who are trying to get qualified. Do you know how many countries are waiting to come in?

Mr. HEYMAN. There are a number of countries that are interested that do not—that are looking to have the program expanded, which we are not expanding at this point, but we are looking to do that perhaps——

Senator VOINOVICH. What I am interested in knowing is how many countries have come to DHS interested in joining the program, and you have told them what the requirements are to get in. Do you have any idea off the top of your head of how many there are?

Mr. HEYMAN. I think it is four, but I can get back with you.

Senator VOINOVICH. OK. Well, the point is that there are not that many right now, but you might get to the point where biometric air exit is not in place, because it is going to take a lot of work. Mr. Beers will be able to tell us just when it will be up and running. And if you get a big backlog of these countries that have done a good job of meeting our requirements and you are saying to them, well, we cannot admit you because we do not have biometric air exit done, it might be an issue and something that you want to look at next year or maybe even the year after. Hopefully, it will be done by then.

Thank you very much.

Chairman LIEBERMAN. Thanks, Senator Voinovich. You have one more official shot, but, I will always take your phone calls when you are back in Ohio. [Laughter.]

Senator VOINOVICH. I have heard that before.

Chairman LIEBERMAN. I will say, "George who?" No, it will be a pleasure to hear from you anytime.

I want to ask two more quick questions. Maybe the answers are not so quick, but just to bring us up to date. Director Healy, the terrorist watchlist, as we have described, is really quite a powerful tool for us in detecting terrorists, denying them the ability to travel. Obviously, it is largely name based, but I understand that in recent times there has been an attempt to add fingerprints, which, of course, would greatly increase the utility of the system.

Tell us a little bit about that and what more you can do to expedite that.

Mr. HEALY. HSPD–24 talks about biometrics, and it talks very specifically, Senator, about three types of biometrics: Fingerprints, iris, and photos.

Chairman LIEBERMAN. Right.

Mr. HEALY. Right now we are working to implement HSPD-24 and will be on time, on schedule by the end of this fiscal year.

Currently, we now receive all three of those biometrics. We store them, and currently we export to Department of State photographs. And so we are working on that. It is a very effective tool. I could give you an example that I do when I talk about the Terrorist Screening Center that we had an individual that knew he was watchlisted, actually changed his identity, came into the country, and was applying for citizenship. And, fortunately, we had his fingerprints, and he was picked up for a driving under the influence

(DUI), was fingerprinted, and was identified as a KST, a known or suspected terrorist.

So we are working in cooperative effort with the Criminal Justice Information Services (CJIS), the FBI, DHS, Department of State, and Department of Defense in making sure that we get those biometrics and that we are able to meet that deadline for HSPD–6. But you are exactly right. When you do have that, especially on the no-fly list, you can actually identify that individual before they get on a plane and be able to avert that travel.

So it is a challenge, but, I think we are up to it, sir.

Chairman LIEBERMAN. So to the extent that you are able to testify in open session, how do you obtain fingerprints of people on a terrorism watchlist?

Mr. HEALY. Again, in consideration that we are in open testimony, sir, I would say that we go through the normal process in terms of the intelligence community to see what they can do in terms of that. We work with the Department of Homeland Security and, again, CJIS and IAFIS to see if there is any type of records available. So we would go through the normal research process that we do to enhance the record as much as we possibly can.

Chairman LIEBERMAN. Am I right that it may be that our troops in Iraq and Afghanistan, when they can, are adding fingerprints to the system?

Mr. HEALY. Yes, sir. And that is primarily where the fingerprints are coming from, especially on the battlefield, sir.

Chairman LIEBERMAN. Correct. Under Secretary Beers, I have a final question about US–VISIT and the fingerprint matching, which is really quite an extraordinary achievement and advance. We have heard reports, however, that it can take up to 72 hours for US–VISIT to, for instance, inform a Customs and Border Protection officer that a biometric match has been made with a criminal record. I understand that the typical primary inspection takes seconds, or minutes at most. But if I am right about this, what are the reasons for delay in returning matches to the inspecting officer at the point of entry? And is there anything being done to try to ensure that this happens in a more timely fashion? Obviously, the nightmare would be that somebody passes the initial screen, is out, and then there is a discovery at the point of entry that this person, in fact, has a criminal record, is on a terrorism watchlist, or is connected to terrorism more directly in a different way than the watchlist.

Mr. BEERS. Yes, sir. Basically, the issue now is the real-time compatibility with the FBI database and our US–VISIT database. The information is shared, but the ability of the Bureau to actually perform the matching requirements, while in many cases is in enough time to be able to do something about it, there are cases where it is not. Director Robert Mocney, who is sitting behind me, has been working assiduously with his colleagues at FBI in order to try to move this ball so that we can get within the 10-second rule, which is what we can do with our own US–VISIT database.

So work is going forward on that. I am hopeful that we will be able to resolve that. We did move, I think successfully, from the two-fingerprint rule to the ten-fingerprint rule that we implemented on our side to make sure that we can then give the Bureau

the same ten prints that we were not able to give them before because we were only taking two prints.

So this is an ongoing effort. I am not sure I can give you a time frame yet when we think that will be resolved, but I can attest because I participated——

Chairman LIEBERMAN. You will work it out?

Mr. BEERS. This is an active issue.

Chairman LIEBERMAN. We will ask you a question about time frame for the record. Maybe you have, as they say on cable news, breaking news.

Mr. BEERS. Yes, but as Mr. Healy indicated—and Mr. Mocney just passed me a note—the KSTs, those people where we have fingerprints that are in his database, that we have.

Chairman LIEBERMAN. That comes up right away.

Mr. BEERS. Right. This is the broader database that is more likely to pick up criminals rather than——

Chairman LIEBERMAN. Criminal background rather than the terrorism.

Mr. BEERS. Right.

Chairman LIEBERMAN. Senator Voinovich, do you have any other questions?

Senator VOINOVICH. No.

Chairman LIEBERMAN. Thank you. Thanks to all of you. I will keep the record open for another 10 days, and I have some additional questions that I will submit to you to answer for the record.

I appreciate what you are doing. Really, we have come a long way. Obviously, in an open country which prides itself on the ease of going in and out, which is something that is fundamental to our country, we have figured out, I think, thanks to information technology, an ability to not inhibit all the people who are coming here for good reasons while also figuring out how to stop the people who are coming here with bad motives. But, it is a constant challenge to be ahead of the enemy here.

So I appreciate very much what you have done. I understand, based on the exchange between Mr. Beers and Senator Voinovich, that you know that some of these programs cost money. But, really, we call on you to advocate to us, because we press you constantly to do everything and not to make any mistakes in doing it. Therefore, you have a right to come back and say to us, hey, this is what it is going to cost to make it happen. Of course, this is a fundamental part of what I think continues to be our primary responsibility, no matter what else we are doing, is to promote the common defense, which includes, in our time, providing the best possible homeland security.

Do any of you want to say anything in closing? No? If not, I thank you. I wish you a good day. The hearing is adjourned.

[Whereupon, at 11:31 a.m., the Committee was adjourned.]

APPENDIX

Five Years After the Intelligence Reform and Terrorism Prevention Act (IRTPA): Stopping Terrorist Travel
Homeland Security and Governmental Affairs Committee
Chairman Joseph Lieberman
December 9, 2009
AS PREPARED FOR DELIVERY

Good morning and welcome to our hearing, "Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel." Identifying potential terrorists and denying them the ability to travel into the United States is one of the most important homeland security challenges facing our country. Today, we will hear testimony from four government officials on the frontlines of our nation's efforts to stop terrorist travel. Their jobs are daunting and complex, and the disastrous consequence of mistakes is a pressure continually weighing upon them – and us.

We cannot afford to let down our guard, which is why I am so concerned about the TSA security breach that was discovered this past weekend. A highly sensitive screening manual was posted online, apparently for months, without being properly redacted. This was a serious breach because this manual includes information that could help terrorists to defeat the TSA inspection process. In this age of freely flowing information we must have adequate safeguards in place to ensure that terrorists aren't being given any advantages as they plot their nefarious acts.

As we all know, the 19 hijackers who attacked our country on September 11, 2001, traveled to the United States with visas, some obtained fraudulently, but most obtained legally. Two of the terrorists had overstayed their visas. The arrests in September of a number of people charged with planning terrorist attacks in the United States – Najibullah Zazi, Betim Kaziu, Michael Finton, and Hosam Smadi - are the most recent reminders that terrorists are still crossing our borders legally, living among us, and plotting to attack us.

This Committee takes very seriously its obligation to ensure that the Executive Branch is tackling head on the challenges posed by violent Islamist extremists who would seek glory by killing innocent Americans, and that begins with keeping these terrorists from entering America.

In the eight years since September 11, 2001, this Committee has authored a number of laws that Congress subsequently enacted to protect the homeland and, more specifically, to stop terrorists from coming to the U.S.

The Intelligence Reform and Terrorism Prevention Act of 2004 is notable among these laws because it enacted most of the recommendations made by the 9/11 Commission after its remarkable investigation into the circumstances surrounding 9/11. Many of the programs and systems we will examine today were recommended by the 9/11 Commission and included in the 2004 legislation.

For example, that law, called for a biometric entry and exit system for travelers into and out of the U.S., required travel documents to contain biometric information, and directed consular posts to collect biometric data from foreigners wishing to travel to the U.S.

It directed the President to negotiate agreements with other nations to share information on lost and stolen travel documents; required that consular officers be trained in the detection of terrorist travel patterns and document fraud; and required that anyone applying for visas to the U.S. be subject to personal interviews at consular posts abroad.

The Act further strengthened our screening system by establishing the National Counter-Terrorism Center and requiring that domestic and international airline passengers be screened against terrorist watch lists.

The Implementing Recommendations of the 9/11 Commission Act of 2007 also strengthened the Visa Waiver program -which allows travelers from certain countries to bypass the visa process and come directly to the United States – by creating the Electronic System for Travel Authorization (ESTA), a program that allows the Department of Homeland Security (DHS) to screen travelers before they board an airplane. Although ESTA is not yet fully implemented, it holds great promise. Countries participating in the Visa Waiver Program are also required to share law enforcement information, with the U.S. government.

Thanks to the dedication and hard work of the agencies represented here today, our travel screening system is far more capable of identifying terrorists and denying them entry to the U.S. than it was pre 9/11.

The interview at a consulate abroad is our first opportunity to identify a potential terrorist, which means consular officers must be trained and given the resources they need to detect potential terrorists.

I am concerned that as travel documents become more secure, terrorists and other criminals will use fraudulent primary-source or breeder documents, such as birth certificates, to obtain legitimate travel documents from our consular offices. Tightening the security of primary source documents here in the U.S. is a core component of the PASS-ID Act, which this Committee has reported to the full Senate. I urge the State Department to work with our partners abroad to ensure that they too are taking steps to improve the security of their primary source documents.

The terrorist watch list may be the most important tool to deny terrorists the ability to travel to this country. This database combines all the information the federal government has on people known to participate or suspected of participating in terrorism in any way. One of the government's largest failures leading up to 9/11 was the inability to share this kind of information across departments. For example, the 9/11 Commission found that information concerning known or suspected terrorists that was in the possession of different Federal agencies was not shared effectively. The investigation uncovered that two of the September 11, 2001, hijackers—Nawaf al-Hazmi and Khalid al-Mihdhar—were known to the CIA, the FBI, and the NSA and were regarded as dangerous by all the agencies. But that information was never shared

with the Immigration and Naturalization Service or the State Department, and therefore, these two terrorists were allowed to enter our country on multiple occasions with valid visas and be part of carrying out the most devastating attack on our homeland in our history. The 9/11 Commission concluded that, on four occasions in 2001, the CIA and the FBI had opportunities to take action against Mihdhar and Hazmi, but that "the U.S. government was unable to capitalize on mistakes made by al Qaeda." Information about these individuals was not entered on the State Department's TIPOFF database, the precursor to the terrorist watchlist, until August 24, 2001. And this, of course, was far too late to stop the attack.

In the months leading up to 9/11, we know that the system was "blinking red," as then CIA Director George Tenet famously put it. The system, however, was not set up to share that information among the different federal agencies involved in a timely manner. We now have the ability to leverage the terrorist watchlist and its integrated connections with other government databases to block the accidental entry into the country of anybody suspected of participating in terrorism.

We must also share information on terrorists and other criminals with our partners overseas. This is why I insisted that information-sharing agreements be mandatory for participation in the Visa Waiver Program. I am told that 13 of the 35 visa waiver nations have entered into agreements to share biometric law enforcement and terrorist watch list data with us – and the United States will be sharing the same types of information on a reciprocal basis to these nations. As a stark reminder of the urgency of these international agreements, this week an American citizen, David Headley, was charged in federal court with six counts of conspiracy to bomb public places in India, to murder and maim persons in India and Denmark, to provide material support to foreign terrorist plots, and to provide material support to Lashkar-e-Taiba (LeT), and six counts of aiding and abetting the murder of U.S. citizens in India.

Headley is alleged to have made five trips to Mumbai from 2006 to 2008 to conduct pre-attack planning and surveillance for LeT of many of the targets that were struck in the November 2008 Mumbai attacks. Because Headley was an U.S. citizen, his travel likely did not raise suspicions, and he was able to use the United States as a base of operations while helping to plan one of the most significant terrorist attacks in Indian history. Although it is not clear at this point whether Mr. Headley's travel raised flags within the U.S. government, this case underscores the need to implement these international agreements as quickly as possible and make sure that all 35 visa waiver nations and other nations with a common interest in preventing acts of terrorism eventually participate in similar agreements.

Finally, the implementation of a biometric entry system at all of our nation's ports of entry has been the centerpiece of our screening system. But we still do not have a biometric exit system in place despite numerous Congressional mandates. Identifying individuals who overstay their visas is a crucial component to stopping terrorist travel, as we saw in the case of the alleged Texas terrorist, Hosam Smadi.

US-VISIT uses biographical information to track overstays, but this is no substitute for a biometric exit system because a terrorist could game the system by having an associate leave the country with their travel document. This would leave a record of their exit in the system while they were actually still in the U.S., throwing investigators off.

I am even more concerned, however, that in some cases it can take up to 72 hours for US-VISIT to inform Customs and Border Protection of a fingerprint match at a port of entry. This means someone could be allowed entry into the country **before** being identified biometrically as a terrorist or criminal. Surely the advanced state of electronic technology today should permit for these matches to be made in seconds, not minutes or hours.

Because the federal government has made significant progress towards implementing these screening requirements, we are much safer today than were eight years ago. But we must do better. This Committee will be vigilant in the coming months to ensure that the federal government continues to strengthen its systems for ensuring that the events of September 11, 2001, never happen again.

Senator Collins?

Opening Statement of
Senator Susan M. Collins

"Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel"

Committee on Homeland Security and Governmental Affairs
December 9, 2009

★ ★ ★

Five years ago, this Committee authored the most significant reform of the nation's intelligence community since the Second World War. Today, we recognize there is no time to rest, no reason to pause, in our efforts to protect our country from terrorist attacks.

Earlier this week we received a chilling reminder of how a lapse in security can pose a serious threat to our homeland. A version of the Transportation Security Administration's (TSA) aviation security manual was posted on the Internet for anyone to read. Knowledge of TSA's passenger screening procedures could prove invaluable to those seeking to harm our citizens. By allowing the aviation security manual to be posted online, TSA has effectively given al-Qaeda and every other terrorist group a textbook for evading airport security.

Terrorists continually change their strategies and mutate their forms of attack. We know, however, that their aim remains to harm this nation and its people.

The 9/11 Commission noted that as many as 15 of the 19 hijackers might have been intercepted by border authorities if a procedure had been in place to link previously accumulated information to their names. Several of the hijackers had been cited in intelligence agency files for terrorist links. Existing but untapped data on travel patterns, bogus visa applications, and fraudulent passport information could have focused attention on some of the terrorists.

Following the attacks, the federal government took initial steps to deploy systems and procedures to help ensure that terrorists would not again slip undetected across our borders. And the Intelligence Reform and Terrorism Prevention Act of 2004, which Senator Lieberman and I co-authored, expanded and strengthened these nascent initiatives and implemented many of the recommendations of the 9/11 Commission. Five years after its enactment, the Intelligence Reform Act has accomplished a

great deal to prevent our nation from being attacked by terrorists whose plots originate outside our borders.

