WRITTEN TESTIMONY OF KELLI ANN WALTHER
SENIOR DIRECTOR FOR SCREENING COORDINATION
OFFICE OF POLICY
THE
U. S. DEPARTMENT OF HOMELAND SECURITY
BEFORE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY
Eleven Years After 9/11: Preventing Terrorist Travel

SEPTEMBER 11, 2012
WASHINGTON, DC

Introduction

Good morning Chairman Miller, Ranking Member Cuellar, and distinguished Members of the Subcommittee. Thank you for the opportunity to appear before the Subcommittee to highlight the Department of Homeland Security's (DHS) work in preventing terrorist travel.

Eleven years ago, screening of passengers coming to the United States was limited to the Department of State (DOS) visa process, if applicable, the inspection of a person by an immigration officer at the port of entry, and processes applied at foreign airports 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, or from aliens seeking admission to the United States. There was limited pre-departure screening of passengers seeking to fly to the United States, virtually no screening of any kind for domestic flights beyond the security checkpoint, and no advance vetting of passengers seeking admission under the Visa Waiver Program (VWP). 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. As the 9/11 Commission pointed out, targeting terrorist travel is one of the most powerful weapons we have to counter terrorist operations. One of the key aspects of the DHS approach is to identify persons that may pose a risk to U.S. citizens or whose entry may violate U.S. law, before they reach the United States.

DHS works to track known threats, while utilizing intelligence-based advanced targeting techniques to help mitigate and identify unknown threats. For example, DHS uses the U.S. Government's consolidated terrorist watchlist and other information derived from investigations and intelligence assets to identify individuals with known or suspected ties to terrorism and other potential threats to the United States. In addition, DHS relies on domestic and international criminal records (e.g., investigative case files domestically and INTERPOL notices internationally) to identify potential criminal movements. Travel data is also compared against passport, visa, and immigration data to determine if travelers are admissible or can enter the United States. Moreover, DHS implements rigorous physical security requirements both in the form of airport checkpoint and airline security standards, as well as physical detection methodologies (e.g., drug sniffing canines) at ports of entry.

Identifying travelers through a risk-based approach remains the foundation of the DHS model today, and in a more comprehensive and sophisticated form than ever before. With the advent of better information technology within government and the transportation industry, DHS has been able to apply this methodology across the life-cycle of a traveler's journey.

DHS's Multi-Layered Approach to Security

Since 9/11, the travel threat has evolved to include not only large-scale attacks, but also smaller operations with potentially catastrophic effects. Our approach employs multiple layers of security measures throughout the travel continuum that are closely coordinated with other U.S. Government counterterrorism, law enforcement, and public security authorities and with state, local, tribal, territorial, and foreign partners and the transportation industry. To support these efforts, DHS collects biographic and biometric data for vetting and screening against various databases to track known threats and better identify and mitigate unknown threats.

This multi-layered approach allows DHS to improve security and to minimize the likelihood that any single measure becomes a single point of failure.

Enhancements Since December 25, 2009
Since the attempted bombing of a commercial aircraft on December 25, 2009, DHS, in coordination with other departments and agencies, has worked to address issues and potential gaps to ensure that we have a comprehensive and multilayered approach that focuses on stopping terrorists at the earliest possible opportunity. As represented by the other officials who have been asked to testify today, we can see that addressing this issue requires significant collaboration and coordination among federal agencies.

Our efforts are not all directed at one area of the travel continuum—but rather are part of our layered approach to strengthen security. Working in concert with other U.S. agencies, DHS has strengthened security, law enforcement, and screening at several points in the travel process:

- 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 a commercial carrier or vessel;
- Upon arrival at a port of entry, when a traveler seeks admission into the United States;
- During the period of stay in the United States, when a non-U.S. person travels by air within the United States; and
- Upon departure, when a traveler leaves the United States.

DHS, in cooperation with commercial carriers and vessels, reviews information about travelers, including their identity and travel documents, prior to arrival at a U.S. port of entry. The traveler establishes his or her identity through the provision of biographic and biometric data, which is confirmed at various points in the travel continuum.

