TESTIMONY OF PAUL S. ROSENZWEIG
COUNSELOR TO THE ASSISTANT SECRETARY FOR POLICY
AND
JAYSON P. AHERN
ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY
BEFORE
THE SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY

Chairman Kyl, Ranking Member Feinstein, and other distinguished Members of the Subcommittee, we are pleased to join you this afternoon to discuss the ongoing efforts of the Department of Homeland Security (DHS) to prevent terrorists from both entering the United States and posing a threat to international air travel.

DHS was born in the aftermath of the most horrific terrorist attack on the United States and the aviation system in history. "Keeping terrorists off the plane," both at home and abroad, has been a central priority for the Department. This is why both air travel and how we vet arriving travelers have changed fundamentally.

The recently dismantled plot to blow up aircraft en route to the United States from Britain reinforces the severity and the importance of our challenge. It reminds us not only that terrorists remain intent on targeting air travel, but of the importance of a layered approach to security, an approach that is supported by close interagency and international cooperation. It's instructive to recall that what could have been the second largest terrorist attack on aviation was disrupted far from the airport. Nonetheless, it was aviation security officials in the United States and London who cooperatively responded to the new environment that investigators presented to them.

Integration of efforts and cooperation with allies are at the forefront of DHS's strategy to identify and interdict those who would do us harm before they can board an aircraft for the United States. Our efforts begin well before the airport, and include both the visa issuance process and decisions to exempt travelers from certain countries from that process. Our efforts continue in the days and weeks leading up to the departure of an aircraft as we receive critical data about the flight, assess it, and, in some cases, alert U.S. Customs and Border Protection (CBP) officers stationed oversees to work with their counterparts to further vet and interdict high risk travelers. This entire process is further supported by the work of Customs and Border Protection and the Transportation Security Administration (TSA) – in partnership with foreign governments, air carriers, and airports – to ensure that passengers and their baggage are properly screened before boarding an aircraft departing for the United States.

We'd like to take a few moments to update you on some of the most critical programs that support our layered-security approach, including the Visa Waiver Program (VWP), our use of Advance Passenger Information and Passenger Name Records to prescreen travelers, and overseas activities to support point of departure screening.

First, DHS is committed to further strengthening the Visa Waiver Program's security features. With almost 16 million people entering the U.S. under this program each year – a number that represents more than one-half of all non-immigrant admissions (excluding those from Canada and Mexico) – the VWP is at the forefront of our efforts to facilitate international travel. It is also at the forefront of our efforts to defend against those from VWP countries who seek to abuse America's welcoming nature.

Originally established in 1986, the VWP allows citizens of designated countries – of which there are currently 27 – to travel to the United States for business or pleasure for up to 90 days without a visa. By permitting qualified low-risk countries to join or remain part of this program, the United States has promoted better relations with allies, eliminated unnecessary barriers to travel, stimulated the tourist industry, allowed U.S. consular offices to focus on higher priority visa screening, and encouraged international cooperation against organized crime, trafficking in persons, drug smuggling, and terrorism.

DHS has used the Visa Waiver Program's existing procedures to set strict security standards for member countries, as well as to enforce milestones for their completion. This is done through frequent assessments on the ability of the 27 VWP countries to meet a host of security guidelines that are constantly being strengthened. Because a passport is the sole document a citizen from a VWP country must have to enter the United States, we must ensure that passports issued by VWP countries meet the most exacting security standards. Accordingly, all VWP country passports issued after October 25th of this year must be "e-passports," which contain a chip to store the user's biometric and biographic information. This change incrementally builds off of an already strict standard instituted last October that requires VWP passports issued after that date to include a digital photo, be machine-readable, and be tamper-resistant. In addition, all VWP travelers were enrolled into the US-VISIT program – which collects fingerprints and photographs from visitors to the United States – as of September, 2004. Combined, these features will make it very difficult for anyone other than the official holder of the passport to enter this country.