One of these successes is a biometric system for screening foreign nationals seeking to enter the United States. The State Department now collects fingerprints of foreign nationals who apply for visas at U.S. Embassies and Consulates overseas and compares them against databases with the fingerprints of potential terrorists and immigration violators. Those fingerprints are now checked at U.S. ports of entry by DHS to confirm that the individual arriving in the U.S. is the same individual who was approved for a visa abroad.

Another important accomplishment since 9/11 has been the creation of a consolidated terrorist watch list based on terrorism-related information from all parts of the Intelligence Community and the FBI. This consolidated list allows the names of individuals to be quickly checked to identify terrorism connections. The Intelligence Reform Act required that passengers on international flights to the United States and flights within the United States be checked against the terrorist watch list.

The GAO has recommended that DHS develop guidelines for the private sector to use the terrorist watch list to screen their employees. These guidelines, however, have not been issued. The owners and operators of our critical infrastructure should be permitted to screen their employees against the terrorist watch list on a voluntary basis, as long as appropriate civil liberties protections are in place. Najibullah Zazi, who plotted terrorist attacks in New York, was an airport shuttle driver at the Denver Airport. This case reminds us that terrorists could seek employment in critical infrastructure.

The federal government also has yet to establish a mechanism to screen mass transit workers, such as those who drive subway trains and buses, against the terrorist watch list. This was required in the 2007 homeland security law. Although 28 months have passed, no regulations have been issued by DHS. These employees have many lives in their hands every day, and a simple check against the watch list - like that already required for hazardous materials drivers, ferry captains, and airline pilots - might prevent a needless loss of lives if this mode of transportation were targeted.

This Committee authored legislation in 2007 that strengthened the Visa Waiver Program, which allows citizens of 35 countries to enter the United States without a State Department interview or advanced biometric screening. There is a significant potential that terrorists in one of these

mostly European countries could seek to do harm to the United States, as the 2006 plot by British citizens to blow up airlines over the Atlantic revealed. I understand, however, that only 13 of the 35 countries have complied with this requirement.

The federal government has done much since 9/11 to prevent terrorists from coming across our borders to do us harm and to prevent terrorists from traveling and working within the United States. We must do more to share terrorist watch list information and make the best use of opportunities to identify potential terrorists, without unnecessarily impeding the flow of legitimate travel and trade.

# # #

Statement for the Record

Rand Beers
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
Washington, D.C.

Terrorist Travel

December 9, 2009

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members, I am pleased to appear before you today to discuss the progress the Department of Homeland Security (DHS) has made in securing our Nation's borders. Our vision is to modernize and improve the immigration and border management system through integration, collaboration, and cooperation among all parts of the immigration and border management community, including U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, and the Department of State (DOS), among many others. These organizations continue to work together to accomplish a single mission—coordinating roles, sharing information and technology, complementing and reinforcing one another's business processes, and eliminating redundancies and gaps.

For terrorists to plan and carry out physical attacks on our homeland, they must have access to our Nation. As the 9/11 Commission's Final Report states, "Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger because they must surface to pass through regulated channels to present themselves to border security officials, or attempt to circumvent inspection points ... for terrorists, travel documents are as important as weapons."

When DHS was created after the terrorist attacks of 9/11, the Department's work to implement measures to identify and stop terrorist travel accelerated rapidly. Three areas received significant investment: 1) creating a biometrics-based screening capability that would also record the entry and exit of foreign citizens; 2) enhancing the security of travel documents; and 3) improving information sharing across Federal agencies to prevent the admission to the United States of known or suspected terrorists. I am pleased to tell you today that work on these three areas has made the Federal Government's traveler screening more collaborative, streamlined, and effective than ever before.

We have made significant improvements in the last five years:

- We have worked to unify immigration and border management systems in order to implement a robust, effective, timely and efficient capability to access and use biometrics-based information on criminals, immigration violators, and known or suspected terrorists.

- ICE identifies visitors who overstay their authorized terms of admission through an average of more than 300 credible leads that US-VISIT provides each week. Through ICE's Secure Communities program, we are also helping to identify immigration violators that state and local law enforcement officers arrest.

- Through the successful implementation of large scale biometric screening by US-VISIT we have provided support and leadership to biometric border management programs undertaken in the United Kingdom and Japan, and continue to support and encourage programs in various stages of application in the European Union, Canada, Mexico, Australia, Argentina, Peru, and other countries.

- We have put better capabilities in place for more efficient identification of fraudulent documents. We cooperated closely with DOS when it introduced an electronic passport, and we made every effort to ensure compliance with new passport standards by Visa Waiver Program countries. We have also worked together with State to implement the U.S. passport card, which provides U.S. citizens a secure, limited-use travel document in a more convenient format.

- We have implemented the Western Hemisphere Travel Initiative, whereby U.S. and Canadian travelers are required to present more secure travel documents that denote identity and citizenship when seeking to enter our country, helping officers focus on threats while making legitimate travel more efficient.

These are significant achievements that have improved national security and have impeded terrorist travel.

Biometrics-Based Screening: US-VISIT

The 9/11 Commission, Congress, and DHS all recognize that accurately documenting the entry and exit of non-U.S. citizens is a priority for securing our Nation's borders and improving the integrity of our immigration system. With biographic screening capabilities already well established, biometrics became the next logical step in the evolution of immigration and border management.

Two primary factors drive our use of biometrics. The first is the need to overcome the increasing sophistication of criminals and terrorists who are determined to circumvent our biographic-based security measures. The second factor is societal change—the public increasingly accepts the use

of biometric technology as an effective, convenient, and efficient means to guard against terrorism and fraud, including identity theft.

Biometrics addresses these factors because they provide a reliable and accurate way to establish and verify visitors' identities. Unlike names and dates of birth, biometrics is unique and difficult to forge. Biometrics helps us meet the challenge of making travel more difficult for those who want to do us harm, while making it convenient and efficient for legitimate visitors to come to the United States.

On January 5, 2004, DHS significantly advanced our Nation's border security by launching US-VISIT, a first of its kind, large-scale, biometrics-based identity and screening system, supporting the work of DOS consular and CBP officers who respectively make visa-issuance and admission decisions.

- Through its use of biometrics, US-VISIT provides identification and analysis services that help decision makers distinguish people known to pose a threat from the millions of people who travel with legitimate purpose. Biometric information is paired with biographic information to establish and verify an individual's identity; that identity is subsequently vetted against watch lists.

- US-VISIT checks a person's biometrics against a watch list of more than 4.7 million known or suspected terrorists, criminals, and immigration violators; US-VISIT also checks a person's biometrics against those DHS has on file associated with his/her travel document to ensure that the document actually belongs to the person presenting it. US-VISIT provides the results of these checks to decision makers when and where they need them.

The Department's implementation of biometric capabilities has laid the foundation for the rapid expansion of biometric identification to other agencies.

Identity and Screening Services for DHS and Other Agencies

In another effort to streamline DHS processes, the Department has designated US-VISIT's Automated Biometric Identification System (IDENT) as the biometric storage and matching service for the Department, providing biometric identification and analysis services to agencies throughout the immigration and border management, law enforcement, and intelligence communities. This information is collected to aid in determining whether foreign travelers: should be prohibited from entering the United States; can receive, extend, change, or adjust immigration status; have overstayed or otherwise violated their authorized terms of admission; should be apprehended or detained for law enforcement action; or need special protection or attention (e.g., refugees).

IDENT plays an important role in the biometric screening and identity verification of non-U.S. citizens for ICE, CBP, USCIS, and the U.S. Coast Guard. US-VISIT also supports the DOS BioVisa Program and shares information with the Federal Bureau of Investigation (FBI).

Additionally, US-VISIT is working with a number of other DHS components, such as the Transportation Security Administration (TSA), on future and planned credentialing and identity-management programs.

Visa Overstay Process

In addition to enhancing security for visa-free travel, DHS is taking steps to identify individuals who have overstayed their terms of authorized admission.

US-VISIT Overstay Identification and Analysis

The Arrival and Departure Information System (ADIS) database was designed to match biographic data on arrivals, departures, extensions, and changes or adjustments of status to identify individuals who have overstayed the authorized terms of their admission.[1] The system provides an overstay status indicator and seeks to determine nonimmigrant status by assessing whether visitors have remained beyond their authorized terms of admission based on the "admit until" dates on the Arrival/Departure Record (I-94).

Immigration overstays fall into two categories: in-country overstays and out-of-country overstays. In-country overstays are individuals who have exceeded their authorized terms of admission by remaining in the United States. Out-of-country overstays are individuals who, according to the arrival and departure dates, have departed the United States, but who stayed beyond their authorized terms of admission by more than seven days for Visa Waiver Program participants or 180 days for those individuals issued a visa.

In-Country Overstay Summary

Records of individuals whose status indicates a possible in-country overstay are verified and validated by the US-VISIT Data Integrity Group (DIG). The records undergo a series of four automated searches, which historically reduce the number of overstay records by 40-45 percent. The remaining records are then manually verified and validated by DIG analysts to ensure that only credible leads are forwarded to ICE. During the manual DIG verification and validation process, additional government systems are checked. Records that cannot be closed after manual review are transmitted to ICE as in-country overstay leads.

Out-of-Country Overstay Summary

The DIG reviews and validates all out-of-country overstay records that ADIS identifies (regardless of priority or non-priority status). If the overstay is confirmed, the DIG creates both biographic and biometric lookouts in TECS (formerly known as the Treasury Enforcement Communications System) and IDENT for these individuals, which are then available to all TECS and IDENT users, including:

- CBP officers, when an individual attempts to enter at a port of entry;

[1]ADIS receives arrival/departure manifests (APIS), officer-confirmed arrivals (TECS), and changes/extensions/adjustments of status (CLAIMS 3 and SEVIS).

- USCIS, if a person applies for an immigration benefit;
- ICE, if a person is encountered in an immigration enforcement context; and
- DOS consular officers, when an individual applies overseas for a visa to enter the United States.

10-Fingerprint Transition

DHS' transition from collecting two to collecting 10 digital fingerprints at U.S. ports of entry from visitors to the United States is nearly complete. DHS deployed new 10-fingerprint scanners at ports of entry in 2008, and today the new 10-fingerprint scanning devices are in place at all major ports of entry, where international visitors can expect to use the upgraded technology when they enter the United States.

The use of 10-fingerprint readers improves the accuracy of identification; improves interoperability with the FBI, DOS, and local and tribal governments; and reduces the number of travelers referred to CBP secondary inspection. DHS is now able to conduct full searches against the FBI Unsolved Latent File, which allows DHS to match against prints lifted from crime scenes and those collected on battlefields and in safe houses overseas.

Interoperability with the Departments of Justice and State

DHS' 10-fingerprint collection standard makes our system more compatible with the FBI's biometric system, the Integrated Automated Fingerprint Identification System, known as IAFIS. DHS, the Department of Justice (DOJ), and DOS signed a memorandum of understanding regarding interoperability on August 1, 2008. The first-phase capabilities for the initial operational capability were deployed in October 2008.

This integrated system will allow authorized users access to all relevant information in a timely manner so that they can make the right decisions about the individuals they encounter. The interoperability also benefits the FBI and other law enforcement organizations by providing them with increased access to immigration information about high-risk individuals to whom DOS has refused visas and those whom DHS has removed.

Developing Interoperability with the Department of Defense (DOD)

One of the Federal Government's greatest challenges is identifying the unknown terrorist—one who poses a threat but whose name is not known to us or who comes in under a false name. The tried and true method for identifying the unknown terrorist is the fingerprint. A latent fingerprint that is left on an object or in a terrorist training camp or safe house is, in fact, a powerful tool for determining who has been in that place or who has handled that object. The defense and intelligence communities collect these latent fingerprints.

DOD currently sends fingerprints to US-VISIT to be checked against the IDENT biometric watch list of known or suspected terrorists, criminals and immigration violators as well as the other individuals who have come in contact with DHS through immigration and border interactions. One of the results of the transition to 10-fingerprint collection is the increased

likelihood that we will identify the nameless suspect based on his or her immigration or criminal history regardless of the kind of fingerprint DOD finds.

As an example, a person accused of associating with a manufacturer of improvised explosive devices (IEDs) was detained by Coalition Forces in Iraq. The FBI and US-VISIT checked his fingerprints against their data, and US-VISIT fingerprint examiners connected the person detained to a fingerprint DOD had collected from electrical tape inside a piece of an IED. Based on that latent print identification made by US-VISIT, DOD increased the person's security threat level. DHS is now working to make US-VISIT's biometric system compatible with DOD's Automated Biometric Identification System, which will facilitate identification of terror suspects that U.S. forces encounter. Information on these individuals is in our systems in the event they attempt to apply for admission into the United States.

Biometric Exit

Developing an automated exit capability consistent with the recommendations of the 9/11 Commission and Congress has been a priority for the Department since the inception of the US-VISIT program. By adding biometrics to the current biographic-based system of recording departures, DHS will have a more accurate and efficient way to determine whether foreign citizens have departed the United States.

Air

DHS has performed significant planning and testing over the past three years to examine possible solutions for integrating US-VISIT biometric exit requirements into the international air departure process. For more than two years, US-VISIT ran biometric exit pilots at 12 airports and two seaports. These pilots evaluated the use of both automated kiosks and mobile devices in port terminals. When the pilots ended in May 2007, an evaluation determined that the technology worked effectively, but traveler compliance was low. DHS determined that biometric air exit needs to be integrated into the existing international traveler departure process.

On April 24, 2008, DHS published a notice of proposed rulemaking (NPRM) proposing that commercial air carriers and vessel carriers collect and transmit the biometric information of international visitors to DHS within 24 hours of their departure from the United States. Before finalizing the Air-Sea Exit NPRM, Congress, in the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (Public Law 110-329), required us to test additional biometric collection to ensure that the best available procedures are implemented.

From May 28 to July 2, 2009, US-VISIT tested biometric air exit procedures at two airports: Detroit Metropolitan Wayne County Airport and Hartsfield-Jackson Atlanta International Airport. In Detroit, DHS tested the collection of passengers' biometrics at the boarding gate by CBP officers. In Atlanta, DHS tested the collection of passengers' biometrics at TSA checkpoints. The Department has submitted to the Committees on Appropriations of the Senate and the House of Representatives, as well as to the Government Accountability Office, an evaluation report of these pilots, consistent with Public Law 110-329. The results of the pilot

evaluation, combined with the review of public comments submitted in response to the NPRM, will inform the decision on the option to be selected for publication in the final rule.

Land

Biometrically recording the departures of non-U.S. citizens at U.S. land border ports of entry poses significantly greater challenges. Each year, our land border ports of entry see more than 300 million crossings at 170 port locations, including seasonal and other ports that are not open year round. Due to variations in infrastructure, environment, and traffic volume from port to port, a one-size-fits-all solution will be difficult. The Department is examining options for the land border environment that will not negatively impact the economy, the environment, or traveler safety.

International Cooperation and Collaboration

When DHS began the US-VISIT program to collect biometrics as part of port-of-entry inspection and screening, the world watched to see if the benefits of biometrics would work on a large scale. Although a handful of nations were testing biometrics, DHS was the first to launch a comprehensive, biometrically based identity-management system for immigration and border management, and we now serve as a model for countries developing similar systems.

Some countries have already begun operations or are nearing deployment. For example:

- Japan has implemented a two-fingerprint biometric entry system similar to US-VISIT's initial system;
- The United Kingdom is collecting 10 fingerprints from visa applicants and testing fingerprint collection at ports of entry;
- The European Union is building a 10-fingerprint visa-issuance program based on the very successful Eurodac;
- Australia, which has been a pioneer in facial recognition, is advancing its identity-management program;
- The United Arab Emirates has long been using iris scans as part of its immigration and border control processes; and
- Other countries, including Peru, Mexico, and Canada, are actively pursuing biometrics implementation.

As the use of biometrics increases worldwide, consistent international standards for biometrics and data sharing are essential to developing compatible systems, and compatible systems are essential to hindering international criminal enterprises as well as terrorists' ability to travel.