Screening in the Travel Planning Phase
This layer of defense consists of deploying safeguards to prevent dangerous individuals from obtaining visas and travel authorizations. To enter the United States, most foreign nationals are required to either obtain a visa issued by a U.S. embassy or consulate or, for citizens or nationals of a Visa Waiver Program (VWP) country[1], obtain a travel authorization via the Electronic System for Travel Authorization (ESTA). Visa applicants are required to provide biometric (fingerprint and digital photo) and biographic data. The applicant's information is checked against the biometric and biographic databases of DHS, DOS, and the Federal Bureau of Investigation. In most instances, individuals must also appear in-person for an interview with a consular official.

DHS is continually working with interagency stakeholders to improve procedures for vetting immigrant and nonimmigrant visa applicants, asylum applicants, 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, asylum applicants, refugees, and those seeking to enter the United States at a port of entry, are subject to rigorous background vetting, biographic and biometric checks. The security 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.

[1] The 36 countries currently designated for participation in the Visa Waiver Program include: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

By continuously vetting all issued U.S. non-immigrant visas against law enforcement data, changes in a traveler's eligibility are identified by DHS in near real-time, allowing DHS to submit timely "no-board" recommendations to carriers, visa revocation requests to DOS, or notifications to other law enforcement agencies in situations where the individual is physically present in the United States.

In an effort to identify potential terrorists and criminals before they obtain a visa to travel to the United States, DHS has 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. The VSP is currently deployed to 19 posts in 15 countries. As part of this program, 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. As of July 31, 2012, the VSP has screened over 1.1 million visa applicants against information held by DHS.

In support of ICE VSP efforts to enhance visa security measures, representatives from DHS, ICE, U.S. Customs and Border Protection (CBP) and DOS have agreed to develop an automated visa screening process that will enable DHS entities to identify derogatory information relating to applicants prior to the visa application being submitted to a Consular Officer. This process will inform and be used in conjunction with the current DOS Security Advisory Opinion (SAO) and Advisory Opinion (AO) programs. Additionally, DHS, DOS, and the Intelligence Community are working to establish a process to screen all visa applications against intelligence information provided by the interagency prior to visa issuance.

Visa Waiver Program

The VWP encourages high security standards and helps facilitate cooperation on security-related issues, including sharing security and law enforcement information, cooperating on repatriation matters, adhering to higher standards for aviation security, and strengthening document security standards. At the same time, the VWP facilitates exchanges—commercial, tourist, and others—that are essential to our economy. According to the Commerce Department, international tourism supported 1.2 million U.S. jobs last year, and tourism revenue in early 2012 was up 14% from the previous year. The VWP is an essential driver of international tourism because it allows eligible nationals of 36 countries to travel to the United States without a visa and remain in our country for up to 90 days. Over 60% of overseas travelers that come to the United States are from VWP countries.

DHS has focused on bringing VWP countries into compliance with the information sharing agreement requirements of *The Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), Pub. L. No.110-53. As of January 2012, all VWP countries have completed an exchange of diplomatic notes or an equivalent mechanism for the requirement to enter into an agreement to share information on lost and stolen passports with the United States through INTERPOL or other designated means. DHS, in collaboration with the Department of Justice (DOJ), has also concluded Preventing and Combating Serious Crime (PCSC) agreements, or their equivalent, with 35 VWP countries and two VWP aspirants. DHS, along with DOJ and DOS, continues to work closely with the remaining country to sign a PCSC agreement. These agreements enable each side to query the fingerprint databases of the other side for law enforcement purposes and enable the sharing of data about criminals and terrorists. Also, the U.S. government has concluded negotiations on arrangements with all VWP countries for the exchange of terrorism screening information.

In addition, nationals from all VWP countries, regardless of their port of embarkation, are required to obtain an approved travel authorization via ESTA prior to boarding a carrier to travel by air or sea to the United States. ESTA vets prospective VWP travelers against several databases, including the terrorist watchlist, lost and stolen passports (including INTERPOL Stolen and Lost Travel Documents), visa revocations, and previous VWP refusals.