As the Subcommittee knows, the Government Accountability Office recently issued several reports on DHS's administration of the VWP. DHS appreciates GAO's continued support for this vital program and its recommendations for improving it. In fact, DHS already has addressed many of the issues GAO identified. For instance, GAO recommends a clear standard operating procedure for the reporting of lost and stolen passport data from foreign governments to the U.S. The Office of International Enforcement already has developed and cleared standards to implement such a policy. Those standards include timely reporting, procedures for reporting, and improved distribution for U.S. officials who need access to such information. Further, DHS is working closely with Interpol to ensure that, as part of the pre-departure screening process, all travelers' passport information vetted against Interpol's lost and stolen travel document database, which contains nearly 12 million records.

Since 2004, the Office of International Enforcement improved the country review process – a review that each VWP country must undergo every two years to determine its continued participation in the program. For instance, we have developed new standard operating procedures for the review, implemented a training program for the country review teams, and

streamlined the review process to target the issues of greatest concern to the U.S. We may also develop a continuous review process that would be more targeted and effective than the "rear view mirror" approach that we currently take every two years.

While the Visa Waiver Program is an important tool in the war on terrorism, there is room for improvement. The existing VWP assesses risks to the United States on a country-by-country basis; the law assumes that a citizen who hails from, say, Britain, poses no threat to the American people. That sort of assumption is no longer sound. The Visa Waiver Program also needs to look for risks on a traveler-by-traveler basis. The Department looks forward to working with Congress to further enhance the VWP's security features as new countries are considered for admission into the program.

Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate *bona fide* travelers so it can focus its resources on areas of highest risk.

The Advance Passenger Information System (APIS) was developed in 1988 in cooperation with the airline industry. At that time, air and sea carriers voluntarily collected passenger and crew biographical data – typically information that would be on the aircraft manifest or the individual's passport – and transmitted this data to the United States Government while the vessel or aircraft was en route to this country.

Current CBP regulations require that an air carrier must electronically transmit passenger arrival manifests to CBP no later than 15 minutes after the departure of the aircraft from a foreign port; carriers also have to electronically transmit passenger departure manifests no later than 15 minutes prior to departure of the aircraft from the U.S. port of departure. Manifests for crew members (on passenger and all-cargo flights) and non-crew members (limited to all-cargo flights) must be electronically transmitted to CBP 60 minutes prior to the departure of any covered flight from a foreign port and 60 minutes prior to the departure of any covered flight from the U.S. port of departure. (A "covered flight" is one to, from, continuing within, or overflying the United States.) Sea carriers are similarly regulated, but with different timeframes for the transmission of the manifest data.

Shortly after the September 11 atrocities, DHS recognized the need to have APIS information provided in advance of an aircraft's departure. Without knowing exactly who is on board an aircraft prior to its departure, our ability to prevent hijackings or suicide attacks is greatly inhibited. Congress saw the need, as well and codified this principle in section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004. As a result, after extensive consultations with our international partners, DHS on July 14, 2006 published the pre-departure Notice of Proposed Rule Making. After evaluating several alternative approaches, the proposed rule offers two options for carriers to transmit passenger data to DHS, in a manner sufficient to allow DHS to screen all passengers prior to the departure. Specifically, air carriers could transmit complete manifests no later than 60 minutes prior to departure. Or they could transmit passenger data as individual, real-time transactions as each traveler checks in, up to but no later than 15 minutes prior to departure. The proposed rule also recommends changing the definition of "departure," as set forth in 19 C.F.R. § 122.49a, to mean "from the moment at which the aircraft is pushed back from the gate."

If the rule is finalized and implemented as proposed – the comment period will close on October 12 of this year – the United States Government would take on the watch list screening responsibility for all travelers arriving into or departing from the United States aboard a commercial aircraft or vessel. This would eliminate the current responsibility of carriers flying into the United States to check the No Fly and selectee lists. It also would bring greater control over this process into government hands.

