WRITTEN TESTIMONY OF DAVID HEYMAN
ASSISTANT SECRETARY FOR POLICY
THE
U. S. DEPARTMENT OF HOMELAND SECURITY

before

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Ten Years After 9/11: Preventing Terrorist Travel

JULY 13, 2011
WASHINGTON, DC

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 preventing and countering terrorist travel. Preventing terrorists from traveling to or remaining undetected in the United States is a significant priority for the Department, and I commend the Committee for holding this and associated hearings, examining the progress that has been made since the tragic events of September 11th, 2001.

Ten years ago, screening of passengers coming to the United States was limited to the Department of State visa process, if applicable, and the inspection of a person by an immigration officer at the port of entry, plus whatever processes were applied at foreign airports and by foreign governments. Provision of advance passenger information was voluntary and, even when provided by air carriers, frequently contained inaccurate or inconsistent data. There was no biometric collection for visa applicants beyond photographs, nor for aliens seeking admission to the United States. There was very limited pre-departure screening of passengers seeking to fly to the United States and there was virtually no screening of any kind for domestic flights beyond airport checkpoints. There was no advance screening of passengers seeking admission under the Visa Waiver Program (VWP) and interagency sharing of information on terrorist threats was minimal.

Today, in response to both 9/11 and evolving threats, and with the help and support of Congress, we have significantly adapted and enhanced our ability to detect and interdict threats at the earliest opportunity. All air and sea passengers intending to travel to the United States under the VWP must now obtain an electronic travel authorization before boarding a carrier for travel to the United States through the Electronic System for Travel Authorization (ESTA) program, which screens passengers against various government databases and has virtually digitized the Form I-94W for authorized travelers from participating VWP countries. Additionally, all passengers seeking to fly to, from, or within the United States are similarly screened prior to boarding an aircraft under the Secure Flight program. For non-citizens, passengers' biometrics are collected and checked against terrorist watch lists prior to being issued a visa or being permitted to enter the United States, and agencies share information on known or suspected terrorists with each other. Further, we have developed new capabilities and systems (such as our Advanced Targeting System and Behavioral Detection program) to help identify possible terrorists who may be 'unknown' to us, but who seek to travel to or within the United States to do harm.

Since 9/11, however, the threat has changed to include not only large-scale attacks but also smaller operations with potentially catastrophic effects, such as continued targeting of the aviation sector. One example was attempted only a few weeks after I last testified before you on the subject of terrorist travel—the attempted bombing of Flight 253 on December 25, 2009.

Enhancements since December 25, 2009
Following that attempted bombing, the Department, in coordination with other components of the Administration, has worked to address issues and potential gaps that have been identified to ensure that we have a comprehensive and multilayered approach that begins abroad to detect and

intercept terrorist travel and focuses on stopping terrorists at the earliest point before they can reach the United States. As represented by the other officials who have been asked to testify today on terrorist travel, we can see that this is truly an issue that requires significant collaboration and coordination among federal agencies.

It is important to point out that these improvements are not all directed at one area of the travel continuum—we must use a layered approach to strengthen security. As the 9/11 Commission pointed out, targeting terrorist travel is one of the most powerful weapons we have to counter terrorist operations. 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, the travel industry, and immigration and border security officials. 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 that now necessitates submitting advance passenger information, using a passport and stopping at ports of entry.

Since 9/11, we have learned that preventing terrorist travel through immigration and border security is more than drawing a line in the sand where we can deny entry into our country. Rather, the exercise of immigration and border security authorities can be powerful resources used to identify and thwart terrorist operations at the earliest opportunity.

Accordingly, we have strengthened our security and screening at points:

- During the travel planning phase, when a traveler seeks a visa or authorization to travel;
- Just prior to travel, when a person seeks to board an aircraft at a point of departure; and
- During travel, when a person seeks to enter the United States.

I'll now discuss some of our recent improvements in screening across this travel continuum.