DHS supports the carefully managed expansion of the VWP to countries that meet the statutory requirements, and are willing and able to enter into a close security relationship with the United States. To this end, we support current bi-partisan efforts by the Congress to expand VWP participation and to promote international travel and tourism to the United States while maintaining our strong commitment to security. Additionally, as part of the President's recent Executive Order (13597), we are working with partner countries to meet existing requirements and prepare for further expansion of the VWP.

Refugee Vetting
DHS is committed to conducting rigorous checks in order to ensure that individuals admitted to the United States, including those through the refugee program, do not threaten our security. Refugees often lack, for legitimate reasons, valid documents that establish their identity. The Department has instituted rigorous 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.

DHS has enhanced this security check regime, including both biographic and biometric checks, over the last several years as new opportunities and interagency partnerships with the law enforcement and intelligence communities have been identified. 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. No case is approved until results from all security checks have been received and analyzed.

Screening Prior to Boarding/Departure
The next layer of defense for air travel includes information-based and physical screening prior to a traveler boarding an aircraft. In partnership with the airline industry and foreign governments, the U.S. government conducts passenger manifest screening and vetting prior to air travel to identify known threats. Passenger and crew manifest screening and vetting are also conducted for commercial vessels in the maritime environment. In addition, physical screening of all air passengers and their baggage is conducted at airport checkpoints.

The actions resulting from inclusion on the No Fly, Selectee, or Expanded Selectee list are generally as follows:

- No Fly matches are prohibited from boarding an aircraft;
- Selectee matches undergo enhanced screening prior to boarding an aircraft; and
- Expanded Selectee matches undergo enhanced screening prior to boarding an aircraft.

Advance Passenger Information System (APIS) and Passenger Name Record (PNR) Data
DHS use of APIS and PNR data has assisted CBP in the positive identification of over 4,000 persons with ties to terrorism in FY 2011.

DHS analysis of PNR information – the information provided to the air carrier when booking international travel—is an indispensable tool for the prevention of terrorist travel. PNR analysis assists in the identification of watchlisted and other high risk individuals up to 96 hours in the maritime environment and 72 hours in the air environment prior to departure.

DHS also uses PNR data to link previously unknown terrorists and criminals to known terrorists or criminals, and identify high-risk travelers by matching them against travel patterns known to have been used by terrorists or other intelligence-based scenarios.

DHS identifies travel patterns and other information to develop targeting rules from intelligence information. These rules are reviewed quarterly by CBP, the DHS Privacy Office, the DHS Office of Civil Rights and Civil Liberties (CRCL), and the Office of the General Counsel. Additionally, the DHS Chief Privacy Officer conducts privacy compliance reviews of the DHS use of PNR and reports the findings to Congress.

APIS data —essentially the flight or ship passenger and crew manifest for a given flight or voyage— contains information such as a traveler's date of birth, citizenship, and travel document number, which is typically collected as passengers check in for their flight or voyage.

Pre-departure Screening
DHS utilizes the Immigration Advisory Program (IAP), at 11 airports in nine countries, to conduct additional screening for high-risk and improperly documented travelers, by using targeting and passenger analysis information. At the invitation of foreign partners, IAP officers can make "no-board" recommendations to airlines for travelers who may present security risks or lack necessary travel documents. This partnership has also benefited air carriers, as it saves them time and the cost of transporting individuals denied entry to the United States back to their port of embarkation. Through direct networks with commercial airlines and connections to CBP officers overseas as part of the IAP, National Targeting Center (NTC) officials are able to issue no-board recommendations to the airline to keep suspected high-risk passengers from traveling to the United States. In FY 2012, to date, there have been more than 3,663 "no-board" recommendations.

Maritime Environment
As the lead DHS agency for maritime homeland security, the U.S. Coast Guard screens all commercial vessel passenger and crew manifests against intelligence holdings and law enforcement data sets. This screening is conducted through the vessel's submission of an Advanced Notice of Arrival (ANOA) up to 96 hours (but no less than 24 hours) prior to arrival at a U.S. port. In 2011, 28.5 million people and over 121,000 ship arrivals were screened, and 120 advance warning reports were generated regarding arriving ships, people, or cargo posing a potential threat.