The information available from Passenger Name Records (PNR) is distinct from, but every bit as important as, Advance Passenger Information. PNR is information contained in an air carrier's electronic reservation system and/or departure control system that describes the identity and travel plans of a passenger or group of passengers included under the same reservation. This data is more extensive than what DHS receives through APIS and conceivably could contain upwards of 50 fields – including information such as travel history, seat assignments, contact phone numbers, and form of payment. The greater depth and breadth of this information makes it a vital tool for a thorough vetting of all passengers. While API allows us to complete checks against watchlists and other records with great accuracy, it does not always include information that would allow us to link an unknown adversary or "clean skin" to known or suspected terrorists and criminals.

CBP has been using PNR data since 1992, when it was a voluntary program begun in cooperation with fourteen airlines. On November 19, 2001, President Bush signed into law the Aviation and Transportation Security Act, which mandated that carriers make PNR data available to CBP. As a result, CBP published an interim rule in 2002 that requires all air carriers operating passenger flights in foreign air transportation to and from the United States to provide CBP with electronic access to PNR data to the extent that it is collected and contained in their reservation and departure control systems. CBP is currently collecting PNR data from 127 airlines, which represents all major carriers operating to and from the United States.

DHS's use of PNR and APIS information has produced a number of successes in the war on terrorism. Using these data, CBP has encountered 4801 positive matches for known or suspected terrorists.

Despite PNR's success stories and 15 year history, the European Union in 2003 approached DHS and expressed concerns about the status of the program under European privacy laws. The result, in 2004, was an agreement that legally protected carriers that complied with the CBP regulation. But the agreement has also limited the ability of counterterrorism officials to have broad access to PNR data and to hold the data long enough to support future investigations. As the Subcommittee knows, in May the European Court of Justice (ECJ) annulled this agreement due to a technicality in European law. The European Union has since notified the United States that the agreement will be terminated at the end of this month.

We are actively engaging the European Union to develop an appropriate replacement agreement. However, it is important to emphasize DHS's belief that the ECJ's ruling should not impact international air travel. The court did not rule that DHS's access to and use of PNR violated European privacy law. Nor did the court seek to curb carrier compliance. In fact, it ruled that the European-wide privacy directive does not apply to DHS's collection and use of PNR. Likewise, after extensive review, the DHS Chief Privacy Officer in September 2005 determined that CBP's use of PNR was in compliance with the representations made in the Undertaking and followed the standards of fair information practices. As such, DHS expects all carriers serving the U.S. market to continue complying with current regulations.

It is also important to keep the overall stakes in mind. The primary lesson from 9/11 was that we cannot effectively combat the terrorist threat if we prevent our law enforcement and counter terrorism agencies from communicating and cooperating. In 2004 Congress passed the Intelligence Reform and Terrorism Prevention Act to ensure that those mistakes are never repeated. Prior to 2004, however, our Immigration and Customs Enforcement investigators effectively used PNR information to combat a host of crimes. Today they are unnecessarily hindered in their ability to use European data to do so. That said, DHS is strongly encouraged by recent statements by European Commission Vice President Franco Frattini and looks forward to developing a mutually acceptable, long term, cooperative arrangement with our European allies.

All of these efforts to separate high and low risk travelers are necessarily supported by DHS programs overseas and by cooperation with our friends and allies. Both CBP and the Transportation Security Administration maintain programs in foreign countries that greatly enhance our prescreening efforts. For instance, the Immigration Advisory Program (IAP) works with airline carriers and host country authorities to identify potentially inadmissible travelers who may pose a threat to the national security. With this added security layer, CBP can reduce suspected overseas threats prior to the flight's departure, thereby avoiding delaying, canceling, or diverting flights destined for the United States.

The IAP teams have no legal authority in these foreign countries, but have forged strong relationships with local law enforcement. Through cooperation they are able to further vet high risk passengers based on information held by the host government and coordinate a response. They may also recommend to the air carrier that the passenger suspected to be traveling on

fraudulent documents not be allowed to board the flight. Although an air carrier is not required to abide by the recommendation, it may be liable for fines and for the cost of returning the passenger to the country of departure if CBP subsequently denies him or her entry to the United States.