The Future of Biometric Screening

Biometric screening offers real opportunities to dramatically increase the efficiency of identifying people. The Department is already researching emerging technologies to expand our screening and identification capabilities, and we recognize that future systems will require increased assurance, efficiency, ease of use, and flexibility.

As DHS further evaluates biometric exit procedures, both at airports and land border ports of entry, we are looking for more efficient, less invasive technologies to verify visitors' departures. Particularly at the land border, we seek technologies that might meet our needs better than requiring visitors to have their fingerprints scanned while driving through a port of entry.

In some cases, the key to expanding biometric screening is to bring the technology to remote locations where decision makers need it. CBP's Air and Marine Operations is examining opportunities to use mobile biometrics in its areas of operation. The Coast Guard is using mobile biometric collection and analysis capabilities off the coasts of Puerto Rico and Florida, in coordination with US-VISIT. This has helped the Coast Guard identify and refer for prosecution and/or administrative immigration proceedings hundreds of repeat illegal migrants who are ineligible to enter the United States, including some wanted for human smuggling or murder.

Success Stories

Our many success stories include stopping more than 8,000 criminals or immigration violators at the ports of entry based on biometrics alone, and identifying thousands who are ineligible to receive visas to travel to the United States. No doubt, we have deterred countless more.

DHS' use of biometrics is helping disable the use of fraudulent or altered travel documents. For example:

- On March 16, 2008, a subject arrived at John F. Kennedy International Airport in New York and applied for admission with a valid Turkish passport and an unexpired B1/B2 visitor visa. He was referred to secondary inspection as a match to the IDENT biometric watch list for a previous voluntary departure. Secondary inspection revealed that on November 10, 2003, the subject had been apprehended taking pictures of the Ft. Leonard Wood Missouri Military Base. While in custody, it was discovered then that he had overstayed his authorized period of admission in the United States. The subject was now attempting to enter the United States using the identity of his twin brother and his brother's travel documents. The subject was denied access and is inadmissible to the United States for willful misrepresentation and not being in possession of valid travel documents.

- Biometrics is also helping at our borders away from ports of entry. In December 2007, the Coast Guard interdicted 10 migrants attempting to enter Puerto Rico illegally by sea. A check of the migrants' biometrics against IDENT revealed that two of the migrants had illegally entered the United States before, had been subsequently removed from the United States, and were suspected of being part of a human trafficking organization. The two suspected traffickers were brought ashore for referral for prosecution along with two witnesses who would testify against them. Since the adoption of the Biometrics at Sea System (BASS) in 2006, the Coast Guard has seen an 80 percent reduction in the number of migrants trafficking through the Mona Pass. The Coast Guard has collected over 2,500 biometrics signatures to date, with over 25 percent of those signatures returning a positive match, or "hit", resulting in over 250 successful prosecutions.

US-VISIT and Privacy

DHS is committed to adhering to the strictest privacy standards. DHS collects only the information needed to achieve program objectives and missions and restricts the use of this information to the purpose for which it was collected. DHS also conducts periodic audits of its systems to ensure appropriate use within the framework of the Privacy Act.

Ultimately, the success of the US-VISIT program will be measured not only by our ability to identify those who may present a threat, but also by our ability to protect against identity theft and fraud. We are acutely aware that our success depends on how well we are able to protect the privacy of those whose biometrics we hold. We have a dedicated privacy officer responsible for ensuring compliance with privacy laws and procedures and for creating a culture of privacy protection within US-VISIT. It bears mention that our policy also extends most of the same privacy protections afforded to U.S. citizens to non-U.S. citizens as well. From the beginning, we have emphasized that the information gathered by DHS or DOS will be used only for the purposes for which it was collected, consistent with those uses authorized or mandated by law. We regularly publish privacy impact assessments and system of records notices to provide the public with a clear view of the information we collect, how we store it, and our policies to ensure it is not abused.

Conclusion

Biometrics has increased our Nation's security and the security of nations around the world to a level that simply could not exist before. Biometrics affords us greater efficiencies and makes travel more convenient, predictable, and secure for legitimate travelers. Biometrics enables people to have greater confidence that their identities are protected, and in turn, decision makers are more certain that the people they encounter are who they say they are.

To ensure we can shut down terrorist plans before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Biometrics provides a new way to bring terrorists' true identities to light, stripping them of their greatest advantage: anonymity.

So what is next?

We must aggressively pursue innovation. Those who want to do harm continue to search for ways to exploit our weaknesses, so we cannot afford to lag behind. We too must search for even more efficient and affordable identification technologies.

We also need to continue to advocate abroad. With the power of biometrics and a foundation of international cooperation, we can transform and enhance the way people travel the world and the way countries protect themselves from those who would do them harm.

The Department's use of biometrics plays a crucial role in supporting many programs and initiatives within DHS and other Federal agencies. Chairman Lieberman, Ranking Member Collins, and distinguished Members, we have outlined our current efforts that, with your assistance, will help DHS continue to protect our Nation.

Thank you again for this opportunity to testify. I will be happy to answer any of your questions.

DEPARTMENT OF STATE

STATEMENT
OF
AMBASSADOR JANICE L. JACOBS

ASSISTANT SECRETARY OF STATE FOR CONSULAR AFFAIRS,
BUREAU OF CONSULAR AFFAIRS,
DEPARTMENT OF STATE

BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS

HEARING
ON
FIVE YEARS AFTER THE INTELLIGENCE REFORM AND
TERRORISM ACT: STOPPING TERRORIST TRAVEL

DECEMBER 9, 2009

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, it is a distinct honor to appear before you today. I would like to express my sincere appreciation for the opportunity to share with you many of the accomplishments of my colleagues in the Bureau of Consular Affairs (CA) in our continuing efforts to strengthen the security of U.S. borders through the vigilant adjudication of U.S. passports and visas while maintaining America's traditional openness to legitimate travelers.

Introduction

Defending security at the borders of the United States starts with consular officers overseas. CA's visa adjudication function and prevention of fraudulent use of U.S. travel documents are one of our first lines of defense against terrorists and others who would do us harm. U.S. visas and passports are some of the most coveted travel documents in the world. We place the utmost importance on the integrity of our visa and passport issuance processes to ensure that only those who meet the eligibility requirements for U.S. travel documents receive them. Our close and fruitful cooperation with our closest partner agencies – the Department of Homeland Security (DHS) and the Justice Department's FBI – supports and strengthens these missions.

Executive Summary

The following is a summary of the technological, procedural, data-sharing, interagency cooperation, training and other enhancements CA has implemented since September 11, 2001 and the enactment of the Intelligence Reform and Terrorism Act. If we were to take a snapshot of our consular activities in August of 2001 and compare it with a snapshot of our operations today, you would see dramatic improvements. In 2001, the Consular Lookout and Support System (CLASS), the database the Department uses to check visa and passport applicants for derogatory information, contained approximately seven million visa records and 2.2 million passport records. At that time CLASS connectivity with Washington could be lost for extended periods, and officers would be forced to use a back-up system – a CD-ROM replica of the database that could have been a month old. In 2001, consular officers depended largely on information provided by the visa applicants to determine their identities. If a visa applicant turned out to be a possible match for a terrorism-related CLASS record, the consular officer requested a Security Advisory Opinion (SAO) from the Visa Office in Washington. Such requests were sent via cables, as were the Department's responses. This multi-step cable process to communicate with posts and to coordinate with other government agencies resulted in long wait times for both the consular officers and the applicants.

Since September 11, 2001, we have revamped our procedures and introduced new technology that makes adjudicating visa and passport applications both more efficient and effective. Barriers to the exchange of information have come down throughout the U.S. government (USG). The CLASS database has grown more than more than 400 percent, to 26 million records, and grown more robust. Improvement in real time connectivity has put an end to CD-ROM back-up systems. This increase in the quantity and quality of CLASS records is largely the result of improved data sharing between the Department of State and the law enforcement and intelligence communities. In 2001, only 25 percent of records in CLASS came from other government agencies. Now, almost 70 percent of CLASS records come from other agencies. The use of biometrics has become standard in the visa process. Using fingerprints and facial recognition technology, we can fix identities through biometric enrollment and biometrically match applicants to derogatory information.

One of the most far-reaching technological improvements in visa operations was the development of the Consular Consolidated Database (CCD). The CCD is a powerful, integrated tool that allows Foreign Service posts, the Department, and our partner agencies and offices to view information about visa applicants. To the extent such access is permitted under confidentiality provisions of the Immigration

and Nationality Act, such information includes photographs, facial recognition check results, comments made by interviewing officers, CLASS namechecks, DHS's Automated Biometric Identification System (IDENT) and FBI's Integrated Automated Fingerprint Identification System (IAFIS) results, and supporting documents. At present, the CCD has more users from other government agencies than from our Department.

The SAO process, by which select visa applicants are screened and cleared by other government agencies prior to visa issuance, has undergone major enhancements. We have done away with cable communications for SAO requests and established direct electronic connectivity between overseas consular posts and Washington agencies. This connectivity allows the government agencies responding to SAO inquires to use the same visa systems that posts use overseas. This direct linkage between the Department and our partner agencies facilitated the Visa Office's processing of nearly two million SAO requests since September 11, 2001. Since that date, we and our partner agencies have engaged in a nearly constant round of SAO process refinements and resource allocations. One result of our dedication to this effort is that, at this time, we have the shortest SAO turnaround times since September 11, 2001 – maintaining the security of our borders while reducing the impact on legitimate travelers.

The wide range of technologies now available to assist consular officers in gathering, organizing and sharing information relevant to visa applications is paralleled by advances in consular training. New consular officers benefit from an increased focus on the security-related aspects of visa adjudication. A continuum of courses covering fraud prevention, interviewing, namechecking, management, and more are offered at the Foreign Service Institute (FSI) in Arlington, Virginia, as well as online training resources available at posts. FSI continuously works with offices throughout the government to develop new training opportunities that meet the challenges of the changing world in which consular officers operate.

Visa and Passport Processing Today

Technology and the Visa Process

The Department of State constantly refines and updates the technology that supports the adjudication and production of U.S. visas. There are many examples of how enhancing the security of the document directly improves the security of U.S. borders. Under the Biometric Visa Program, before a visa is issued, the visa applicant's fingerprints are screened against IDENT, which contains all available fingerprints of terrorists, wanted persons, and immigration law violators, and against IAFIS, which contains more than 50 million criminal history records. The

Biometric Visa Program partners with the DHS US-VISIT Program to enable Customs and Border Protection (CBP) officers at ports of entry to match the fingerprints of persons entering the United States with the fingerprints that were taken during visa interviews at overseas post and transmitted electronically to DHS IDENT. This biometric identity verification at ports of entry ensures the security of the U.S. visa by essentially eliminating the possibility of visa fraud through counterfeit or photo-substituted visas, or through the use of valid visas by imposters.

In 2007, we transitioned from capturing two fingerprints at the time of visa adjudication to taking all ten prints. In FY 2009, fingerprints of more than 6.7 million visa applicants were screened against IDENT and IAFIS databases. From IAFIS, more than 49,000 criminal arrest records were sent to posts. More than 10,000 watch list hits are returned to posts every month from IDENT.

We also use facial recognition technology to screen visa applicants against a watch list of photos of known and suspected terrorists obtained from the FBI's Terrorist Screening Center (TSC), as well as against the entire cache of visa applicant photos contained in our CCD. Facial recognition screening has proven to be another effective way to combat identify fraud.

Today, every visa applicant undergoes extensive security checks before a visa can be issued. The CLASS namecheck system, which is updated daily, includes information from the Department of State, FBI, DHS, and intelligence from other agencies. Also included in CLASS is derogatory information regarding known or suspected terrorists (KSTs) from the Terrorist Screening Database, which is maintained by the TSC and contains the names of terrorists nominated by all USG sources. Possible matches are reviewed by USG agencies in Washington, D.C., prior to any visa being issued. Under a complementary program, new name entries in the Terrorist Screening Database are checked against records of previously issued valid visas, enabling us to revoke visas issued to KSTs. Since September 11, 2001, we have revoked more than 1,700 visas of individuals about whom, subsequent to visa issuance, we received information that potentially connected the visa holder to terrorism.

In October 2008, the Department of State took over responsibility for producing the Border Crossing Card (BCC) used as a visa by Mexican nationals to cross the southern border. The Department of State extensively redesigned the BCC, and made it compatible with the radio frequency (RFID) technology used by CBP at land ports of entry. The RFID chip on the card contains a number that allows the CBP system to access the card issuance data forwarded by the Department of State

to a secure DHS database. The card issuance data, including the bearer's photo, appears on the computer screen of the CBP officer when a vehicle arrives at the primary inspection booth. This new BCC facilitates both the inspection process for the CBP officers and the entry process for qualified Mexican nationals entering the United States.

Another major technological advance is the Consular Electronic Application Center – a new electronic platform where applicants submit visa applications and photos via the Internet, eliminating paperwork, decreasing visa application and adjudication times, and reducing to one the number of forms applicants must complete. This new online system, now being deployed overseas, will provide consular and fraud officers the opportunity to analyze data in advance of the interview, enhancing their ability to make decisions. The online form offers foreign language support, but applicants will be required to answer in English, to facilitate information sharing between the Department of State offices and other government agencies. The new application forms are "smart," meaning that subsequent questions are triggered by an applicant's answers to earlier questions. The system will not accept applications if the security-related questions have not been fully answered and "irregular" answers are flagged to ensure that officers make note of them.

The Consular Visa Interview

One of the most significant changes in consular practice after September 11, 2001, was a re-emphasis on the personal interview. Requirements for in-person interviews of visa applicants were codified in the Intelligence Reform and Terrorism Prevention Act. The interview is an opportunity for consular officers to assess the credibility of the applicant and the applicant's travel plans. Consular officers are trained in interview techniques, foreign languages, and cultural awareness skills they leverage during visa interviews. Because misrepresentation or fraud can be present in a variety of forms, such as false documents, fictitious relationships and identities, and mutilated fingerprints, CA employs a layered approach to secure the integrity of the visa adjudication process. We have put in place an array of measures, including analytic interviewing techniques, biometric checks, database checks, and document verification. This layered approach poses a significant obstacle and deterrent to foreign persons seeking entry to the United States to do us harm.

Fraud Prevention Techniques

We have a variety of tools available, in addition to the consular interview, to separate fact from fiction in visa applications. Since 2001, we have increased the

number of staff dedicated to the prevention of consular fraud. Consular fraud prevention personnel posted domestically and abroad have developed robust networks and mechanisms to verify information presented in visa applications. We employ increasingly sophisticated tools to detect links between different fraudulent cases and analyze fraud trends.

CA will also soon deploy a global system called the Consular Case Management Service (CCMS) for tracking and conducting consular fraud investigations. This system, among other things, will improve consular officers' ability to easily and effectively share information on suspect cases. We expect to release the first phase of the system, which will support the full spectrum of visa fraud cases, to posts worldwide in early 2010. Future deployments will add the capability to manage passport fraud cases – both overseas and domestically. We believe CCMS will greatly enhance our ability to track and analyze global fraud trends.

Inter-departmental Cooperation

Our principal goals in visa adjudication are to facilitate travel that is legitimate and prevent travel that is not. Often, however, we run across cases involving organized crime or fraud that may be prosecutable in the United States or under local law. In such instances we turn immediately to our law enforcement colleagues in the

Bureau of Diplomatic Security (DS). CA and DS coordinate very closely. Many DS agents go through the Basic Consular Course, the same one all consular officers take as part of their initial training, and may be assigned as overseas criminal investigators based in consular sections abroad. In many cases, based on DS's excellent liaison relationships with local police, a perpetrator of fraud not only is denied a visa, but is then placed under arrest at the front gate on departing the embassy. In some cases, information gathered as a result of these investigations overseas is also used to disrupt and prosecute sophisticated document fraud operations in the United States. This coordination with DS is a very powerful factor in deterring terrorists' attempts to secure visas, as well as deterring other kinds of fraud.

CA and DS have established a jointly-staffed Consular Integrity Division (CID) within CA's Office of Fraud Prevention Programs. The CID is responsible for strengthening internal controls throughout CA and investigating cases of internal corruption or malfeasance, for which we adhere strictly to a policy of zero tolerance.

