



WRITTEN TESTIMONY

of

**DAVID HEYMAN
ASSISTANT SECRETARY FOR POLICY,**

**MARY ELLEN CALLAHAN
CHIEF PRIVACY OFFICER,**

and

**THOMAS L. BUSH
DIRECTOR, ANALYSIS AND TARGETING/CBP**

U. S. DEPARTMENT OF HOMELAND SECURITY

before

**UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE**

on

***How DHS Addresses the Mission of Providing Security, Facilitating Commerce and
Protecting Privacy for Passengers Engaged in International Travel***

OCTOBER 5, 2011

WASHINGTON, DC

Introduction

Chairman Meehan, Ranking Member Speier, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss how the Department of Homeland Security (DHS) works to prevent individuals that may pose a risk to our national security from entering the country—all while facilitating legitimate travel and commerce and protecting the privacy of individuals engaged in international travel.

Specifically, I want to highlight the Department's pre-screening of passengers, and in particular, the use of Passenger Name Record (PNR) data in our work to prevent and counter terrorist and criminal threats to the Homeland. PNR data and analysis play a unique role in enabling the U.S. Government to identify both known *and* unknown threats. Recent cases underscore the vital benefit of PNR and reflect its value today—a value that has grown in recent years as the Department has improved and expanded its data matching and processes. We have been able to advance the development, implementation, and use of this tool, while also protecting travelers' data and privacy.

Other countries, recognizing the utility of PNR, have expressed interest in developing their own PNR systems for screening travelers. Our ongoing negotiation with the European Union (EU) over how PNR from flights with ties to the EU is handled by DHS is one manifestation of our ability to advance security, data protection, and privacy together. I commend the Subcommittee for holding this important hearing on this topic.

Multiple Layers of Defense

Since 9/11, we have learned that the exercise of immigration and border security authorities can be powerful resources used to identify and thwart terrorist operations at the earliest opportunity. We have significantly adapted and enhanced our ability to detect and interdict threats at the earliest opportunity by instituting a layered aviation and border security architecture, incorporating both seen and unseen assets.

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.

PNR is one of five automated systems that assist the Department in identifying travelers likely to pose a risk. The five reinforcing systems are: PNR; the visa application process (conducted by the Department of State and supported by DHS); the Electronic System for Travel Authorization (ESTA) for travel under the Visa Waiver Program; the Advance Passenger Information System (APIS), and; Secure Flight. These are the systems DHS uses to begin conducting screening before an aircraft's departure and function in conjunction with physical security procedures such as checkpoint screening.

Passenger Name Record—PNR

The term PNR refers to the data an airline receives from a traveler to book and manage travel plans, and may include the traveler's itinerary, payment method, and contact information. In light of the lessons learned from 9/11 about identifying and preventing terrorists traveling into and out of the United States, Congress mandated that carriers make PNR data available to the U.S. Government in the *Aviation and Transportation Security Act of 2001* (ATSA, P.L. 107-71). Presently, all carriers flying to and from the United States provide DHS with PNR pursuant to ATSA and DHS implementing regulations. DHS analyzes PNR provided by the airlines to identify terrorists and criminals attempting to blend into the traveling public before committing criminal acts against innocent people. Our analysis of PNR data, reinforced through cooperation with Federal partners, has helped to identify approximately 1,750 unique suspicious cases every year, and has been vital in many of the United States' most well-known terrorism investigations since 9/11.

To ensure the protection of privacy and civil liberties, DHS' use of PNR data is subject to oversight from multiple independent bodies, including the Department's Chief Privacy Officer, the DHS Inspector General, and the Government Accountability Office, as well as the U.S. Congress. In addition, periodic joint reviews with EU officials have confirmed the value of PNR data and our adherence to the highest data protection and privacy standards. The findings of these joint reviews are available online on the DHS and EU websites. Over the last decade, the Department has demonstrated its firm commitment to protecting the privacy of travelers. Of the literally billions of passengers traveling to and from the United States during the past 10 years, there has not been a single data breach or use of PNR in violation of established privacy protections.

Continued Threat / Risk of Terrorist Travel

This year witnessed the deaths of both Osama bin Laden and Anwar al-Awlaki, as well as the 10-year anniversary of the deadly terrorist attacks of 9/11. As we reflect on the past decade, it is important to remain cognizant of the continued, evolving threat of terrorism to the traveling public. Since 9/11, the threat has changed to include not only large-scale attacks but also smaller operations with potentially catastrophic effects, including the continued targeting of the aviation sector. One of the most important responsibilities of government is the protection of its citizens, a duty this Department well recognizes and takes seriously. Passengers have a right to privacy and protection of their civil liberties and personal information, but also have a right to know that their government is doing everything it can to ensure their safety and security when they board an airplane. It is necessary, therefore, to ensure the continued use of proven and effective security measures. PNR is a proven asset in the fight against terrorism and other transnational crimes.