IAP was initiated at two locations in FY 2004: at Amsterdam – Schiphol International Airport in June, and Warsaw – Chopin International Airport in September. IAP expanded to the London – Heathrow International Airport as a 120-day pilot in April 2006, and subsequently extended an additional 120-days ending December 2006. The establishment of a fourth site at Tokyo – Narita International Airport has just been agreed to by the Japanese government. Pending host government approval, CBP's fiscal year 2007 budget includes converting Amsterdam, London, and Tokyo to permanent locations.

As of August 24, 2006, IAP teams have made more than 700 no-board recommendations for high-risk or inadequately documented passengers. They also have intercepted 78 fraudulent documents. These accomplishments equate to approximately $1.6 million in avoided costs associated with detaining and removing passengers who would have been returned after having been refused admission to the United States, and $1.5 million in air carrier potential savings for fines and passenger return costs.

Similarly, DHS works with individual carriers and airports to ensure their processes for physically screening each passenger prior to boarding meet adequate standards. Our goal is to ensure that carriers and airport authorities remain a critical partner in identifying those that may be trying to travel on fraudulent documents or threaten the aircraft.

Despite all our prescreening programs, it is still important to have trained eyes reviewing a person's documentation to confirm they are who they claim to be. Other than the airports at which IAP is active, the first opportunity DHS has to make such a determination for an international passenger is after the passenger disembarks from the aircraft. The Carrier Liaison Program (CLP) was developed to enhance border security by helping commercial carriers identify improperly documented passengers who are traveling to the United States. The CLP provides training and technical assistance directly to carrier staff on topics such as U.S. entry requirements, passenger assessment, fraudulent document detection, and imposter identification. The program uses state of the art document examination material, equipment, and training tools. To date, CLP has trained over 1800 carrier personnel and security personnel.

Likewise, our electronic prescreening systems will never be able to identify all potential threatening passengers with a 100 percent degree of reliability. A single radical person can seek to carry out his own personal attack on an aircraft. As a result, it's equally critical that airline and airport personnel are properly trained and equipped to detect explosives and other weapons on a passenger or in their luggage. To this end, TSA regulates the security operations of all air carriers operating flights to the United States. Over 140 non-U.S. passenger air carriers and 30 non-U.S. all-cargo carriers have TSA-approved security programs for operations to and from the U.S. TSA is able to rapidly update these plans by issuing Emergency Amendments (EAs). The EA process proved critical in ensuring that all carriers received immediate notice of the recent ban on liquids and effectively implemented it.

To ensure these rules are being followed, TSA operates the Foreign Airport Assessment and Air Carrier Inspection Programs. During airport assessments conducted in foreign countries, International Aviation Security Inspectors focus on application of International Standards and Recommended Practices defined by the International Civil Aviation Organization, to which 189 countries are signatories. TSA international inspectors visit every airport that serves as a last point of departure for the United States, those locations where U.S. aircraft operators fly, and any site deemed necessary by the Secretary of Homeland Security. Each foreign airport assessment, mandated by law, is performed at least triennially. Nearly 270 airports are regularly visited by TSA inspectors and an average of 30 new inspection locations are identified each year, requiring comprehensive surveys and follow-on assessments. The air carrier inspection protocols focus on U.S. aircraft operators and foreign air carriers' compliance with applicable TSA regulations. Over 800 air carrier stations are inspected each year.

* * *

We've outlined many distinct DHS programs for you today. Each fills an important niche in securing the diverse activities that together comprise every international flight to the United States. The visa application process remains our first opportunity to vet a prospective traveler against our knowledge of known and suspected terrorists. As such, how we decide which friends and allies will be exempted from a visa requirement is a vital factor in adverting risk. Only through strong requirements regularly enforced can we prevent our close economic and cultural relationships from becoming a security liability. That said, the availability of extensive and reliable data long before departure remains our greatest asset. By applying the full force of the information and analytical capabilities of the U.S. intelligence and law enforcement communities, we can identify many threats and prevent them from evolving into disasters.