In July 2007, a Government Accountability Office (GAO) Report on border security recommended developing close coordination and liaison among

counterfeit deterrent specialists within DHS and other Federal agencies. CA continues to develop this capacity, including the creation this year of the Forensic Document Design and Integrity Coordination function. This coordinating mechanism draws together a team of professionals from all areas of CA who are committed to "state of the art" counterfeit document deterrence. Their recommendations have already brought about improvements in security documents.

Visa Waiver Program

Not everyone requires a visa to travel to the United States. We have worked closely with DHS to increase the security of the Visa Waiver Program (VWP). Together with DHS's Visa Waiver Program Office, we are engaging VWP member countries to help them meet the enhanced security requirements contained in the *Implementing Recommendations of the 9/11 Commission Act of 2007 (the 9/11 Act).* CA also worked closely with DHS's CBP on the creation of the Electronic System for Travel Authorization (ESTA) and continues to assist in its implementation. In fact, ESTA provides a lookout to our CLASS system for every ESTA authorization DHS denies, thereby informing consular officers when a visa applicant had previously attempted to obtain an ESTA approval. ESTA also uses visa refusal records from CA to check applications against.

Technology and the Passport Process

Recognizing that the U.S. passport is one of the most sought-after travel documents in the world, CA has committed itself to issuing passport documents that include advanced technological features to foil the efforts of counterfeiters. We are also doing everything in our power to ensure that passports are issued only to U.S. citizens who are eligible to receive them.

In August 2006, the Department of State began issuing the ePassport, the first U.S. passport to contain a contactless chip that stores the bearer's photograph and biographical data. The data is secured through the use of public key cryptography and digital signatures. This is a transformational step forward in document security. Unlike paper passports, where a photo could be potentially substituted or the biographic data overwritten, the information on the chip, once locked by the key, cannot be changed. There are more than 45 million U.S. ePassports in use.

In July 2008, to address one of the key objectives of the Western Hemisphere Travel Initiative, we began issuing a passport card. The passport card is a driver's license-sized card that contains a contactless chip. No personal information is contained in the chip – only a unique number that, once read, points to the bearer's

information in secure DHS databases. The passport card uses state-of-the-art security features to prevent counterfeiting and forgery.

As important as the security of documents themselves is the integrity of the passport adjudication process, including the electronic databases used to screen passport applicants and verify their citizenship and identity. All valid U.S. passports are supported by the Passport Information Electronic Records System (PIERS), a database of more than 214 million passport records, including photos, applications, and history. PIERS is available to consular officers and passport adjudicators worldwide to verify the identity and citizenship of those to whom U.S. passports have previously been issued. We have granted access to PIERS data to several components of DHS, law enforcement and intelligence agencies to aid in successfully protecting our borders. With each of these agencies, we also have agreements in place to ensure that the proper training, monitoring, and reporting procedures are in place to safeguard the personally identifiable information of every passport applicant.

The Consular Lost and Stolen Passports (CLASP) database includes more than eight million records concerning U.S. passports. CLASP data is shared with DHS and other domestic law enforcement and intelligence agencies as well as with

international organizations such as Interpol. In addition, the Department of State maintains 24/7 operations to help foreign authorities check on U.S. passport validity and authenticity, using the CLASP database.

All domestic passport applications are checked against CLASP, PIERS, the Social Security Administration's (SSA) database, and CLASS, which includes, among other data, information provided by the Department of Health and Human Services and federal, state, and local law enforcement agencies. CA is holding discussions with SSA to obtain real-time access to their data to conduct verifications.

Recent evaluations of our passport adjudication process by the GAO and the Department of State's Office of the Inspector General identified areas of vulnerability. In response, we have greatly enhanced our fraud-prevention efforts over the past year. In coordination with DS, we launched a program that consists of unannounced testing of the processes and procedures for passport acceptance and adjudication in much the same manner used by the GAO. The program is an ongoing effort to test systematically for potential individual and systematic vulnerabilities. Each test scenario will be followed by on-site training for employees of the affected passport agency and/or acceptance facility, and immediate reporting to CA of any deficiencies in our systems or procedures. We

expect to correlate lessons learned, facilitate debriefing and training to employees and management, provide constructive suggestions on systematic improvements to mitigate these vulnerabilities, and strengthen management controls.

We have also reached out to interagency law enforcement and state government partners to enhance our ability to detect fraudulent documents such as birth certificates and driver's licenses submitted to support citizenship and identity in passport applications.

Data Sharing

Distinguished Members of the Committee, cooperation with partner USG agencies and departments is the critical foundation of our mission. In accordance with both the Department of State's own objectives of detecting and stopping would-be terrorists and the provisions of the Enhanced Border Security and Visa Entry Reform Act of 2002, we have taken significant steps to increase the quantity and efficiency of data sharing between the Department of State and the law enforcement and intelligence communities.

In one recent month, more than 12,000 employees at other agencies and entities including DHS, the FBI, the Department of Defense, TSC, the National

Counterterrorism Center, and the Department of Commerce submitted 900,000 queries on visa records to the CCD, which, as noted previously, includes information such as photos of visa applicants, consular officer notes on visa cases, and relevant documents scanned into the database. CA also has data sharing agreements with these same agencies to access passport records for known or suspected persons of interest.

Visa applicant data, including photographs, is replicated within minutes from posts worldwide to the CCD, which relays it to the DHS TECS computer system for use by CBP officers at ports of entry. This rapid visa data sharing allows visa records, including photos, to be displayed on CBP officers' computer screens as travelers present their visas at ports of entry. Department of State also provides U.S. passport issuance data, including photographs, to the DHS TECS computer system for use by CBP officers to verify U.S. passports the same way they verify visas. Certain DHS officers can also access passport data in PIERS, ensuring the ability to verify U.S. citizen identities at ports of entry.

We increasingly rely on data from our partners to enhance our ability to make the right decisions when adjudicating visa and passport applications. A valuable tool to which we have recently been granted access is DHS's Arrival Departure

Information System (ADIS). ADIS tracks foreign nationals' entries into and most exits out of the United States. The tool has uncovered previously undetected cases of illegal overstays in the United States that render foreign nationals ineligible for visas. ADIS is currently available to a limited number of consular officers, but DHS and CA are working together to make entry-exit data broadly available to all interviewing consular officers by March 2010.

CA and DHS are also working to provide consular officers access to several other DHS systems, especially those that U.S. Citizenship and Immigration Services (USCIS) use to adjudicate immigration and naturalization benefits within the United States. We are also pursuing access to various other DHS databases that would assist us in pre-screening visa applicants before they appear for their interviews.

The State Department and the TSC have also concluded formal agreements or arrangements with 17 foreign partners for the reciprocal exchange of terrorism screening information, which enhance our existing channels of information sharing about known and suspected terrorists. Thirteen of these countries are Visa Waiver Program countries. We continue to work with the TSC to expand these bilateral cooperative arrangements.

As I mentioned, we already have a data sharing relationship with the SSA that allows us to check passport applications against their databases to ensure that passport applicants are not using the identities of deceased U.S. citizens. We have an agreement in place with the National Association for Public Health Statistics and Information Systems to facilitate verification of birth certificates presented in support of passport applications. The association has provided us with access to the Electronic Verification of Vital Events (EVVE) system, which allows CA to verify vital records' data from 17 states. All 50 states are expected to participate in EVVE by 2011. This tool is currently available to our fraud prevention offices and we are looking to expand its use to passport adjudicators in the near future.

DS recently helped CA obtain access to driver's license data from the National Law Enforcement Telecommunications System, Inc. Access to such data helps us verify driver's licenses submitted in support of passport applications. CA fraud prevention managers now can access state driver's license data from 48 states, Puerto Rico, and the District of Columbia. We continue to work to obtain access to the remaining two states and territories. We will expand the use of this tool by all passport adjudicators in the near future, which also satisfies previous GAO recommendations. Some states have been hesitant to share their data because CA

lacks status as a law enforcement entity for data sharing purposes. We are discussing possible legislation with the Subcommittee on Terrorism, Technology, and Homeland Security of the Senate Judiciary Committee that will grant CA access to law enforcement data for verification purposes.

In addition to the programs above, CA representatives meet regularly with representatives of the intelligence and law enforcement communities to develop strategies to utilize the newest technology and enhance the timely and effective sharing of information. CA also works with DHS Immigration and Customs Enforcement (ICE) Visa Security Unit (VSU) officers who are assigned overseas pursuant to Section 428 of the Homeland Security Act of 2002. VSUs are required by law to review 100 percent of visa applications in Saudi Arabia. ICE/VSUs have also been established at Foreign Service posts in several other countries. CA is working cooperatively with ICE as it considers adding VSUs at additional posts.

Consular Training

Mr. Chairman and distinguished Members, you know that those who wish to do us harm are constantly searching for our weaknesses and vulnerabilities. Therefore, we must ensure that our greatest front-line resource – our consular officers and passport specialists –develops the best skills possible in identifying and uncovering

new fraudulent schemes to obtain U.S. travel documents. Section 7201 (d)(3)(B)(ii) of the Intelligence Reform Act mandates that the Department of State report our efforts to enhance, via training, consular officers' ability to effectively detect and disrupt terrorist travel to the United States. As noted in Congressional findings under Section 7201(a), travel documents are as important to terrorists as weapons. The Department of State is committed to providing the highest level of training to our consular officers, who occupy the key point of control over the issuance of documents valid for travel to the United States.

Presently, there are more than 1,500 consular officer positions in the Foreign Service. Those positions are filled from a larger, mobile, Foreign Service officer workforce, any member of which may at any given time fill a consular or a non-consular position. All officers in consular positions may inspect or review travel or identity documents as part of their official duties. Every single one of those officers is required to have completed the Basic Consular Course prior to performing duties as a consular officer. In addition, whenever an officer returns to consular work after a gap of five years or more, that officer is required to repeat the entire 31-day course.

In fiscal years 2003-2008, more than 500 officers graduated from the Basic Consular Course annually. FY 2009 saw that number grow to 698 as demand and course offerings increased to meet the hiring surge of new Foreign Service and Civil Service personnel. In addition to consular personnel, 59 DS Special Agents completed the Basic Consular Course in FY 2009 in preparation to conduct visa and passport fraud field investigations. Twenty-two agents work in consular sections at overseas posts while the others fill domestic investigative jobs. The Department believes that the Basic Consular Course does an excellent job in addressing the topics mandated under Section 7201(d)(2). The course was lengthened and improved substantially during the past six years, and we are continually reviewing it for further enhancements.

The majority of consular training is offered by FSI. The Basic Consular Course includes modules on the following core consular subjects: Passport and Nationality, Immigrant Visas, Nonimmigrant Visas, American Citizen Services, SAFE (Security, Accountability, Fraud, and Ethics), Interviewing, and Consular Management. The methodology of the course mixes lectures, case studies, practice interviews, hands-on practice with computer applications (including biometric tools), group exercises, graded written examinations, and interagency contact

(including briefings from the CIA and observation of DHS passenger inspection operations at Dulles International Airport).

As noted earlier, the Department of State is scanning fingerprints that are checked against the DHS IDENT watch list and US-VISIT databases, and the FBI's fingerprint based criminal history record information administered by the Criminal Justice Information Services Division. At GAO's recommendation, the Department also uses advanced facial recognition technology to screen all immigrant and nonimmigrant visa applicants. To prepare consular officers to use these tools properly and effectively, the Basic Consular Course incorporates extensive hands-on computer training sessions (including the use of the most up-to-date, 10-print biometrics collection technology), integrated throughout the course. In addition to the curriculum material described above, all students in the Basic Consular Course receive personal copies of the 9/11 Commission Report, the 9/11 Commission's Staff Report on Terrorist Travel and the National Strategy to Combat Terrorist Travel.

Additional training courses keep consular officers' skills current and enhance their ability to detect, intercept, and disrupt terrorist travel. The fraud prevention manager course is a one-week course aimed primarily at mid-level consular

officers who are or will be serving as fraud prevention managers in consular sections abroad. One hundred thirty-four officers, including two officers from USCIS's Fraud Detection Laboratory, received the training during FY 2009. We welcome more interagency participation in consular courses.

At the same time that this course was expanded, the content was revised to include new material on the current terrorist threat, briefings by DHS and CA fraud prevention personnel, and other valuable new content, in addition to core skills such as detecting counterfeit documents and consular interviewing. The hands-on anti-fraud technologies curriculum, originally created in 2006, is continually being revised and updated to teach fraud prevention managers how to use Lexis-Nexis, Dun and Bradstreet, and other on-line resources as well as the new anti-fraud tools connected to the CCD.

To date, 1,382 officers and passport adjudicators have successfully completed the mid-level Advanced Consular Namechecking course. The course incorporates new material on biometric technology and use of databases to screen applicants and verify identity. In 2008, we developed a version of the course for use by adjudicators at our domestic passport agencies.

A course for mid-level consular officers on consular interviewing was expanded in October 2007 to include content analysis techniques that can be used during interviews and to assess written statements for use in the overseas and domestic adjudication context. To date, 986 consular officers and passport agency adjudicators have completed the consular interviewing course.

For those officers unable to come to Washington for training, FSI is using distance learning tools to present material on consular fraud prevention and countering terrorist travel. These distance learning tools supplement the Basic Consular Course and subsequent mid-level consular training courses, allowing consular officers to review and refresh their earlier training.

In October 2005, FSI released guidance and a set of specific training modules designed to facilitate orientation and on-the-job training for consular officers newly arrived at their posts of assignment. These modules are designed to identify key topics, but rely on briefers at posts to impart post-specific procedural and other information, much of which is relevant to countering terrorist travel. In August 2009, FSI established a SharePoint website with examples of post-specific training programs and standard operating procedures. This resource is available to all

overseas consular posts and domestic CA officers, and is designed to encourage the sharing and spread of good training practices and procedures.

CA has expanded the National Training Program (NTP), a two-week comprehensive adjudication course that is required for all newly-hired passport specialists. In addition to basic adjudication skills, the NTP includes fraud training and covers topics such as detecting counterfeit documents, identity evidence, analysis of fraud indicators, and fraud resources and referrals. We have also revised the standardized fraud training for passport acceptance agents which now emphasizes identifying an applicant and verifying their identity. We developed a Reference Guide to Counterfeit Documents which provides a quick reference for reviewing a document, understanding its creation, and recognizing the differences between genuine and counterfeit documents.

CA is developing monthly standardized fraud training for passport specialists at each domestic agency and center. The training will include modules on Facial Recognition and Detecting Look-alike Impostors, Foreign Handwriting Detection, Significant Fraud Indicators on Passport Applications, and Delayed Birth Certificate Fraud.

In summary, the Department of State is committed to safeguarding the United States via proper adjudication of visas and U.S. passports. We believe that we have made significant improvements since the attacks of September 11, 2001, but we are constantly looking for ways to do better. As we strive to push our borders outward and seek to interdict terrorists before they ever reach our ports of entry, we have not overlooked the importance of facilitating the travel of legitimate visitors. Advances in technology, data sharing, interagency cooperation, and training, all contribute to a more robust process for screening visa applicants. We have leveraged these same advances to increase the efficiency of the process in order to meet the needs for legitimate travel. We do not view border security and facilitation of travel as goals in opposition. We believe the record of the past seven years shows that we can make advances in both spheres, and we are dedicated to implementing the best possible solutions to further these goals.

Thank you again for the opportunity to be here. I appreciate the Committee's continued interest in our work and have enjoyed the chance to share some of the many accomplishments we have had over the past several years. I am pleased to take your questions.

VerDate Nov 24 2008 12:33 Apr 29, 2011 Jkt 056149 PO 00000 Frm 00082 Fmt 6601 Sfmt 6601 P:\DOCS\56149.TXT SAFFAIRS PsN: PAT

WRITTEN TESTIMONY OF DAVID HEYMAN
ASSISTANT SECRETARY OF POLICY
THE DEPARTMENT OF HOMELAND SECURITY
BEFORE
THE SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
ON
TERRORIST TRAVEL
12/09/09

Introduction

Chairman Lieberman, Senator Collins and other distinguished Members, thank you for the opportunity to appear before the Committee to highlight the Department of Homeland Security's (DHS) work in the area of preventing and countering terrorist travel. This is an issue of singular importance, and I commend the Committee for holding this hearing.