Evolution of U.S. Prescreening Efforts Since 9/11

Ten years ago, screening of passengers coming to the United States was limited to the Department of State visa process, if applicable; the inspection of a person by an immigration officer at the port of entry; and any processes applied at foreign airports by

foreign governments. Provision of advance passenger information was voluntary. 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.

Today, in response to both 9/11 and evolving threats, and with the help and support of Congress, DHS has significantly adapted and enhanced its ability to detect and interdict threats at the earliest opportunity, including through the access to and analysis of PNR data as mandated by Congress. PNR data are analyzed in conjunction with other screening tools such as visa applications, the Advance Passenger Information System, and the Electronic System for Travel Authorization (ESTA). DHS analysis of PNR data is an indispensable layer in a comprehensive approach to security. Each tool plays a unique role in the screening process. ESTA and the visa issuance process (depending on the country and traveler) allow us to prevent a known criminal or terrorist from preparing to travel. Secure Flight and APIS help DHS decide how the carriers and CBP officers, respectively, should handle travelers as they prepare to board. PNR data further enable this decision with additional and earlier information. APIS and PNR then help DHS decide who warrants a secondary examination upon arrival. In all cases, trained DHS personnel review and analyze the results of these automated systems.

As the 9/11 Commission pointed out, targeting terrorist travel is one of the most powerful weapons this country has to counter terrorist operations. Terrorists travel in order to: identify and engage in surveillance of potential targets; plan attacks; receive training on tactics and operations; collect and transfer funds and documents; and communicate with other operatives. Every step along this pathway presents a vulnerability for 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—a step that often necessitates submitting advance passenger information, using a passport, and undergoing screening by immigration and border officials while at ports of entry.

The Role of PNR Data Within that System

PNR data analysis can help identify individuals up to 72 hours prior to departure, including watchlisted individuals, non-watchlisted co-travelers, and terrorists or criminals adopting known illicit travel patterns. DHS is able to link previously unknown terrorists and criminals to known terrorists or criminals by matching contact information, flight patterns, and other data. After this analysis is complete, DHS works with foreign and industry partners to interdict illicit travelers prior to boarding or prioritizes resources for their inspection at U.S. ports of entry. PNR data collection and analysis also support terrorist and criminal investigations, including the three most prominent U.S. terrorist investigations in 2009 and 2010. Further, PNR served as a critical tool in supporting United States Government efforts to investigate 9/11 threats over the tenth anniversary weekend.

The retention of PNR data after a flight allows DHS to unravel more complex plots by looking at travel practices over time. Data that does not appear to be relevant at the time

of travel can be critically important when tied to a specific case later. Remember that the 9/11 plot was originally conceived in the early 1990s; an attempt on the World Trade Center occurred in 1993, and the actual 9/11 plot planning and execution began in earnest in 1996. This included numerous dry runs and practice flights, as well as travel for recruitment and planning. Retained travel data was important in securing convictions by the Department of Justice in a number of recent counter-terrorism cases, including the conviction of Mumbai plotter David Headley.

Identifying Unknowns

Following 9/11, the United States Government collected intelligence on al-Qa‘ida and its affiliate networks and established the FBI’s consolidated Terrorist Screening Database (TSDB) of known or suspected terrorists. Today, we check travelers to the United States against the TSDB, no matter what mode of transportation they plan to use to come to the United States.

As DHS has seen in recent cases, however, intelligence and law enforcement agencies may have limited or no derogatory information about individuals who pose a real risk to the United States. In fact, we know that some terrorist groups are deliberately looking to recruit individuals who are specifically *unknown* and can remain undetected by heightened security measures. Fortunately, PNR data analysis, particularly of historic records, allows us to help identify individuals who may be unknown to us as terrorists or criminals, but exhibit a pattern of behavior that is consistent with known or suspected terrorist or transnational criminal behavior. For example, a few years ago, two organized crime syndicates in Latin America devised a simple and effective way to smuggle kidnapped children into the United States for sale. They would pay women to fly to the United States with their own children’s legitimate passports but with kidnapped babies. The women would then return alone. By looking for such a pattern in PNR records over a number of years DHS arrested 11 smugglers, removed 10 criminals and identified 37 victims. The same technique of analyzing travel patterns has proven effective against a myriad of crimes and terrorism.

At the same time, DHS realizes that sometimes innocent travelers may adopt what may appear to be suspicious patterns. As a result, DHS has established automated procedures so if a traveler is repeatedly flagged for further inspection and found not to pose a risk, DHS will automatically ‘de-flag’ the traveler in the future. Further, all pattern-based rules are evaluated quarterly by the DHS Chief Privacy and Civil Liberties Officers for effectiveness and appropriateness. A Customs and Border Protection (CBP) officer, however, may still determine that a closer inspection is warranted, depending on the individual circumstances and travel.