First, fulfilling a key 9/11 Commission recommendation, DHS fully implemented Secure Flight in November 2010. Under Secure Flight, DHS now prescreens 100 percent of passengers on flights flying to, from, or within the United States against the No Fly and Selectee portions of the U.S. known and suspected terrorist watchlist, and other specific data using passenger names, dates of birth, gender and, if applicable, redress numbers before travelers receive their boarding passes. In addition to facilitating secure travel for all passengers, this program helps prevent the misidentification of passengers who have names similar to individuals on government watchlists. Prior to Secure Flight, airlines were responsible for checking passengers against watchlists. Through Secure Flight, TSA now vets over 14 million passengers weekly. Approximately 25 individuals per month are denied boarding an aircraft through the Secure Flight program.

After the attempted attack on December 25, 2009, the United States also implemented threat-based screening measures to strengthen the safety and security of all passengers for air carriers with international flights to the United States. These new measures, which cover 100 percent of

commercial airline passengers traveling by air to the United States, utilize real-time, threat-based intelligence along with multiple layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats.

In addition, in 2010, DHS/TSA updated the Secure Flight program to use all terrorist watchlist records containing a full name and a full date of birth; travelers who are identified as a match against the terrorist watchlists are then designated for enhanced physical screening prior to boarding an aircraft.

DHS has also implemented the Visa Security Program (VSP) through which U.S. Immigration and Customs Enforcement (ICE) deploys trained special agents overseas to high-risk visa activity posts to identify potential terrorists and criminals before they obtain a visa to travel to the United States. The VSP is currently deployed to 19 posts in 15 countries. ICE special agents conduct targeted, in-depth reviews of individual visa applications and applicants prior to the issuance of a visa and recommend to consular officers refusal or revocation of applications, when warranted. Beginning in 2010, DHS began a new initiative with the Department of State where CBP recurrently vets *approved* visa applications so that as new information is discovered, DHS and the Department of State are able to proactively identify individuals who have visas and who may already be in the United States. To date, for fiscal year 2011, we have revoked 782 visas using this process, including 493 who were matches to the TSDB.

Additionally, DHS is continually working with interagency stakeholders to improve and expand procedures for vetting immigrant and nonimmigrant visa applicants, asylees, and refugees. The interagency vetting process in place today is more robust and considers a far broader range of information than it did in past years. Visa applicants, refugees, asylum applicants, and those seeking to enter the United States at a port of entry are subject to rigorous background vetting, biographic and biometric checks—including checks against records obtained from the Department of Defense in Iraq and Afghanistan. The security screening procedures for all of these categories have been enhanced over the past several years as vetting capabilities have evolved and interagency partnerships with the law enforcement and intelligence communities have been strengthened. Further, beginning last year, the Department began piloting a new recurrent vetting process for those applying directly to DHS for immigration benefits, similar to the process previously described for visas. As new derogatory information surfaces, we double-check those who have approved immigration status, such as refugee or asylee status, against this new information. These enhancements are a reflection of the commitment of DHS and other agencies to conduct the most thorough checks possible to prevent dangerous individuals from gaining access to the United States through the immigration process.

In addition, prior to the attempted terrorist attack on December 25, 2009, CBP conducted in-bound passenger targeting using Advance Passenger Information (API) and Passenger Name Record (PNR) data provided by the airlines, but could not easily prevent high-risk travelers from boarding flights to the United States unless they were traveling from a foreign location with an Immigration Advisory Program (IAP) or preclearance presence. After the December 25th attempted terrorist attack, CBP re-engineered its in-bound targeting operations to enable CBP to identify high-risk travelers who are likely to be inadmissible into the United States and to recommend to commercial carriers at <u>all</u> airports with direct flights to the United States that

those individuals not be permitted to board a commercial aircraft. Since the inception of this program—known as the Pre-Departure program—in January 2010, through mid-June 2011, CBP has identified 2,600 passengers who CBP determined would likely have been found inadmissible upon arrival to the United States.

DHS has worked closely with its intelligence and law enforcement counterparts to develop new mechanisms that identify high-risk applicants based on a broader set of data, including information that is not otherwise available to DHS or the Department of State. Similarly, since 2009, the U.S. Government has reformed the criteria and nomination processes for the terrorist watchlist and enhanced its information sharing capabilities so that measures now in place can comprehensively connect available pieces of intelligence to identify individuals who are known to be of security concern as well as people and connections that would otherwise remain unknown. Collectively, these enhancements help us to prevent dangerous individuals from entering the United States, and to support enforcement efforts within the United States if derogatory information develops after a subject of concern has already been admitted.