The U.S. Government employs a number of tools to counter terrorism, including collaborating with foreign partners, cutting off terrorist financial resources, enforcing export controls to prevent terrorists' access to sensitive technology and weapons, intercepting terrorist communications, targeting terrorist leadership, and countering efforts at recruitment, among others. But, to paraphrase the 9/11 Commission, targeting terrorist travel is perhaps one of the most powerful weapons we have to counter the ability of terrorists to attack us.

Those who seek to attack us rely on access to travel networks. Terrorists travel in order to identify and engage in surveillance of potential targets, to plan their attacks, to train on tactics and operations, to collect funds and documents, and to communicate with other operatives.

Every step along this pathway presents a vulnerability to would-be attackers, who must come out of the shadows and interact with the traveling public and our officers at ports of entry. At some point along the travel pathway, for example, many terrorists cross international borders—to communicate and engage others, train, or receive resources—a step which necessitates submitting advance passenger manifest information, using a passport and going though checkpoints managed by the Transportation Security Administration (TSA) and Customs and Border Protection (CBP). This type of interaction presents not only a moment of engagement where our adversaries must make themselves known, but also an opportunity for interdiction and observation. Consequently, terrorists devote extensive resources to acquiring and manipulating passports, entry and exit stamps, and visas to avoid detection.

What we have learned over the past few years is that border security and preventing terrorist travel is more than drawing a line in the sand where we can deny entry into a country. Rather, the exercise of authorities associated with border security can be a powerful resource to identify and thwart terrorist operations at the earliest opportunity.

We work and live in a seamless economic environment connected by global systems and networks that transcend national boundaries. As much as these global systems and networks are critical to the United States and our prosperity, they are also vital conduits by which our

adversaries, terrorists, and criminals conduct their illicit activities. As such, we have a strong interest, obligation, and opportunity to prevent these networks from being exploited for terrorist purposes. By constraining terrorist travel, we limit the ability of our adversaries to operate. Our aim must be to identify and disrupt terrorist travel at the earliest point.

The Department of Homeland Security was created for and is uniquely positioned to accomplish these goals:

- Customs and Border Protection's twin goals remain border security and the facilitation of legitimate trade and travel. CBP – among other activities – detects and prevents the illegal entry of people and smuggling of contraband into the United States (including a vigilant watch for terrorist threats); protects our agricultural and economic interests from harmful pests and diseases; protects American businesses from theft of their intellectual property; enforces violations of textile agreements; collects import duties; and enforces United States trade laws.
- Immigration and Customs Enforcement's (ICE) mission is to protect the security of the American people and homeland by enforcing the nation's immigration and customs laws. As the nation's second largest investigative law enforcement agency, and the one responsible for the vast majority of federal arrests of non-U.S. persons, ICE plays a central role in targeting, investigating, and dismantling transnational criminal operations through long-term, intelligence-driven investigations.
- The Transportation Security Administration protects United States transportation systems, including air transportation, to ensure freedom of movement for people and commerce.
- U.S. Coast Guard's mission is to protect the United States from maritime intrusions and threats, and to ensure the safety and mobility of maritime traffic.
- The mission of the DHS Office of Intelligence & Analysis (I&A) is to collect, analyze, produce, and disseminate information, intelligence and counterintelligence to support national and departmental missions.
- The mission of United States Citizenship and Immigration Services (USCIS) is to administer the immigration benefits system. USCIS touches 12 million applications yearly and every application is subject to rigorous screening processes to ensure benefits are not afforded to those who present a threat to our national security.

Taken together, this expertise and these authorities have made DHS not only essential to preventing terrorist travel to the United States, but increasingly in preventing terrorist travel around the globe. Today I will discuss three areas in which the Department plays a central role in disrupting and denying terrorist travel: (1) identification of known and suspected terrorists as well as other individuals who pose a threat to national security; (2) screening of travelers and those seeking immigration benefits to deny travel prior to departure, target for additional inspection, prevent entry at arrival, and/or prevent an individual from remaining in the U.S. if they are not authorized; and finally (3) securing and verifying travel documents to prevent people from illicitly traveling on an assumed identity.

Identifying High Risk Travelers

The first critical step to thwarting terrorist operations along the travel pathway is to identify those associated with, suspected of being engaged in, or supporting terrorist or other illicit activities as well as the technique they use to avoid detection. This is done by collecting, maintaining, and updating data and integrating knowledge of terrorist travel patterns into our border screening systems operations.

While watchlists existed prior to 9/11, they were neither coordinated nor consolidated to a degree and depth commensurate with what we now know to be the threat of terrorism. The 9/11 Commission recommendations and subsequent government hearings, reports and recommendations provided guidance to properly enhance this avenue for identifying and preventing the terrorist the threat.

Terrorist Screening Center

The Terrorist Screening Center (TSC) is a multi-agency center where identifying information on Known and Suspected Terrorists (KST) data from several agencies is consolidated into the Terrorist Screening Database (TSDB). This information is used to support authorized law enforcement, regulatory, and intelligence agencies in their responsibilities to screen individuals for association with terrorist activity. This mission facilitates secure, effective, and timely interagency information sharing related to encounters with individuals included in the TSDB. TSC does this while ensuring the data it stores is maintained in a manner that maximizes privacy and civil liberties protections of U.S. Citizens.

The TSC provides law enforcement officers with the information needed to help them positively identify known or suspected terrorists trying to obtain visas or immigration benefits, enter the country, board aircraft, or engage in other activity that could jeopardize national security. The system uses biographic and biometric identifiers to support border and immigration screening and inspection procedures. As an example, the system stores and maintains photographs of KSTs and makes this information available to the Department of State for visa screening. The broad range of information available and ability to securely deliver it to the front line screening agency, overseas, at the border, or within the U.S. is a major improvement to the processes in place prior to 9/11.

National Targeting Center

A key tool for DHS in analyzing, assessing, and making rapid determinations based on TSC TSDB and other information, is the National Targeting Center (NTC), run by CBP. The NTC is a 24 hours a day, 7 days a week operation, established to provide tactical targeting information aimed at interdicting terrorists, criminal actors and implements of terror or prohibited items. Crucial to the operation of the NTC is CBP's Automated Targeting System, a primary platform used by DHS to match travelers and goods against screening information and known patterns of illicit activity often generated from successful case work and intelligence. Since its inception after 9/11, the NTC has evolved into two Centers: the National Targeting Center Passenger (NTC-P) and the National Targeting Center Cargo (NTC-C). The NTC analysts generate targets of interest or interdiction based upon the results of their research.

On a typical day, the National Targeting Center Passenger:

- Handles approximately 280 telephone inquiries;
- Generates 178 targets of interest and
- Initiates and completes research queries on approximately 328 individuals.

The National Targeting Center Cargo is a critical layer in CBP's layered enforcement strategy. NTC-C's responsibilities are international in scope, leveraging classified, law enforcement, commercial, and open source information to proactively target and coordinate examinations of high-risk cargo in all modes of transportation. NTC-C provides high-quality research and support to all international Container Security Initiative, Secure Freight Initiative, and domestic analytical and targeting units, as well as other government agencies. NTC-C fosters international partnerships and promotes relationships across the federal government with the Drug Enforcement Agency (DEA), Immigration and Customs Enforcement, National Counterterrorism Center (NCTC), and Federal Bureau of Investigations (FBI).

Yearly and daily statistics for the National Targeting Center Cargo:

- In a typical year, the NTC-C processes more than 11.3 million maritime containers bound for U.S. seaports from foreign ports – an average of 31,000 per day.
- On a typical day CBP NTC-C processes more than 70,200 truck, rail, and sea containers.
- In FY2009, CBP officers stationed at Container Security Ports reviewed over 9 million bills of lading, and conducted over 56,000 exams in conjunction with their host country counterparts.
- CBP's Laboratories and Scientific Services spectroscopy group at the National Targeting Center has responded to some 21,599 requests from the field for technical assistance in resolving alarms. To date 100 percent of all alarms have been successfully adjudicated as innocent.

Human Smuggling and Trafficking Center

In addition to the NTC, DHS also supports and uses the information and intelligence of the Human Smuggling and Trafficking Center (HSTC) to combat illicit and terrorist travel. Section 7202 of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) established the interagency HSTC to achieve greater integration and overall effectiveness among the U.S. government's enforcement and response efforts, and work with other nations to address alien smuggling, human trafficking, and criminal support of clandestine terrorist travel. The Steering Group that oversees the Center is co-chaired by senior representatives of the Secretary of State, the Secretary of Homeland Security and the Attorney General. The Center is unique among U.S. organizations and centers in that it concentrates on illicit travel on a global basis through activities that directly enable terrorist travel and/or offer financial support.

The HSTC brings together experienced law enforcement, intelligence and diplomatic officials from U.S. agencies who are subject matter experts to work together on a full time basis to convert intelligence into effective law enforcement and other action. The HSTC combats illicit travel by:

- Facilitating the broad dissemination of all-source information
- Preparing strategic assessments

- Identifying issues for interagency coordination or action
- Coordinating select initiatives
- Working with, and exchanging information with allied foreign governments and organizations.

The Departments of State, Justice, Homeland Security, and Defense, along with other U.S. agencies participate in and assign personnel to the HSTC. The recent addition of Department of Defense representative to the HSTC has already strengthened efforts to combat the facilitation and flow of foreign fighters. In August DHS Policy and U.S. Special Operations Command co-hosted a conference on illicit travel networks to better coordinate efforts on combating foreign fighter flows and terrorist travel. This conference was attended by 64 individuals from across the government.

National Counterterrorism Center

Among the recommendations put forward by the 9/11 Commission and implemented under the Intelligence Reform and Terrorism Prevention Act of 2004, was the creation of the National Counterterrorism Center and its strategic operational planning capability. The NCTC is charged with integrating all instruments of national power to ensure unity of effort combating terrorism. Pursuant to this authority, the Director of NCTC is responsible for providing strategic counterterrorism plans and effectively integrating and sharing counterterrorism intelligence inside and outside the United States. DHS has personnel assigned to the NCTC and utilizes the resources that the NCTC has at its disposal to coordinate and combat terrorist travel.

Multi-layered Approach to Screening

The second critical step to thwarting terrorist operations along the travel pathway is the screening of travelers or prospective travelers against databases either prior to travel or prior to entering the United States. Terrorist-related screening, as defined under Homeland Security Presidential Directive – 11 (HSPD-11) is "the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security." Terrorist screening is a multi-agency effort that relies on good data, good intelligence and information, and automated capabilities to ensure identification of high-risk activities and individuals.

DHS has the responsibility for the effective control of the United States' borders and securing our domestic transportation systems. This includes reducing the likelihood of terrorists' entry into our country by identifying and interdicting those who pose a terrorist threat or who are not authorized to be in the United States. DHS has been able to play a critical role in preventing terrorist activity through the use of the consolidated watch list, as well as through the development of threat-based screening capabilities based on threat assessments and intelligence information from the Intelligence Community.

DHS creates layers of defense by building security into each step of the transportation process and applying targeting techniques to the unique measures a terrorist traveler must take to get from one place to another. We have built this system to work with existing industry practices and ensure the efficient operation of the travel system by harmonizing business processes across

screening and credentialing programs; prioritizing investments in screening technologies and systems; developing metrics for evaluating and improving screening processes; and setting an overall framework for the business and technical support of DHS screening and credentialing activities.

Advance Screening Information

An effective border screening system must include three reinforcing tracks: first, a consultative mechanism to ensure that an individual matched to a watchlist is in fact the person the U.S. government is interested in; second, a vehicle to accurately and reliably identify all travelers adopting known terrorist and criminal travel tactics even for which we do not yet have reliable identity information (name, passport number, etc); and third, a way for innocent travelers incorrectly caught in the system to seek correction and redress. DHS's layers of defense include all three.

DHS begins its work days before a traveler encounters Customs and Border Protection or the Transportation Security Administration and concludes well after the traveler has completed their trip. In the international context, six steps apply:

1. The first step, applicable only to non-U.S. citizens, is either the adjudication of a visa application or authorization for travel through the Electronic System for Travel Authorization (ESTA), depending on which provision of the Immigration and Nationality Act the individual is traveling under. These systems are designed to weed out the most obvious risks as early as possible. When successful, the illicit traveler may not even book a ticket.

2. Second, DHS reviews the traveler's identity information and travel practices through three reinforcing systems:

    a. The Advance Passenger Information System (APIS), which compares the traveler manifest of commercial and private aircraft, as well as commercial vessels, against law enforcement databases;
    b. Secure Flight, which compares passenger information to the No Fly and Selectee List components of the TSDB;
    c. ATS-P, or Passenger Name Records (PNR) data, which analyzes information from the carriers' reservation system to detect links to KSTs or patterns of criminal or terrorist activity.

    DHS obtains this information and conducts screening shortly before an aircraft's departure (Secure Flight and PNR data is applied up to 72 hours prior to an aircraft's departure; APIS is available when a traveler checks in at the ticket counter or no later than 30 minutes prior to departure). Combined, APIS, PNR and Secure Flight identify over 5,000 known or suspected terrorists a year.

3. Third, at nine airports around the world (selected based on volume of traffic, risk and foreign policy priorities), the Immigration Advisory Program allows CBP Officers to work with foreign law enforcement officers to interview suspect travelers prior to

departure and issue recommendations on the propriety of alien passenger's travel to the United States.

4. Fourth, at the port of entry, alien travelers provide biometric data, including fingerprints to be screened through the US-VISIT program, making it easier to ensure that if a false identity were successfully adopted during the previous steps, this fraud would be caught at the border.

5. Fifth, at the border, CBP Officers apply knowledge gained during the screening process by NTC analysis and training, including behavioral observation techniques, to assess whether the traveler may merit inspection to detect criminal activity, grounds for inadmissibility by non-U.S. citizens or immigration violations.

6. Sixth, the Traveler Redress Inquiry Program allows anyone, regardless of citizenship, who feels he/she has been identified incorrectly to seek an annotation to his/her record and a redress number. This also improves security by ensuring that we don't waste limited resources on innocent people.

In addition to these core layers, DHS, through CBP's Trusted Traveler Programs, has implemented several other tools to allow low-risk travelers to voluntarily submit to additional advance screening in order to gain expedited entry at the port of entry:

- **SENTRI** allows pre-approved travelers to receive expedited processing at dedicated U.S./Mexico land border crossings.
- **NEXUS** allows pre-approved travelers expedited crossing at air, land, and marine ports of entry along the U.S./Canada border.
- **Global Entry** allows pre-approved, frequent international travelers, presently U.S. and Dutch citizens and U.S. Permanent Residents who have passed a background check, to use an automated kiosk to clear passport control, and provides an expedited exit lane out of the CBP processing area.

These programs look at the information the individual presents through the application process through an in-depth vetting process. Only persons who we have deemed to not pose a risk of terrorism or serious crime are allowed to participate in the programs.

Domestically, a similar approach applies. TSA's Secure Flight program adds a vital layer of security against terrorist travel. Secure Flight implements the Intelligence Reform and Terrorism Prevention Act of 2004 requirement for DHS to assume from aircraft operators the responsibility of prescreening passengers against terrorist watch lists on all domestic and international commercial flights (into, out of, within, or over the United States, and point-to-point international flights operated by U.S.-based aircraft operators). Secure Flight provides: early insight into intended travel by potential terrorists through watch list matching; earlier law-enforcement notification and coordination; and a consistent watch list matching process across all aircraft operators. Once Secure Flight is fully implemented in 2010 DHS will have assumed the matching function presently delegated to the air carriers. As a result, TSA will no longer need to distribute the terrorist watchlist to the carriers decreasing the chance terrorist watchlist

data may be released inappropriately. Further, Secure Flight has an integrated redress process for individuals whose name may be similar to a name on the watch list. Secure Flight is being phased in gradually with full implementation for domestic and foreign aircraft operators scheduled to be completed by the end of 2010.