Checkpoint Screening
DHS employs measures both seen and unseen by travelers, including walk-through metal detectors, explosive trace detection equipment, trained canines, vapor trace machines that detect liquid explosives, full-body pat-downs, and behavior detection officers—both at and beyond the checkpoint. Advanced Imaging Technology (AIT) machines are also employed to screen passengers for metallic and non-metallic threats that cannot be detected by walk-through metal detectors. DHS has also strengthened the presence and capacity of law enforcement to prevent terrorist attacks on commercial aviation.

DHS has increased Federal Air Marshal Service (FAMS) coverage of U.S.-flag carriers' international flights. 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.

Inspection at a Port of Entry

All travelers to the United States, regardless of the means by which they arrive (land, sea, or air), must present valid travel and identity documents in order to obtain admission. Upon arrival at a port of entry, a traveler presents his or her secure travel document (i.e., passport) and visa (if required) or other appropriate travel authorization. The CBP officer will conduct information-based checks against federal databases, and, when applicable, will collect biometrics (including fingerprints) to vet them against the DHS Automated Biometric Identification System (IDENT). IDENT will match biometric data previously collected from the traveler, such as during the visa application or a past visit to the United States, to verify the person's identity. Travelers may also undergo a secondary inspection prior to an admissibility determination.

IDENT enables DHS to store and analyze biometric data—digital fingerprints and photographs—and then link that data with biographic information to establish and verify identities; IDENT contains biometric data on known and suspected terrorists, criminals, and immigration violators, and aids in distinguishing potential threats from bona fide travelers. "Anchoring" an identity on the first encounter—usually with the collection of biometrics through the visa and entry processes—helps prevent misidentifications and dramatically reduces the ability of individuals to use fraudulent identities on subsequent encounters.

Western Hemisphere Travel Initiative

DHS continues to balance the need to prevent terrorist travel with the need to facilitate the legitimate travel of known individuals. The Western Hemisphere Travel Initiative (WHTI), implemented for air travel in 2007 and travel by land and sea in 2009, requires all travelers – U.S. citizens and aliens alike – to present a passport or another acceptable secure document denoting identity and citizenship for entry into the United States. WHTI also expanded the use of radio frequency identification (RFID) technology to efficiently balance security needs and facilitation of legitimate trade and travel, resulting in an almost five-fold increase in RFID-enabled documents in two years. In addition to a decrease in counterfeit documents, and altered documents, WHTI has contributed to reduced wait times at ports of entry through Ready Lanes, which expedite the travel of individuals possessing WHTI-compliant and RFID-enabled documents.

Global Entry

In an effort to ensure security while facilitating legitimate trade and travel, DHS has also expanded Global Entry, which allows pre-approved, low-risk travelers expedited inspection at select airports. More than one million trusted traveler program members are able to use the Global Entry kiosks, and we are expanding the program both domestically and internationally as part of the Administration's efforts to foster increased travel and tourism.

In addition to U.S. citizens and Lawful Permanent Residents, Mexican nationals can now enroll in Global Entry, and Global Entry's benefits are also available to Dutch citizens enrolled in the Privium program; South Korean citizens enrolled in the Smart Entry Service program; Canadian citizens and residents through the NEXUS program; and citizens of the United Kingdom, Germany, and Qatar through limited pilot programs. In addition, we have signed agreements with Australia, New Zealand, Panama, and Israel to allow their qualifying citizens and permanent residents to participate

in Global Entry. Global Entry applicants, like applicants for DHS's other Trusted Traveler programs (i.e., NEXUS, SENTRI, and FAST) are vetted against criminal and terrorist databases, and provide biometrics prior to acceptance into the program.

Screening within the United States

Foreign visitors to the United States may undergo additional screening while in the United States for a variety of reasons, including if the visitor chooses additional domestic travel.