DHS has also strengthened the presence and capacity of law enforcement to prevent terrorist attacks on commercial aviation. Following the December 25 incident, DHS increased Federal Air Marshal Service (FAMS) coverage of U.S.-flag carriers' international flights through increased operational tempo by existing personnel. With the passage of the FY 2011 year-long continuing resolution, Congress appropriated sufficient funding to allow the FAMS to hire additional air marshals in order for the FAMS to return to pre-December 25 domestic coverage levels while maintaining existing heightened international coverage levels. The expanded FAMS program builds upon additional programs created since 9/11 that further increase the safety of aircraft, including the hardening of cockpit doors and allowing certain law enforcement officers to carry weapons on aircraft.

Building Bridges: International Partnerships, Information-sharing, and Interagency Cooperation

In addition to these recent enhancements and initiatives, there are several cross-cutting efforts that are worth pointing out that underlie all that we do to combat terrorist travel on a day-to-day basis. These efforts represent some of the critical linkages that that are vital for our daily operations to come together and work as a system, and not merely exist as the sum of the various parts. They include increasing international cooperation, sharing intelligence and participating in interagency information sharing, and using a multilayered approach to screening.

International Cooperation

To prevent terrorist travel we must work closely with our international partners—we must work bilaterally, regionally, and globally.

ICAO

In order to enhance global aviation security measures and standards following the attempted December 2009 attack, DHS initiated a broad international campaign to strengthen the global

aviation system against the evolving threats posed by terrorism. The first step of this campaign was to raise global awareness with key partners and allies.

Immediately following the thwarted attack, Secretary Napolitano and Deputy Secretary Lute contacted their Mexican, Canadian, and European counterparts to share information and solicit support for the need for aviation security enhancements worldwide. Subsequently, Deputy Secretary Lute and I traveled to meet with senior officials from 11 countries throughout the Middle East, Africa, Asia and Europe to lay the groundwork for improved aviation security standards.

In the weeks and months that followed, DHS worked with the International Civil Aviation Organization (ICAO) on an unprecedented initiative to strengthen global aviation against threats posed by terrorists, working in multilateral and bilateral contexts with governments as well as industry. Secretary Napolitano participated in regional aviation security summits in Spain, Mexico, Japan, Nigeria, and in the United Arab Emirates, helping to bring about historic consensus with the international community to strengthen the civil aviation system through enhanced information analysis and sharing, cooperation on technological development, and modernized aviation security standards.

These efforts culminated at the ICAO Triennial Assembly in October 2010, where the Assembly adopted the Declaration on Aviation Security, which forges a new foundation for aviation security to better protect the entire global aviation system. The extraordinary global collaboration demonstrated by nearly 190 countries during the ICAO General Assembly has helped to bring about a truly 21st century international aviation security framework that will help make air travel safer and more secure than ever before.

This is not to say that there won't be new threats, or that there will be a new level of security overnight. To the contrary, this effort is foundational, but also transformational, and will lay the groundwork for a strengthening of the entire system over the next several months and years. It includes and underscores, for example, the critical value of analyzing travel data such as passenger name record or 'PNR' data and sharing information with our international partners in order to identify both known and unknown individuals traveling for purposes of terrorist training or committing acts of terrorism. It re-affirms the importance of working closely with our allies to identify those individuals who pose a risk but have not, until now, come to the attention of law enforcement or intelligence agencies. Every day, DHS prevents individuals seeking to travel to the United States by employing a number of tools that provide for advance information collection and analysis to identify potential threats. This process, which is a tenet of our own security, is now also one that has been embraced internationally as a result of our work over the past year.