International Cooperation

International travel is a network relying on the fast-paced interaction between travelers, business and government – travel agents in one country, immigration inspectors in another country, and reservation system managers in yet another country may all play a role in moving a terrorist from a training camp abroad to a target in the United States. Our approach to international screening engagement responds to the realities of this network. Our goals are to ensure domestic practices in key partner nations are adequate to minimize risks posed to the United States and to jointly respond to the illicit movement of terrorists and criminals. In many cases, foreign nations can be the best source of information about which of their citizens are most likely to pose a risk.

Central to both of these goals has been DHS' work to reinforce the security features of the Visa Waiver Program (VWP). Since 1986 the VWP has allowed eligible citizens of certain countries to travel to the United States for business or tourism without obtaining a visa. The 35 countries currently in the VWP are among our closest international partners in the fight against terrorism. Participation in the program provides tremendous incentives for countries to maintain high security standards and deepen their cooperation with the United States on security-related issues. These enhanced measures—including sharing lost and stolen passport data (LASP) information with the United States through INTERPOL; sharing security and law enforcement information with the United States; cooperation on repatriation matters; and strengthening document security standards, and airport and aviation security—help secure the United States and prevent terrorist and criminal activities within our VWP partner nations.

Beyond the VWP, DHS has relied on a variety of bilateral and multilateral partnerships to combat terrorist travel. In particular, our bilateral cooperation with Canada, Germany, the United Kingdom, other European Union member states, and other partners including the International Criminal Police Organization, coupled with our multilateral work through the Five Country Conference (Australia, Canada, New Zealand, UK, and the United States), the Caribbean Community (CARICOM), the Asia-Pacific Economic Cooperation forum, the Group of 8 Lyon/Roma Working Group, and the International Civil Aviation Organization has proven critical. International screening programs are intended to leverage data and resources held by other governments to improve the ability of DHS and its foreign partners to identify illicit activity as part of the normal travel or migration process. Successful partnerships include:

- By comparing the fingerprints of a small subset of asylum seekers, Canada, the United Kingdom and the United States have cooperatively identified over 200 cases of fraud. On November 24th, Secretary Napolitano and Minister of Public Safety Canada Peter Van Loan announced an agreement under which DHS and Public Safety Canada may exchange up to 3,000 fingerprints per year to assist in immigration related cases. The UK, Australia and New Zealand intend to adopt compatible practices through the Five Country Conference.

- Since September 2009, the United States and United Kingdom have cooperated to jointly screen visa applications for persons in the U.S. seeking to travel to the UK, already identifying nearly 40 suspect applications.
- As a result of the 2006 terrorist plot to destroy aircraft flying from the UK to the United States, the National Targeting Center now works regularly with its British equivalent, the Joint Border Operations Center, to collaborate and exchange information on high-risk flights between the two nations.
- DHS and CARICOM worked together to support security efforts during the 2007 Cricket World Cup, identifying 94 travelers with derogatory information in the Terrorist Identities Datamart Environment (TIDE) or held by INTERPOL matches.
- Since 2007, every person entering the United States by air or sea or submitting an application to ESTA has had his/her passport number vetted against the INTERPOL Stolen and Lost Travel Documents database (SLTD). This initiative regularly nets five or more cases of fraud per month that would not have been identified without the system. Through a partnership with Australia and New Zealand, similar work is accomplished through the Regional Movement Alert System (RMAS).

Through these efforts, DHS seeks to create an international norm for sharing terrorism and criminal information and identity management. Portions of the international community, however, have not agreed to share such information due to concerns regarding privacy protection. The Department, along with the Departments of Justice and State, is working to develop broader privacy agreements to ensure that data sharing can be facilitated under strong privacy norms not requiring legal harmonization. In October 2009, the U.S. Government agreed with the European Union on a set of common principles that unite our approaches to protecting personal data when exchanging information for law enforcement and security purposes. This was an important step towards greater cooperation.

Securing Travel Documents

Working with our international partners and strengthening our requirements for which documents are acceptable for entry to the United States has led to the development of more secure passports and travel documents. At today's hearing, the Department of State and Under Secretary Rand Beers from DHS will provide greater insights into what is being done to secure passports and incorporate biometric verification during screening.

The Western Hemisphere Travel Initiative (WHTI) requires U.S. and Canadian travelers to present a passport or other document that denotes identity and citizenship when entering the United States, facilitating entry for U.S. citizens and legitimate foreign visitors, while strengthening U.S. border security. WHTI went into effect June 1, 2009 for land and sea travel into the United States. WHTI document requirements for air travel went into effect in 2007.

US-VISIT supports the Department of Homeland Security's mission to protect our nation by providing biometric identification services to federal, state and local government to help them accurately identify the people they encounter and determine whether those people pose a risk to the United States. US-VISIT collects biometrics—digital fingerprints and a photograph—from international travelers at U.S. visa-issuing posts and ports of entry, helping immigration officers to determine whether a person is eligible to receive a visa or enter the United States. US-VISIT

helps prevent identity fraud and makes it more difficult for criminals and immigration violators of the ability to cross our borders or remain in the United States. US-VISIT also supports the Department's ability to identify international travelers who have remained in the United States beyond their period of authorized admission by analyzing biographical information.

US-VISIT is helping to make U.S. immigration and border management efforts more collaborative, more streamlined and more effective. As Congress required and through the VWP, the U.S. has mandated secure passport issuance processes and documents from VWP countries. Because this is becoming the norm, other countries are also moving to develop and implement more secure passport issuance processes and documents. Through the Credentialing Framework Initiative, DHS has set the direction for DHS screening entities to use recurrent vetting—the process by which stored identity data is compared against new derogatory information (i.e., watchlist nominations, wants and warrants, convictions) as it becomes available where the person being screened has an ongoing eligibility requirement. As a result, vetting and risk assessments conducted are based on current information and not just point in time checks. This process is in place for biometric checks conducted through DHS's Automated Biometric Identification System (IDENT), CBP's Trusted Traveler populations, and for TSA's Threat Assessment and Credentialing programs.

Conclusion

Thank you again for this opportunity to testify about our efforts to counter and prevent terrorist travel. As I am sure you and your colleagues appreciate, this phenomenon presents a real and serious challenge to our nation, and requires that we utilize the full gambit of intelligence and law enforcement resources. I look forward to answering any questions you may have.

Department of Justice

STATEMENT OF

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

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ENTITLED

"FIVE YEARS AFTER THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT: STOPPING TERRORIST TRAVEL"

PRESENTED

DECEMBER 9, 2009

Statement of Timothy J. Healy
Director
Terrorist Screening Center
Before the Senate Homeland Security
and Governmental Affairs Committee
December 9, 2009

Good morning Chairman Lieberman, Ranking Member Collins and members of the Committee. Thank you for the opportunity to discuss the Terrorist Screening Center (TSC) and its role in combating terrorist travel.

Over the past six years, the TSC has become a powerful tool to fight terrorism and integrate the law enforcement and intelligence communities by consolidating terrorist information into a single Terrorist Watchlist. We are continuing to move forward to enhance our partners' ability to combat terrorism by improving the U.S. Government's approach to terrorist screening and safeguarding civil liberties in the process. Our interagency watchlisting and screening efforts have matured into a true information sharing success, and with your continued support we hope to improve upon our initiatives to provide critical terrorist identity information to our domestic and foreign partners for terrorist screening purposes. Let me begin by telling you about where we are today and where we want to be in the future.

Overview

Established in 2003, the TSC is a multi-agency center that connects the law enforcement communities with the Intelligence Community by consolidating information about known and suspected terrorists into a single Terrorist Screening Database, which is commonly referred to as the "Terrorist Watchlist." The TSC facilitates terrorist screening operations, helps coordinate the law enforcement responses to terrorist encounters developed during the screening process, and captures intelligence information resulting from screening.

Of paramount significance is the TSC's success in making this critical information accessible to the people who need it most – the law enforcement officers who patrol our streets, the Customs and Border Protection Officers who protect our borders, and our other domestic or foreign partners who conduct terrorist screening every day. In the six years since we began operations, the Terrorist Watchlist has become the world's most comprehensive and widely shared database of terrorist identities. The current terrorist watchlisting and screening enterprise is an excellent example of interagency information sharing whose success is due to the superb collaborative efforts between the TSC, the FBI, the Department of Homeland Security (DHS), the Department of State, the Department of Defense, the National Counterterrorism Center (NCTC) and other members of the Intelligence Community.

Operating in the Interagency and International Environment

Issued on September 16, 2003, Homeland Security Presidential Directive (HSPD) 6 directed the Attorney General to establish an organization to consolidate the U.S. Government's approach to terrorist screening and provide for the appropriate and lawful use of terrorist information in screening processes. That organization, the TSC, became operational on December 1, 2003. The TSC is administered by the FBI with support from the DHS, the

Department of State, the Department of Defense and others in the Intelligence Community. Staffed with personnel from these agencies, the TSC's single strategic goal is to enhance our partners' ability to combat terrorism. In order to do so, we provide those who conduct terrorist screening operations throughout the world with a thorough, comprehensive and consolidated listing of all known or suspected terrorists. We strive to maintain the highest-quality data concerning known or suspected terrorists to aid in the identification process. We ensure the timely dissemination of terrorist identity data and that prompt notification is made when a known or suspected terrorist has been identified through a screening process. We also ensure that privacy is protected and civil liberties are safeguarded throughout the entire watchlisting and screening process.

The identities contained in the Terrorist Watchlist originate from credible information developed by our intelligence and law enforcement partners or by our trusted foreign partners. Federal departments and agencies submit nominations of known or suspected international terrorists to the NCTC for inclusion in the NCTC's Terrorist Identities Datamart Environment (TIDE) database. These nominations are reviewed and then forwarded to the TSC for final adjudication and inclusion in the Terrorist Watchlist. In a similar process, nominations of domestic terrorists are provided to TSC directly by the FBI.

TSC accepts nominations into the Terrorist Watchlist when they satisfy two requirements. First, the biographic information associated with a nomination must contain sufficient identifying data so that a person being screened can be matched to or disassociated from a watchlisted terrorist. Second, the facts and circumstances pertaining to the nomination must meet the "reasonable suspicion" standard of review established by terrorist screening Presidential Directives. Reasonable suspicion requires "articulable" facts which, taken together with rational inferences, reasonably warrant a determination that an individual is known or suspected to be or has been engaged in conduct constituting, in preparation for, in aid of or related to terrorism and terrorist activities, and is based on the totality of the circumstances. Due weight must be given to the reasonable inferences that a person can draw from the facts. Mere guesses or inarticulate "hunches" are not enough to constitute reasonable suspicion.

Most of the individuals on the Terrorist Watchlist are not U.S. citizens, but are terrorists living and operating overseas. The Terrorist Watchlist is made up of approximately 400,000 people. The reasonable suspicion standard includes known or suspected terrorists ranging from suicide bombers to financiers. The "No Fly" list has its own minimum substantive derogatory criteria requirements which are considerably more stringent than the Terrorist Watchlist's reasonable suspicion standard. In order to be placed on the "No Fly" list, a known or suspected terrorist must present a threat to civil aviation or national security. Consequently, the "No Fly" list is a very small subset of the Terrorist Watchlist currently containing approximately 3,400 people, of those approximately 170 are U.S. persons. On a daily basis, the TSC receives between 400 and 1,200 unique additions, modifications or deletions of terrorist identities. It is through this nomination and review process that the TSC strives to maintain a thorough, accurate and current database of known or suspected terrorists for lawful and appropriate use in the screening process.

The Terrorist Watchlist is utilized by law enforcement, intelligence and other U.S. Government agencies including Department of Homeland Security and Department of Sate as well as foreign partners who conduct terrorist screening operations. The screening process leverages thousands of our law enforcement officers and other governmental partners to help identify, detect and deter terrorists. Terrorist screening occurs throughout the world at our embassies, ports of entry, and international postal and cargo facilities. Terrorist screening occurs during police stops, during special events, when a HAZMAT license is issued, or when a gun is purchased.[1] Screening occurs when passports or visa applications are processed, as well as when citizenship and immigration applications are processed. Select foreign partners use a subset of the Terrorist Watchlist when they conduct screening operations abroad.

Our Tactical Operations Center runs 24 hours a day and receives approximately 150 calls a day. They determine whether individuals encountered are a positive match to a watchlisted known or suspected terrorist. All positive matches, which are approximately 30-40% of all reported encounters, are forwarded to the FBI's Counterterrorism Division for an appropriate law enforcement response. The response could range from arresting the subject, if there is an outstanding federal warrant, to merely gathering additional intelligence information about the subject. During FY2009, the TSC processed over 55,000 "encounters" from federal, state, local, tribal and territorial screening agencies and entities. Of those encounters, over 19,000 were a positive match to a watchlisted known or suspected terrorist.[2]

Most encounters provide valuable intelligence to the FBI case agent. Each provides information regarding the specific time, place, geographic location and circumstances of the encounter with the watchlisted individual. During an encounter, additional biographic or biometric identifiers for the watchlisted individual might be discovered, new derogatory information could be obtained or additional terrorist associates could be identified. Throughout FY2008 and FY2009, the number of daily encounters steadily increased. We expect the number of daily encounters will continue to increase as new screening partners join our national and international enterprise.

In conjunction with Department of State, we have completed bilateral terrorist screening agreements with 17 foreign governments. Furthermore, we have provided additional screening support for certain international events, such as the World Games. Over the past two years, our outreach teams have coordinated with all 72 state and local fusion centers. In response to requests from state, county and local law enforcement agencies, terrorism-related information is now electronically available online via Law Enforcement Online (LEO). It is also available to the Regional Information Sharing System (RISS), and the Homeland Security State and Local Intelligence Community of Interest (HS-SLIC). To provide situational awareness, TSC now notifies fusion centers when encounters occur within their area of responsibility or when encounters occur with cases that originated from their area of responsibility. We also provide coast-to-coast briefings and training to both police dispatchers and law enforcement officers

[1] In fact, based on figures from a GAO report from 2004 to 2009, less than 1,000 background checks resulted in positive matches to the Terrorist Watchlist with less than 100 individuals (or approximately 10% of the total) being prevented from purchasing a weapon.

[2] The watchlisted person being screened may not always be present during the screening encounter. For example, a watchlisted person may apply for immigration benefits by mail and will, therefore, not be present during the screening encounter that takes place at a distant U.S. Citizenship and Immigration Services office.

concerning the importance of notifying TSC of any encounter they have with a watchlisted known or suspected terrorist. Because of the significance of TSC's contribution to fusion centers, the TSC was recognized for its innovative information sharing initiatives at the 2009 National Fusion Center Conference.

The Road Ahead

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

Our watchlisting efforts must be predicated upon four basic operational concepts: maintenance of high-quality terrorist identity data, timely dissemination of terrorist identity data, responsive information sharing, and safeguarding civil liberties. We update existing Terrorist Watchlist records as more current information becomes available as a result of screening encounters. This screening process triggers an automatic review of the record, ensuring its accuracy, and determines the continued appropriateness for inclusion into the Terrorist Watchlist. We also continuously conduct reviews of every record already contained within the Terrorist Watchlist to ensure its current accuracy.

Once a known or suspected terrorist is identified and included in the Terrorist Watchlist, we must ensure the timely dissemination of the terrorist identity data to our screening partners. The utility of the watchlisting enterprise is of little value unless the information contained within the Terrorist Watchlist is efficiently disseminated to those who need it the most. The screening agencies throughout the world who attempt to ascertain if a person screened is watchlisted constitute a global network, dedicated to identifying, preventing, deterring and disrupting potential terrorist activity. U.S. Customs and Border Protection uses the Terrorist Watchlist at all 327 ports of entry and all of the 15 pre-clearance offices located in Canada, the Caribbean, and Ireland. They also use the Terrorist Watchlist to conduct screening operations at international mail and cargo facilities. State, local, tribal and territorial law enforcement agencies use the Terrorist Watchlist when conducting police checks. The Transportation Security Administration uses the Terrorist Watchlist when they coordinate the screening of all commercial air passengers traveling on domestic and international flights. Department of State diplomatic posts and passport offices use the Terrorist Watchlist to screen aliens seeking visas, and U.S. persons applying for U.S. passports. Our 17 foreign partners seek access to the Terrorist Watchlist to conduct screening operations in their respective countries.