Secure Flight

In November 2010, DHS achieved a major aviation security milestone by assuming responsibility from the airlines for terrorist watchlist screening for 100 percent of aircraft operators covered by the Secure Flight Final Rule for flights into, out of, and within the United States. This year, DHS expanded the program to include overflights (i.e., flights that pass over but do not land in the United States) by requiring all Foreign Air Carriers to report Secure Flight passenger data for covered flights. Transportation Security Administration (TSA) continues to work with foreign air carriers to ensure compliance of this requirement. In addition to facilitating secure travel for all passengers, Secure Flight helps prevent the misidentification of passengers who have names similar to individuals on government data sets.

DHS revised the Secure Flight program to screen passengers against all records on the Terrorist Screening Database (TSDB) that contain a full name and a full date of birth (not just the No Fly and Selectee lists); travelers identified under this new initiative are designated for enhanced physical screening prior to boarding an aircraft.

DHS uses a passenger's name, date of birth, and gender to vet airline passengers against terrorist information up to 72 hours before those passengers are permitted to board planes. Passengers who are potential matches are immediately identified by DHS for appropriate notifications and coordination with our federal partners.

Secure Flight screens more than 14 million passenger reservations against terrorist information each week. Approximately 25 individuals per month are denied boarding under the Secure Flight program.

TSA Pre✓™

DHS has worked to develop a strategy for enhanced use of intelligence and other information to support a more risk-based approach in all facets of transportation security. TSA Pre✓™ is part of the Department's ongoing effort to implement risk-based security concepts that enhance security by focusing on travelers DHS knows least about. More than two million passengers have received expedited screening through TSA Pre✓™ security lanes since the initiative began last fall. TSA Pre✓™ is now available in 22 airports for select U.S. citizens traveling domestically on Alaska Airlines, American Airlines, Delta Air Lines, United Airlines and US Airways, and members of CBP's Trusted Traveler programs. TSA expanded TSA Pre✓™ benefits to U.S. military active duty members traveling through Ronald Reagan Washington National and Seattle-Tacoma International airports. In addition to TSA Pre✓™, TSA has implemented other risk-based security measures including modified screening procedures for passengers 12 and younger and 75 and older.

As always, DHS will continue to incorporate random and unpredictable security measures throughout the security process, and at no point are TSA Pre✓™ travelers guaranteed expedited screening.

Screening upon Departure

Over the past year, we have worked to better detect and deter those who overstay their lawful period of admission. These efforts, and DHS's overall approach is documented extensively in the comprehensive biometric air exit plan submitted to Congress this past spring. The ability to identify and sanction overstays is linked to our ability to determine who has arrived and departed from the United States. By matching arrival and departure records, and analyzing entry and exit records stored in our systems and using additional data collected by DHS, we can better determine who has overstayed their lawful period of admission.

In May 2011, DHS began a coordinated effort to vet all potential overstay records against Intelligence Community and DHS holdings for national security and public safety concerns. Using those parameters, we reviewed the backlog of 1.6 million overstay leads in the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program and referred leads based on national security and public safety priorities to ICE for further investigation.

Through limited automated means, DHS cross-referenced additional overstay leads with DHS location and immigration holdings, closing additional records by confirming changes in immigration information or travel history that had not yet been recorded. Previously, these records would not have been examined, except in instances when resources allowed. Now, we are vetting all overstays for public safety and national security concerns, and DHS is also conducting automated reviews for changes in immigration status or travel history. This is performed on a recurrent basis.

In July, following the submission of the comprehensive air exit plan, Congress approved DHS to continue improvements related to identifying individuals who may have overstayed their lawful period of admission. DHS is implementing elements, and expects to have these enhancements in place by early 2013. Once completed, this initiative will significantly strengthen our existing capability to identify and target for enforcement action those who have overstayed their authorized period of admission, and who represent a public safety and/or national security threat by incorporating data contained within law enforcement, military, and intelligence repositories.

This strategy also will also enhance our ability to identify individual overstays; provide DOS with information to support visa revocation; prohibit future VWP travel for those who overstay; execute "lookouts" for individuals who overstay, in accordance with existing Federal laws; establish greater efficiencies to the VWP; and enhance the core components of an entry-exit and overstay program.

Concurrently, the Department's Science and Technology Directorate (S&T) is working to establish criteria and promote research for emerging technologies that would provide the ability to capture biometrics and develop a biometric exit capability at a significantly lower operational cost than is currently available. S&T is collaborating with the National Institute of Standards and Technology (NIST) on this initiative.