VWP

The *Implementing Recommendations of the 9/11 Commission Act* of 2007 made even more explicit the connection between security cooperation and the VWP. Designation as a VWP member country provides tremendous incentives for countries to maintain high security standards and deepen their cooperation with the United States on security-related issues. The

cooperation that the VWP engenders - entry into agreements to share lost and stolen passport data with the United States through INTERPOL; sharing security and law enforcement information with the United States; cooperation on repatriation matters; the strengthening of document security standards; and airport and aviation security - helps secure the United States and prevent terrorist and criminal activities within VWP member nations, while also helping to facilitate and spur exchanges—commercial, tourist, and others—that benefit our economy, as well.

Due to these security requirements, all VWP countries now report lost and stolen passports to INTERPOL. This achievement, which contributes to the decreasing use of fraudulently-obtained passports, is a milestone and has contributed to the overall decline of fraudulent document intercepts at the border from VWP countries, from 712 in FY2004 to 36 in FY2010. In addition, 17 European countries have signed Preventing and Combating Serious Crime Agreements with the United States to share information about serious crime and terrorism, and negotiations with several other countries are in the final stages. These agreements enable each side to query the fingerprint databases of the other side for law enforcement purposes and otherwise enable each side voluntarily to provide data about criminals and terrorists. Also, VWP countries are required to enter into agreements under Homeland Security Presidential Directive (HSPD) 6 with the United States regarding the systematic exchange of identifying information on known or suspected terrorists and encounter management procedures. The Department of State and the Terrorist Screening Center have negotiated 15 of these agreements with European countries, and others are currently being negotiated.

PNR

As mentioned earlier, DHS analysis of Passenger Name Record (PNR) information – the information provided to the air carrier when booking international travel - is an indispensible part of transportation security and the prevention of terrorist travel. PNR data analysis assists in the identification of watchlisted individuals up to 72 hours prior to departure. DHS is then able to use PNR data to link previously unknown terrorists and criminals to known terrorists or criminals. Uniquely, our analysis of PNR allows us to identify high-risk travelers who have not previously come to our attention by matching them against travel patterns known to have been used by terrorists. The value of this technique is increasingly recognized internationally with other nations deploying or developing their own PNR systems. For some in the European Union (EU), however, this system has raised privacy concerns. As a result, DHS has concluded a series of four negotiations with the EU in the last decade to provide and maintain a legally certain operating environment to the airlines and to reassure our partners that DHS handles their citizens' data appropriately. Our most recent negotiation with the European Commission was concluded on May 16, 2011. The text, which represents an enormous amount of progress in terms of enhancing security and improving data protection, underscores the United States and the EU's continuing commitment to combat terrorism and serious transnational crime, while respecting both privacy and security. It must now be approved by the Council of the European Union and ratified by the European Parliament. While data continues to be utilized in the meantime, DHS encourages these bodies to quickly approve the agreement so its enhanced provisions may take effect.

DHS has also worked with countries, including those in the Caribbean, to help them stand up passenger prescreening capabilities, focusing initially on Advance Passenger Information systems that will help them identify known illicit travelers.

North American Perimeter Security

DHS is also working to implement the President's February 2011 "Beyond the Border" declaration with Canadian Prime Minister Harper, which will strengthen North American security and make both Canada and the United States safer through a series of mutually beneficial initiatives. Specifically, we have jointly committed to taking a 'perimeter' approach to security in North America, and thus to collaborating to address threats well before they reach our shores, We will do so by developing a common understanding of the threat environment through improved intelligence and information sharing, as well as joint threat assessments to support informed risk management and targeting decisions. We will look for opportunities to integrate our efforts and where practicable, to work together to develop joint facilities and programs – within and beyond the United States and Canada – to increase efficiency and effectiveness for both security and trade. To increase travel security, counter fraud, and improve overall efficiency, we will also work together on an initiative to establish and verify the identities of travelers coming to North America and conduct screening at the earliest possible opportunity. This effort will include working toward common technical standards for the collection, transmission, and matching of biometrics that enable the sharing of information on travelers.

Capacity Building

In addition to screening travelers against derogatory information, it is important to ensure that officials also have the proper training and access to intelligence to detect fraudulent travel documents so that such documents cannot be used by terrorists seeking to subvert the screening process. The ICE Forensic Document Laboratory (FDL) is another tool in the arsenal against document fraud. The FDL is the federal government's only forensic crime laboratory dedicated exclusively to fraudulent document detection and deterrence. In partnership with the Department of State, the FDL provides training to international and domestic partners on identifying fraudulent documents.