Throughout the entire watchlisting and screening process the TSC continues to play a significant role in ensuring that civil liberties are safeguarded and privacy is protected. The TSC led the interagency initiative to develop an effective interagency redress process and maintains a separate unit dedicated to resolving redress matters regarding individuals who believe they have been incorrectly watchlisted. The goal of the redress process is to provide a timely and fair review of redress inquiries referred to the TSC. Working closely with our interagency partners, we implemented a Memorandum of Understanding (MOU) on Terrorist Watchlist Redress Procedures that was signed in September 2007. The MOU standardizes interagency watchlist

redress procedures and provides complainants with an opportunity to receive a timely, fair and accurate review of their redress concerns. A traveler or complainant who believes they were inconvenienced as a result of screening can submit a redress complaint through the DHS Traveler Redress Inquiry Program, commonly referred to as DHS TRIP. Pursuant to the interagency Redress MOU, the complaint is reviewed by the agency that received it, and referred to the TSC Redress Unit after it has been determined that there is a connection to the Terrorist Watchlist. Of note, only 0.7% of the DHS TRIP complaints actually have some connection to the Terrorist Watchlist. Of the 0.7% that have a connection to the watchlist, approximately 51% are appropriately watchlisted, 22% have been modified or reviewed prior to redress, 10% were similar names, and 15% were removed or downgraded due to the redress process. Our Redress Unit researches the complaints, coordinates with the agency that nominated the complainant to the Terrorist Watchlist, and, if warranted, corrects any Terrorist Watchlist data that may cause the individual difficulty during a screening process. We review all available information and work with the nominating or originating agency to determine if the complainant's watchlisted status should be modified. Upon the conclusion of our review, we advise DHS TRIP representatives of the outcome so they can directly respond to the complainant. In some cases, we determine that the individual should remain watchlisted, but we may modify the individual's watchlist status (i.e. downgrade the individual from being on the "No Fly" list to the "Selectee" list).

We have also established protocols to aid individuals who have continuously been misidentified as possible known or suspected terrorists during the screening process because their name is similar to that of a properly watchlisted individual. In these situations, we often determine that their identity is very similar to a known or suspected terrorist. To provide relief, we issue what is called a "Primary Lookout Override," so the individual will not be inconvenienced during future screenings.

Additionally, when the TSC is advised, through media or Congressional inquiries, of individuals who have encountered travel difficulties due to their perceived watchlist status, we review the pertinent watchlist encounter records to determine if the individuals are indeed being misidentified. If they are misidentified, we examine our records to determine if there is any additional information that could be added that would reduce future misidentifications. The TSC neither confirms nor denies that an individual is watchlisted. We do, however, assure the inquiring entity that we have examined applicable Terrorist Watchlist records to ensure they contain current and accurate information, and that we have taken all reasonable measures to reduce any future misidentifications.

The operating procedures that we have implemented to accurately process all watchlisting data, expeditiously respond to terrorist screening encounters, and promptly provide a redress mechanism to resolve watchlisting discrepancies are all designed to enhance our partners' ability to combat terrorism, while simultaneously protecting privacy and safeguarding civil liberties. Our ongoing commitment to maintain high-quality terrorist identity data, to timely disseminate terrorist information, and to share what has been identified during encounters is evidenced by the following projects and initiatives:

Secure Flight: Previously, air carriers were responsible for screening airline passengers. Under the Secure Flight program, the U.S. Government assumes that responsibility. As the Secure Flight program expands, I will ensure that we continue to provide our support for that important effort.

DHS Watchlisting Service (WLS): When the DHS WLS is fully operational, the current process of exporting Terrorist Watchlist data to individual DHS components will be replaced with one daily Terrorist Watchlist export. This initiative will be completed during the FY2010 timeframe.

Biometrics: We are implementing a process to include biometric identifiers to the Terrorist Watchlist. Working with the NCTC and the FBI's Criminal Justice Information Services Division, we anticipate being able to receive, hold and export biometric data, in accordance with HSPD-24.

Gold and Platinum Projects: Our Gold Project proactively notifies the FBI when a known or suspected terrorist that has been nominated by another government agency has been encountered in the United States, so the FBI can take appropriate investigative action. We track these cases very closely to confirm that the applicable FBI field office is cognizant of the terrorist encounter within its jurisdiction and has taken appropriate action. Our Platinum Project identifies known or suspected terrorists who are nominated by other government agencies, but who have a connection to the United States (like a U.S. driver's license) that indicates they might already be located in the United States or might possibly attempt future travel to the United States. We will continue to track the efforts to actually locate these known or suspected terrorists and will not consider the matter resolved until they are found.

Editable Terrorist Watchlist: To ensure that the records TSC exports to our screening partners are as accurate as possible, we are working with the NCTC to expedite daily modifications to the Terrorist Watchlist.

Conclusion

As previously stated, our watchlisting and screening enterprise would not be where it is today without the superb collaborative efforts between the TSC, the FBI, the DHS, the Department of State, the Department of Defense, the NCTC and other members of the Intelligence Community. Chairman Lieberman, Ranking Member Collins and members of the Committee, thank you for the opportunity to address this Committee. I look forward to answering your questions.

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator George V. Voinovich
Senate Committee on Homeland Security
and Governmental Affairs
December 9, 2009

Question:

I understand that the individuals who carried out the September 11, 2001 terrorist attacks entered the U.S. on visas rather than under the Visa Waiver Program. It's clear that even today our visa issuance process isn't perfect, since in October the FBI announced the arrests of both U.S. citizens and foreign nationals in the United States who were working with criminal counterparts in Ukraine to fraudulently obtain U.S. visas for Ukrainian nationals who then traveled to the United States. What is being done to prevent situations like this from occurring?

Answer:

Individuals seeking to enter the United States, whether with a visa or under the terms of the Visa Waiver Program (VWP), undergo namecheck screening against constantly updated and shared interagency watchlists, which include the names, biographic and, increasingly, biometric information of individuals linked to terrorism, criminal, and illegal migration activities. For visa applicants, namechecks are run in the Department of State's Consular Lookout and Support System (CLASS); VWP travelers submit online applications in DHS's Electronic System for Travel Authorization (ESTA) program. Consular officers also have a powerful array of commercial and other USG databases available to verify applicant's identities, relationships, and supplemental information.

In addition to the technological resources available, consular officers place a great deal of importance on the personal interview as it is perhaps the best opportunity for consular officers to determine the credibility of an applicant and the applicant's travel plans and the stated purpose of visit to the United States. Consular officers are trained in interview techniques, foreign languages, and cultural awareness skills they leverage during visa interviews. Because visa application fraud can be present in a variety of forms, such as fraudulent documents, fictitious relationships and identities, and mutilated fingerprints, CA employs a layered approach to secure the integrity of the visa adjudication process. We have put in place an array of measures, including analytic interviewing techniques, biometric checks, database checks, and document verification. In addition, issued visas are constantly checked against terrorist databases and revoked if appropriate. This layered approach poses a significant obstacle and deterrent to foreign persons seeking entry to the United States to do us harm.

To further enhance border security, special agents with the State Department's Diplomatic Security Service are assigned to 73 overseas posts, including Kyiv. We are seeking to expand the program by assigning up to 48 more special agents abroad in the forthcoming year. The primary task of these

investigators is to conduct criminal investigations related to passport and visa fraud.

Despite our best efforts to combat document and travel fraud, U.S. travel documents are coveted by a wide variety of transnational criminal actors, both for access to the United States as well as for the credibility a U.S.-issued travel document affords travelers anywhere in the world. As the incident you describe suggests, we must constantly increase our knowledge, refine our procedures, and maintain our cooperation with federal government and international partners in our ongoing efforts to combat visa fraud.

Question:

I am told that the VWP can be used as a "carrot" to get countries to act in certain situations. Please tell us about how the potential to participate in the VWP was used this summer to get Greece to ratify the U.S.-EU Mutual Legal Assistance Treaty.

Answer:

Cooperation on law enforcement and security issues is a main component of the VWP statute. We are pleased that Greece has ratified the MLAT, a prominent tool in our law enforcement cooperation efforts.

Question:

In February the State Department wrote to me that "the VWP is a unique and valuable instrument that furthers our joint goal of protecting our borders while promoting legitimate travel to the United States." Please explain in detail why the State Department believes the VWP is a valuable tool that helps protect our borders.

Answer:

The Department of State believes the security of the Visa Waiver Program (VWP) was greatly enhanced by the passage of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the 9/11 Act), which amended Section 217 of the Immigration and Nationality Act. Countries must satisfy myriad security standards to participate in the VWP, including initial and periodic eligibility reviews and document and border security standards, as well as entering into information-sharing agreements with the United States. To meet 9/11 Act requirements for information sharing, we are engaging with VWP countries regarding sharing information on specific individuals who may be a threat to our security. Through Homeland Security Presidential Directive 6 (HSPD-6), State and the Terrorist Screening Center (TSC) are negotiating bilateral arrangements to share terrorism screening information with VWP member countries. To share criminal history information on a bilateral basis, State, DHS and DOJ are negotiating agreements with VWP countries.

This information sharing and security cooperation strengthens border security by improving our ability to identify when travelers from 36 countries may pose a serious threat. VWP also allows us to free up consular resources to focus on travelers who need greater scrutiny.

The VWP has also proven a critical tool for assessing, exporting and enforcing standards and best practices. By mandating the issuance of electronic passports, for example, the VWP has expedited the adoption of enhanced travel security techniques. The required VWP review process, in turn, helps ensure that these standards continue to be met.

The implementation of DHS's Electronic System for Travel Authorization (ESTA) requires VWP travelers to be approved for VWP travel before they can board a flight or ship bound for the United States. ESTA provides DHS with the capability to conduct both advance and recurrent vetting of VWP travelers against multiple law enforcement and security databases. Travelers denied an ESTA must apply for a U.S. visa. Denial cases are entered as a lookout in CA's CLASS system so consular officers are aware of not only the fact that a traveler was denied an ESTA approval, but the reason for the denial, and can take that reason into account during the visa interview.

Question:

Additionally, please explain whether and why the VWP is an important tool of smart power.

Answer:

As Secretary Clinton said "We must use what has been called smart power: the full range of tools at our disposal – diplomatic, economic, military, political, legal, and cultural – picking the right tool, or combination of tools, for each

situation." The VWP is an important legal tool that gives us flexibly, particularly in the consular and immigration context. As a travel program, the VWP allows the Department to focus our limited consular resources in countries whose nationals require more in-depth scrutiny. The VWP also serves as a mechanism to spread around the world best practices such as electronic passports and the reporting of lost and stolen passport data; both of which contribute to our goal of safer and more secure international travel for all travelers. In hopes of joining the VWP, many countries have been strengthening their security and border procedures to meet our VWP requirements. Approximately half of the nonimmigrant travelers to the United States each year come under the VWP. This makes the VWP an important economic tool that facilitates exports of U.S. goods and services, valuable foreign investment in the American economy, travel on U.S. airlines and tourism to all parts of our country. European and East Asian VWP members allow U.S. citizens reciprocal visa free travel to their countries, making it easier for U.S. citizens to conduct business overseas, as well as building the other country's economy.

Question:

In 2008, GAO estimated that the elimination or suspension of the VWP could cause a dramatic increase in visa demand that would require about 45 new facilities that could cost almost $6 billion to build. Please tell us how you believe abolishing the VWP, or enacting legislation that would exclude many of the 35 member countries from the Program would impact the State Department.

Answer:

The GAO's May 2008 Border Security Report (GAO-08-623) examines the impact on visa demand, resource needs, and revenues, were the Visa Waiver Program (VWP) to be eliminated or expanded. The information it contains is still useful and relevant today. The report stresses the impact that elimination would have on security, trade, commerce, business, tourism, diplomacy, reciprocity of fees, and the significant negative effects on those interests as well as on our relations with those countries.

Elimination of the program would dramatically increase the demand for visas in the current 36 VWP countries (which now includes Greece), and overwhelm visa operations in the short-term. In the first twelve months, the demand for visa services in those countries would jump from about 760,000 processed in 2009 to about 14 million (over 13.8 million travelers applied for ESTA travel authorizations in 2009). To understand the magnitude of this increase, the total *worldwide* FY 2009 nonimmigrant visa workload was 7.7 million.

Attempting to meet demand would be extremely expensive. State would need to respond with a surge of Temporary Duty personnel who are on per diem, staying in expensive temporary lodging, and working in costly temporary office facilities. Manpower needs would cover the entire spectrum of support: Foreign

Service Officers, local hire consular staff, security, consular management, and general services support (financial, IT, management, property, procurement, and others).

Longer-term, the demand could stabilize, because visas are typically issued for a five to ten year validity period. Nevertheless, the remaining long-term higher demand would directly affect the resources that State would need to meet the demand, maintain its consular operations, and the amount of visa revenue that State receives.

The May 2008 GAO report remains a relevant source of information; the following information is still applicable:

- approximately 45 new facilities required to handle the increased visa demand;
- $3.8 billion to $5.7 billion to construct new facilities;
- seven years to complete construction;
- 540 new Foreign Service officers at a cost of around $185 million to $201 million per year;
- 1,350 local Locally Engaged Staff (LES) at a cost of around $168 million to $190 million per year;
- $93 million to $111 million per year for additional management and

support positions overseas and in Washington.

To quote from the GAO report, "Any response would be fully reliant on significant levels of additional funding and staffing, and would reflect the circumstances that brought about elimination."

Question:

What impact would such action have on our public diplomacy efforts?

Answer:

Membership in the Visa Waiver Program is an important bilateral issue for the 36 member countries. Any modifications to the program receive significant media attention and any suspension of the program would lead to enormous negative publicity in the countries affected by such change. We would make tremendous efforts to meet the new demand for visas. However, we believe that elimination of the VWP would – at least in the short run – lead to greatly reduced travel of business persons and tourists to the United States.

Question:

I understand that several of the countries that participated in the VWP prior to 2008 have not complied with the information sharing requirements included in the *Implementing the Recommendations of the 9/11 Commission Act.* How much time and manpower have been required to negotiate and enter into information sharing agreements that your Department has executed to date, and what do you believe is a reasonable amount of time to have such agreements in place with all 35 of the VWP countries?

Answer:

We agree with DHS and the interagency that the information-sharing agreements should be completed with each country by the end of its next biennial review. While we have not tracked the exact time or manpower hours spent to date on concluding information sharing agreements with our foreign partners, the total resources committed have been sizable and have included both policy officers and attorneys from DHS, DOJ, The Terrorist Screening Center (TSC) and the State Department. We will continue to devote substantial resources to these efforts because we believe the value of these information sharing programs fully justify these expenditures.

To date, many VWP countries are in full compliance with the information sharing requirements of the 9/11 Commission Act, and the remaining countries have been engaged on their outstanding requirements. State and DHS recently sent a cable to our Embassies in VWP capitals which are not compliant reminding them of the 9/11 Act requirements for information sharing on law enforcement and security matters.

Question:

What can Congress do to help you ensure that those agreements are put into place in a timely manner?

Answer:

We appreciate Congress' interest in helping us conclude these agreements, but we note that the primary obstacles we encounter relate to our foreign partners' legal requirements, specifically those related to data protection and privacy concerns. Although the United States and our foreign partners are all committed to protecting the data that would be exchanged in these agreements, our domestic legal structures and privacy regimes are different and we have often found those differences difficult to reconcile. We are committed to working hard to address our foreign partners' concerns to the extent possible under our own laws.

Question#:	1
Topic:	VWP
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to the Honorable David F. Heyman
From Senator George V. Voinovich

Question: DHS can terminate a country's participation in the VWP if a situation in that country threatens U.S. law enforcement or security interests, and DHS has used this authority in recent years.

How and when does DHS determine whether a VWP country presents such a threat to the U.S.?