Last, as part of the Beyond the Border Action Plan signed by President Obama and Canadian Prime Minister Harper in December 2011, we are creating an exit program on the United States northern border. In accordance with the Action Plan, the United States and Canada will exchange entry records so that an entry to one country essentially becomes an exit record from the other country.

Overall, these elements constitute DHS's comprehensive approach to biometric exit implementation.

Building Bridges: International Partnerships and Information Sharing
DHS works closely with international partners, including foreign governments, major multilateral organizations, and global businesses, to strengthen the security of the networks of global trade and travel, upon which our nation's economy and communities rely. Today, DHS is in just about every corner of the world, with 11 Components and over 1,400 personnel stationed in more than 75 countries.

Perimeter Security
DHS is 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 and economic competitiveness in North America, and thus to collaborating to address threats well before they reach our shores. To address threats early, the United States and Canada are improving our intelligence and information sharing, and developing joint and parallel threat assessments in order to support informed risk management decisions. We also are enhancing our efforts to identify and screen travelers at the earliest point possible, with a common approach, including biometrics. Specifically, we are working toward common technical standards for the collection, transmission, and matching of biometrics that enable the sharing of traveler information.

DHS and DOS have worked with our closest allies to develop routine sharing of biometric information collected for immigration purposes. Last year, DHS chaired an initiative with Australia, Canada, New Zealand, and the United Kingdom to build on these efforts and expand security and information sharing cooperation to mutually enhance travel security among these five countries. A program that began in 2010, which shares biometric information with Australia, Canada, New Zealand, and the United Kingdom, has identified cases of routine immigration fraud, as well as dangerous people traveling under false identities.

Intelligence and Information Sharing
A critical step to thwarting terrorist operations along travel pathways 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 inspection systems and operations. DHS has created a standing intra-departmental working group to facilitate the sharing of DHS travel data with the Intelligence Community. The DHS Privacy Office and CRCL are key participants in the working group.

Since 9/11, the federal government has improved the sharing of information and intelligence among stakeholders. Several organizations within DHS provide critical resources to the Department's ability to understand, anticipate, and thwart terrorist travel.

CBP's National Targeting Center (NTC) 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 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).

DHS implements programs around the world to provide training and technical assistance to build the capacity of foreign governments to counter terrorism activity, prevent terrorist movement, and strengthen the security of the United States. It is imperative that officials 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 the U.S. government's only forensic crime laboratory dedicated exclusively to fraudulent document detection and deterrence. The FDL also provides training to international and domestic partners on identifying fraudulent documents.

Redress

With all of these efforts, DHS is deliberate in its effort to give travelers an opportunity to be heard when an issue arises. The Department has established the DHS Traveler Redress Inquiry Program (DHS TRIP), a single point of contact for individuals, regardless of citizenship, who have inquiries or seek resolution of difficulties they experience during travel, including: denied or delayed airline boarding; denied or delayed entry into and/or exit from the United States; or frequent referral for additional screening. Individuals who complete the redress process are issued a redress number that can be used to book travel to prevent misidentifications.

Privacy, Civil Rights, and Civil Liberties

Protecting privacy, civil rights, and civil liberties is a core mission of DHS. DHS has the first statutorily required privacy office of any federal agency, as well as a senior official responsible for civil rights and civil liberties. DHS builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development.

Both the DHS Privacy Office and CRCL partner with every DHS component to assess policies, programs, systems, technologies, and rule-makings for privacy and civil liberties risks, and recommends appropriate protections and methods for handling personally identifiable information in accordance with the Constitution, the Privacy Act, and the Fair Information Practice Principles. At DHS we work hard to create an environment where privacy, civil rights and civil liberties and security go hand in hand, helping to secure our nation while honoring the principles on which the country was founded.

Conclusion

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. We must utilize a multi-layered, many-faceted, and multinational effort that weaves together intelligence, information-sharing, security and law enforcement programs from 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: the facilitation of legitimate travel and commerce while thwarting threats, and simultaneously protecting privacy and civil liberties.

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