DHS also works to implement significant programs around the world to provide training and technical assistance to build the capacity of foreign governments to confront terrorists, prevent terrorist movement, and strengthen our own security. DHS generally is not authorized to use its appropriated funds for foreign capacity-building purposes[1]; therefore, when our interests and priorities overlap, DHS works with the U.S. agencies that hold authority to fund foreign assistance, including capacity building efforts. These cooperative efforts to work with our international partners, and often to provide training and technical assistance, are based on where our assistance can help build a partner's capacity to combat terrorism. Some of these efforts

[1] There are a few exceptions for training the sharing of best practices by TSA in locations that have non-stop flights to the United States.

include: Border, Customs, and Immigration Police Training; Maritime Security and Seaport Interdiction; Civil Aviation Security and Reconstruction and Stabilization efforts.

Finally, DHS and the Department of State have worked with our closest allies to develop routine sharing of biometric information collected for immigration purposes. I will chair an initiative this year with the United Kingdom, Canada, Australia, and New Zealand that will build on these efforts and expand security and information sharing cooperation to mutually enhance travel security among our five countries. This type of cooperation, when implemented, can quickly reveal those who travel under multiple identities, or those who conceal their true identity in order to withhold pertinent information in an effort to obtain an immigration benefit. A new program that began in 2010, for example, which shares biometric information with the United Kingdom, Canada, Australia, and New Zealand, has identified many cases of routine immigration fraud, as well as dangerous people traveling under false identities.

As evidenced by this program, the information we gather and share with and from our international allies can be of great benefit. It also illustrates the importance of using all available resources to identify and prevent threats.

Intelligence and Information Sharing

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 techniques they use to avoid detection. This is done by collecting, maintaining, and updating data and integrating knowledge of terrorist travel patterns into our immigration and 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 threat.

Four unique centers across the federal government provide critical resources to the Department's ability to understand, anticipate, and thwart terrorist travel. They have distinct areas of expertise and each serves a vital function for DHS. They are the Terrorist Screening Center, the National Counterterrorism Center, the National Targeting Center, and the Human Smuggling and Trafficking Center.

The Terrorist Screening Center (TSC), administered by the FBI, maintains the TSDB and provides information needed to help identify persons known to be, or reasonably suspected of being, associated with terrorism (referred to as "KSTs"). The terrorist watchlisting process incorporates biographic and biometric identifiers to support immigration and border screening. As an example, the TSDB maintains photographs of KSTs and makes this information available to the Department of State for screening visa applications. The broad range of terrorist watchlist information available and the ability to securely deliver it to the front line screening agency, overseas, at the border, or within the United States is a major improvement to the processes in place prior to 9/11.

The National Counterterrorism Center (NCTC), by law, serves as the primary organization with the U.S. government for analyzing and integrating intelligence pertaining to terrorism and counterterrorism. Reporting to the Director for National Intelligence (DNI), it also serves as the central repository on KSTs and international terrorist groups. 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.

The National Targeting Center (NTC), run by CBP, provides 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 platform used by CBP 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.

The Human Smuggling and Trafficking Center (HSTC) combats illicit and terrorist travel by bringing 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; and
- Working with, and exchanging information with allied foreign governments and organizations.

ICE Homeland Security Investigations (HSI) plays a lead role in the U.S. government's attempt to identify, disrupt and dismantle foreign-based human smuggling organizations that pose a threat to U.S. security interests. It co-chairs a highly successful targeting project under the auspices of the Interagency Working Group on Alien Smuggling and Trafficking that identifies and prioritizes law enforcement action against the most dangerous smuggling organizations. In partnership with the Criminal Division of the U.S Department of Justice, HSI provides direct operational support under the Extraterritorial Criminal Travel Strike Force (ECT) program for the investigation and prosecution of these targets.

Layered Approach to Screening

As I mentioned earlier, 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.

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 (e.g., name, passport number); and third, a way for innocent travelers incorrectly caught in the system to seek correction and redress.