Response: By law, DHS is required to formally review countries participating in the VWP at least once every two years. DHS has developed a continuous and vigorous monitoring process—to include site inspections by DHS-led technical teams—to ensure awareness of changing conditions in Visa Waiver Program (VWP) countries, which may affect countries' VWP designation status. In the event that DHS identifies an issue of concern with a VWP country that could compromise U.S. security or law enforcement interests (including immigration enforcement interests), DHS—in consultation with the Department of State (DOS)—can terminate that country's VWP designation. Since the program's inception, one country has been terminated after a formal review period. In 2003, Uruguay's VWP membership was terminated because its participation in the VWP was determined to be inconsistent with U.S. interest in enforcing immigration laws of the United States.

Through its continuous monitoring function and its active engagement with U.S. officials in VWP countries, DHS works to identify issues of concern early and works proactively with VWP countries so that any issues can be corrected without resorting to termination or employing other sanctions.

Question#:	2
Topic:	provisional status
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: Additionally, DHS can place a VWP country on provisional status if DHS needs additional time to determine whether the country's continued participation in the VWP is in the security interest of the U.S.

How and when does DHS determine whether to use this authority?

Response: In the event that DHS identifies an issue of concern with a Visa Waiver Program (VWP) country that could compromise U.S. security or law enforcement interests (including immigration enforcement interests), DHS —in consultation with the Department of State—can decide to allow that country to maintain its VWP designation on a provisional basis. In 2003, for example, the Department of Justice—which oversaw the VWP at that time—allowed Belgium to continue its participation in the VWP on a provisional basis because of concerns about the integrity of its non-machine-readable passports and the inadequacy of its lost and stolen passport reporting to the United States. In a subsequent review, DHS removed Belgium's provisional status and allowed Belgium to continue its participation in the VWP without conditions.

DHS notes that, through a continuous and vigorous monitoring process and its active engagement with U.S. officials in VWP countries, it has other means at its disposal to identify issues of potential concern and work proactively with VWP countries so that corrective measures can be taken without using provisional status or employing punitive actions.

Question#:	3
Topic:	carrot
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: I am told that the VWP can be used as a "carrot" to get countries to act in certain situations.

Please explain how the potential to participate in the VWP was used this summer to get Greece to ratify the U.S.-EU Mutual Legal Assistance Treaty.

Response: Countries seeking initial or continued designation in the Visa Waiver Program (VWP) must meet certain statutory and other requirements. These countries must have a robust law enforcement relationship with the United States. DHS—in consultation with the Department of Justice and other agencies—thoroughly reviews a country's law enforcement relationship with the United States prior to program designation and as part of the periodic evaluations for continuing designation to determine if appropriate agreements and/or procedures are in place.

One indication of robust law enforcement cooperation is a bilateral agreement to prevent and combat serious crime (a PCSC Agreement). Another, for European Union (EU) Member States, is the ratification and implementation of the United States (US)-EU Extradition Treaty and Mutual Legal Assistance Treaty (MLAT). All three of these critical instruments enable law enforcement officials on both sides to employ state-of-the-art tools to cooperate more effectively to fight terrorism and to bring criminals to justice. For the US-EU Extradition Treaty and MLAT to enter into force, bilateral protocols were required with each of the 27 EU Member States. Greece was the last EU country to ratify the bilateral protocols, which were originally signed on January 18, 2006. This delay not only impeded U.S.-Greek law enforcement cooperation, but also prevented the wider implementation of these agreements throughout the EU. Applying the leverage of the VWP led directly to Greek ratification of the protocols in August 2009, thereby accomplishing a long-standing U.S. objective. The US-EU Extradition Treaty and MLAT came into force with Greece and other EU members on February 1, 2010.

Question#:	4
Topic:	travel
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: I received a letter from Secretary Napolitano in July that stated that "the VWP is a valuable instrument that furthers our goal of protecting our borders while promoting legitimate travel to the United States."

Please explain in detail why the Department of Homeland Security believes this is true.

Response: The VWP is an essential tool in enhancing U.S. border and transportation security while promoting information sharing and stronger partnerships with allied countries.

VWP countries are subject to initial and periodic (biennial) reviews of eligibility by DHS in cooperation with other departments and agencies such as the Department of State and the Department of Justice. These reviews are based on the collection and analysis of comprehensive information on the country's security and law enforcement risks and capabilities. The initial and subsequent biennial reviews normally include site inspections by DHS-led technical teams to observe and evaluate, among other things, the country's counterterrorism capabilities as well as border and passport security procedures. No other mechanism provides DHS with the opportunity to conduct as broad, frequent and—above all—consequential inspections of foreign security standards as does the VWP.

DHS has also implemented a continuous monitoring process to ensure awareness of changing conditions in VWP countries between eligibility reviews. This process includes established protocols for direct communication with the relevant U.S. and foreign embassies for updates of law enforcement or security concerns related to the VWP. DHS regularly makes and follows up on recommendations to mitigate any security risks that are revealed by the continuous country monitoring process.

To gain and maintain eligibility in the program, pursuant to the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), VWP countries are further required to share information with the United States on travelers that may pose a threat to the security or welfare of the United States or its citizens. This requires entering into written bilateral arrangements and agreements to share information on known or suspected terrorists and perpetrators of other serious crimes. In addition, the 9/11 Act requires entering into an agreement with the United States to report lost and stolen passports within strict time limits and in a specific manner.

Question#:	4
Topic:	travel
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Travelers using the VWP are subject to stringent passport security standards. All VWP travelers must use, at a minimum, a machine-readable passport that conforms to the specifications of the International Civil Aviation Organization (ICAO). The use of e-passports, which are particularly difficult to forge, is mandatory for all VWP travelers from countries admitted to the program in 2008 or thereafter and for travelers from pre-existing VWP countries with passports issued after October 26, 2006.

DHS also receives advance passenger information on VWP travelers through the Electronic System for Travel Authorization (ESTA). Prior to any travel to the United States, each VWP traveler is screened—via ESTA—against multiple law enforcement and security databases to determine, on an individual basis and prior to boarding, whether there is any law enforcement or security risk in permitting travel to the United States (with the added benefit that ESTA applications are screened against these databases frequently and recurrently). This ESTA data is not shared with all agencies within the Intelligence Community. As of January 20, 2010, airline carriers are required to confirm that all VWP travelers have an approved ESTA prior to boarding a flight to the United States.

To verify identity, VWP travelers are enrolled into US-VISIT at the port of entry. Their biometric information (ten fingerprints and picture) is collected at the time of first entry to the United States rather than at the time of visa application, as would be case for visa travelers.

Question#:	5
Topic:	al Qaeda
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: In 2007, the Director of National Intelligence testified that al Qaeda is recruiting Europeans because most of them do not require a visa to travel to the U.S. under the VWP.

Is that still the case, and how are you working to prevent a member of al Qaeda or another terrorist organization from entering the U.S. using the VWP?

Response: The Department of Homeland Security (DHS) recognizes that terrorists or individuals with malign intent may attempt to exploit visa-free travel. That is why the Department worked with Congress to transform the Visa Waiver Program (VWP) from a program that evaluated security threats on a country-by-country basis into one that also has the capability to screen for risks on an individual passenger basis. To prevent terrorist travel to the United States, DHS relies on four interrelated elements — advance passenger information, enhanced information sharing, secure travel documents, and intelligence-based VWP assessments — all of which are part of a secure, modernized VWP mandated by the 9/11 Act.

Advance Passenger Information
The Department receives Advance Passenger Information (API) from air carriers before a plane departs for the United States. This information is checked against watchlists and other relevant databases. DHS also collects Passenger Name Record (PNR) data from carriers pursuant to the Aviation and Transportation Security Act, and, in the case of flights to and from the European Union, in conformity with the 2007 U.S.-EU PNR Agreement. This information enables DHS to identify terrorists and criminals known to U.S. law-enforcement and intelligence agencies as well as make connections between known and suspected terrorists and unknown associates.

DHS also receives advance passenger information on VWP travelers through the Electronic System for Travel Authorization (ESTA). Each VWP traveler is screened—via ESTA—against multiple law enforcement and security databases to determine, on an individual basis and prior to boarding a U.S.-bound flight, whether there is any law enforcement or security risk in permitting travel to the United States (with the added benefit that ESTA applications are screened against these databases frequently. As of January 20, 2010, airline carriers are required to confirm that all VWP travelers have an approved ESTA prior to boarding a flight to the United States.

Question#:	5
Topic:	al Qaeda
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Enhanced Information Sharing
The individualized ESTA screening process is enhanced by the additional information sharing agreements required for VWP countries. The 9/11 Act requires that VWP countries enter into an agreement with the United States to share information on travelers that represent threats to the security or welfare of the United States or its citizens. DHS, with the support of the interagency, has determined that entering into two agreements will satisfy this requirement: 1) a Preventing and Combating Serious Crime (PCSC) Agreement to exchange information on potential criminals and; 2) a Homeland Security Presidential Directive 6 (HSPD-6) Arrangement to share terrorist screening information with the United States.

Secure Travel Documents
VWP travelers are subject to stringent passport security standards. To be valid for VWP travel, a passport issued on or after October 26, 2006, is required to include an integrated biometric chip with the facial image and biographical data of the passport holder stored electronically.

The 9/11 Act also requires VWP countries to enter into an agreement to report lost and stolen passport (LASP) data to the United States. As important as the agreements themselves, DHS regularly monitors the frequency and quantity of each VWP country's LASP reporting in order to ensure the country complies with the requirement to report LASPs within strict time limits.

Intelligence-Based VWP Threat Assessments
The DHS Visa Waiver Program Office (VWPO)—in cooperation with other departments and agencies—conducts thorough biennial reviews of VWP countries. Often, these reviews include site visits to the country being evaluated so that DHS can observe, among other things, the country's border and passport security procedures. DHS regularly makes and follows up on recommendations to mitigate any security risks that are identified by that review.

In addition to DHS site-visits, the initial designation and biennial review processes include an independent intelligence community assessment led by the DHS Office of Intelligence and Analysis, on behalf of the Director of National Intelligence (DNI). These assessments, which are incorporated into the DHS VWPO review, specifically analyze the potential for illicit actors, including transnational criminals, extremists or terrorists, to exploit the country's travel systems and security profile to gain entry into the United States under the VWP.

Question#:	5
Topic:	al Qaeda
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

DHS has also developed a continuous and vigorous monitoring process to ensure awareness of changing conditions in VWP countries, including established protocols for direct communication with points of contact in the relevant U.S. and foreign embassies for updates on law enforcement or security concerns related to the VWP. As a result, no other mechanism provides the USG with the opportunity to conduct as broad and as consequential an inspection of foreign security standards as does the VWP.

As a result of these measures, DHS is able to screen VWP passengers far more effectively than we did before the 9/11 attacks and to detect, apprehend, and limit the movement of terrorists, criminals, and other dangerous travelers.

Question#:	6
Topic:	9/11 Commission Act
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that several of the countries that participated in the VWP prior to 2008 have not complied with the information sharing requirements included in the Implementing the Recommendations of the 9/11 Commission Act.

How much time and manpower have been required to negotiate and enter into information sharing agreements that your Department has executed to date, and what do you believe is a reasonable amount of time to have such agreements in place with all 35 of the VWP countries?

What can Congress do to help you ensure that those agreements are put into place in a timely manner?

Response: Since the expansion of the Visa Waiver Program (VWP) in November 2008, DHS' primary VWP-related focus has been bringing the 27 pre-2008 countries into compliance with the information sharing requirements of the Implementing Recommendations of the 9/11 Commission Act (9/11 Act). To date, the Department has made substantial progress in this endeavor; for example, approximately 20 pre-2008 VWP countries have reached understandings with the United States to report lost and stolen passport (LASP) data, as is required by the 9/11 Act. As important as the agreements themselves, DHS regularly monitors the frequency and quantity of each VWP country's LASP reporting in order to ensure the country complies with the requirement to report LASPs within strict time limits.

DHS, with the support of the interagency, has determined that signing a Preventing and Combating Serious Crime (PCSC) Agreement to exchange criminal history information and a Homeland Security Presidential Directive 6 (HSPD-6) Arrangement to share terrorist screening information will satisfy the 9/11 Act requirement that VWP countries enter into an agreement with the United States to share information on travelers that represent threats to the security or welfare of the United States or its citizens. To date, four pre-2008 VWP countries have signed PCSC Agreements with the United States (Germany, Italy, Portugal, and Spain). The interagency has also determined that the United Kingdom has met the criminal information sharing requirement through a number of pre-existing agreements. PCSC negotiations with several other countries are ongoing and DHS expects to conclude additional agreements in the coming months. The Department of State (DOS) has the lead for negotiating HSPD-6 agreements, on behalf of the Terrorist Screening Center (TSC). Details on which pre-2008 VWP countries that

Question#:	6
Topic:	9/11 Commission Act
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

have signed HSPD-6 Arrangements are classified, and DHS would refer requests about HSPD-6 to DOS to provide this information through appropriate channels.

DHS—in cooperation with the DOS and the Department of Justice (DOJ)—has invested considerable resources in negotiating and concluding PCSC agreements. In most cases, the PCSC requires face-to-face discussions with foreign governments to explain the agreement in detail and address each country's concerns, which usually stem from data privacy issues. DHS, with the support of the interagency, has determined that the 27 pre-2008 countries will be given until the end of their current or their next statutorily required VWP continuing designation review cycle to meet the information sharing requirements of the 9/11 Act. DHS will continue to engage pre-2008 VWP countries that have not completed the information sharing requirements to ensure compliance before the end of their respective review cycles.

The VWP is a critical tool for increasing security standards, promoting better information sharing, and strengthening international partnerships. DHS appreciates Congress' continued support of the VWP and its recognition of the substantial security, economic, and public diplomacy benefits the program affords the United States.

Question#:	7
Topic:	authorization
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to the Honorable David F. Heyman
From Senator John Ensign

Question: During the hearing I posed a number of questions with regard to the TSA screening document that was placed on a website and contained Sensitive Security Information including the identification cards of Members of Congress. The questions are as follows:

How high up did the authorization have to go before the document was placed on the website?

Did the authorization go as high as the political appointees or was it just a career employee that placed the document online for all to read?

Response: All the decisions related to this inadvertent posting of Sensitive Security Information (SSI) on the FedBizOpps web site were made at the career employee and staff level. The Transportation Security Administration's (TSA's) Office of Inspection suspended its process review when the Department of Homeland Security (DHS) Office of the Inspector General (OIG) commenced an independent review at the request of the DHS Secretary. The OIG report, dated January 25, 2010, though not specifically naming the individuals responsible for authorizing the placement of the document on the website, states the following regarding decisions made by TSA's Office of Acquisitions (ACQ) and TSA's Screening Partnership Program Office (SPPO) staff:

> **Concerns Surfaced that the Solicitation Did Not Include the Screening Management SOPs**
>
> ... On February 26, 2009, ACQ and SPPO staff discussed whether to include the Screening Management SOPs with a new amendment to the solicitation.
>
> These conversations resulted in a decision to provide a redacted Screening Management SOPs to ensure potential bidders had access to the necessary information to create meaningful proposals in response to the solicitation ....
>
> ACQ staff posted Amendment 2 to FedBizOpps.gov on March 3, 2009 ... This is the first posting of the Screening Management SOPs to FedBizOpps.gov. Interviews with staff from the SPPO and ACQ revealed that neither SPPO nor ACQ performed any check of the electronic document to ensure the redactions were applied correctly. Both SPPO and ACQ staff believed it was the Sensitive Security Information Office's responsibility to provide a fully protected document.

Question#:	8
Topic:	Administrative Leave
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: You mentioned that people were put on Administrative Leave following this release of TSA security sensitive information. Were the people who authorized the release of this information also put on Administrative Leave?

Response: Yes, the staff members responsible for the review and securing of the released Sensitive Security Information were placed on administrative leave.

Question#:	9
Topic:	investigations
Hearing:	Five Years After the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that there are currently 2 simultaneous investigations ongoing with regard to the release of this information, an Inspector General review and an Office of Investigations review.

How long will it take to complete the review process?

Can you provide a timeline as to when people can be held accountable for this release?

When policies may be changed?

Response: Two separate reviews were conducted. The Office of Inspection (OOI) initiated a review on December 6, 2009. It was concluded on December 10, 2009 at which time it was referred the DHS Office of the Inspector General (OIG). The OIG rendered a final report on January 25, 2010.