DHS reviews the traveler's identity information and travel practices through six reinforcing systems:

a. The visa application process, for which DHS provides vital support to the Department of State.
b. ESTA, which determines eligibility of a person for travel under the Visa Waiver Program.
c. The Advance Passenger Information System (APIS), which allows CBP to compare the traveler manifest of commercial and private aircraft, as well as commercial vessels, against law enforcement databases, including the TSDB.
d. Secure Flight, which compares passenger information to the No Fly and Selectee List components of the TSDB.
e. PNR data, which analyzes information from the carriers' reservation systems to detect links to KSTs or patterns of criminal or terrorist activity.
f. The refugee application process through which DHS checks a myriad of systems in order to detect links to criminal or terrorist activity.

DHS obtains this information and begins conducting screening before an aircraft's departure. Combined, APIS and PNR data have assisted CBP in the identification of over 5,000 KSTs per year. These passengers were denied boarding, received enhanced security screening, or were removed from the watchlists after it was determined that they no longer posed a threat.

Additional Screening Mechanisms Used by the Department

A critical innovation of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. No. 110-53) (9/11 Act) was the requirement for the development and implementation of an electronic system for travel authorization (ESTA) to determine in advance of travel the traveler's eligibility for VWP travel. ESTA was launched by DHS in August 2008 and, screens prospective VWP travelers against several databases, including the terrorist watchlist; lost and stolen passports (including INTERPOL's Stolen and Lost Travel Documents database); visa revocations; previous VWP refusals; and public health records. Since January 2009, nationals from all VWP countries, regardless of their port of embarkation, have been required to obtain an approved travel authorization via ESTA prior to boarding a carrier to travel by air or sea to the United States under the VWP.

DHS's U.S. Visitor and Immigration Status Indicator Technology (US-VISIT) program and the Automated Biometric Identification System (IDENT) database of biometric holdings support the Department'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. Upon arrival at a port of entry, alien travelers provide biometric data including fingerprints which are screened through

the DHS IDENT biometric watchlist, and also matched with previous biometric data collected from the person, such as during a visa application, to verify the person's identity.

DHS is committed to conducting rigorous screening in order to ensure that those being admitted to the United States, including those through the refugee program, are not seeking to harm the United States. Refugees legitimately are without documents that are needed to prove their identity. The Department has instituted rigorous screening methods to mitigate this vulnerability. In May 2007, DHS announced and implemented an Administration-coordinated, enhanced background and security check process for Iraqi refugees applying for resettlement in the United States. The security check regime, including both biographic and biometric checks, has been enhanced over the last several years as new opportunities and interagency partnerships with the law enforcement and intelligence communities have been identified. These enhancements are a reflection of the commitment of DHS and other agencies to conduct the most thorough checks possible to prevent dangerous individuals from gaining access to the United States through the refugee program. The latest enhancement to the refugee security check regime involves a new "pre-departure" check shortly before refugees are scheduled to travel to the United States. It is intended to identify whether any new derogatory information exists since the initial checks were conducted. These pre-departure checks went into effect in late 2010. No case is finally approved until results from all security checks have been received and analyzed.

As these enhancements which were initially designed for high risk refugee applicants have been implemented and proven valuable in identifying bad actors seeking to exploit our nation's immigration system, DHS has worked both internally and with our interagency partners—including the State Department and Intelligence Community—to expand these checks to certain other individuals seeking to travel or emigrate to the United States.

Enhancing background vetting for immigration benefits is an ongoing process. We are continuing to work with agencies that have potentially relevant data to determine whether and how to incorporate this information into the existing security check protocols for refugee applicants and others seeking immigration benefits or travel to the United States.

Conclusion

This nation has taken significant steps to counter and prevent terrorist travel since 9/11. They entail a multi-layered, many-faceted, and multinational effort that weaves together intelligence, information-sharing, security and law enforcement programs from across DHS, the interagency, and across a multitude of partnerships with our international and domestic partners. Together they reflect one of our nation's most pressing priorities: to ensure the safe and secure movement of literally millions of people traveling to, from, and around the United States on a daily basis, while thwarting the few would-be terrorists who seek us harm, at the earliest point in their journey.

Thank you again for this opportunity to testify. I look forward to answering any questions you may have.