Early Identification – Activation of IAP Teams

CBP stations Immigration Advisory Program (IAP) officers at certain foreign airports to work with airlines and foreign officials to identify high-risk and improperly documented travelers before they board aircraft bound for the United States. At the invitation of

foreign partners, IAP officers make “no-board” recommendations to airlines on the basis of passenger data analysis and a review of individual travel documents. To be most effective, several hours before a flight is scheduled to depart, an IAP officer must know who will likely be on a flight and whether they warrant further exam prior to departure. Frequently, PNR data analysis is the first information IAP officers receive to assist in making these determinations. CBP’s National Targeting Center-Passenger (NTC-P) analyzes PNR data received up to 72 hours prior to departure and provides recommendations to the IAP officers. NTC-P later validates this analysis with APIS closer to departure. IAP officers are currently posted at ten airports in eight countries, and have recommended, in part based upon PNR data, a total of 2,875 no-boards in fiscal year 2011, including nine No-Fly hits, 74 confirmed Terrorist Screening Database matches, and 109 cases of fraudulent document use.

Examples of PNR Effectiveness

Headley, Zazi, Shahzad

I would like to take a little time to discuss some of the high-profile cases where PNR data analysis has been instrumental in critical national security investigations and prosecutions. As background, I mentioned earlier that analysis of PNR data have proven to be the critical tool for annually identifying around 1,750 suspicious cases. PNR data have also aided nearly every high profile terrorist investigation, including: David Headley, who pled guilty for his role in the 2008 Mumbai terrorist attacks; Najibullah Zazi, who pled guilty to plotting to bomb New York City subways; and Faisal Shahzad, who pled guilty to attempting to detonate a car bomb in New York’s Times Square. Just as fingerprinting was first used and became an important tool in criminal investigations in the beginning of the 20th century, so too at the start of the 21st century has PNR analysis become a vital tool for identifying terrorists and transnational criminals. DHS has also relied on PNR data analysis in nearly every human smuggling case involving air travel.

The case of Faisal Shahzad clearly demonstrates the effectiveness of DHS’s prescreening programs. Early in this investigation, the Federal Bureau of Investigation (FBI) learned of Shahzad’s cell phone number from a report shared by DHS. The FBI ran the phone number in their ACS system and was able to connect it to the DHS report. Through good interagency cooperation, the FBI asked DHS if it had encountered any individual who reported this phone number during border crossings. DHS searched its PNR database for the phone number, identified Shahzad, and learned other information he had provided to DHS. DHS then provided the additional data to the FBI. Later, Shahzad attempted to flee the United States, but DHS’s analysis of departing passenger data identified him before departure and DHS removed him from the aircraft.

Strong Record of Privacy Protection

DHS provides robust privacy protections and strict safeguards over PNR data. Through a combination of law, policy, and oversight, DHS ensures its compliance with stringent standards of privacy and security in the collection and use of PNR data. DHS applies fair information practice principles to its collection and use of PNR, including data integrity, data security, purpose specification, auditing and accountability, individual access, and redress. Moreover, the Department is firmly committed to transparency when it comes to

informing our partners and the public about its mission, including how we use and safeguard personally identifiable information such as PNR data.

By leveraging the congressionally-mandated authorities of the DHS Chief Privacy Officer, DHS is working diligently to assure all U.S. and international travelers that the highest standards are being applied to the protection of their personal information. The Chief Privacy Officer has managed two internal audits of DHS's use of PNR data and coordinated two joint reviews with the EU since 2004. When preparing for the joint review that took place in February 2010, the DHS Privacy Office spent approximately ten weeks of employee time analyzing and assessing DHS collection and use of PNR data and published two public reports related to that assessment. The reports from these audits are publicly available on the websites of the DHS Privacy Office and the EU. The DHS Privacy Office found, and the EU acknowledged, that there has not been a single incident involving the unauthorized use of PNR data.

Individual travelers have many opportunities to learn how DHS handles PNR data. The PNR data rule, System of Records Notice, and Privacy Impact Assessment are all available for public review and comment. In addition, individuals, both U.S. and non-U.S. citizens, have multiple opportunities for access and redress. The *U.S. Freedom of Information Act* (FOIA) applies equally to U.S. citizens and non-U.S. citizens. Anyone can request his or her PNR data directly from DHS; DHS receives and answers these types of requests routinely. If the traveler seeks to change or delete information contained in his/her PNR, he or she can submit a request to DHS and changes deemed appropriate will be made. U.S. and non-U.S. citizens alike also have access to the DHS Traveler Redress Inquiry Program (DHS TRIP) to correct or amend records. More information on these programs can be found at www.dhs.gov/privacy.

U.S – EU PNR Agreements

Despite this operational and privacy success, last year, the EU sought to re-negotiate our bilateral PNR Agreement to obtain further reassurance that data with ties to Europe is being handled properly by the United States. To protect U.S. industry partners from unreasonable lawsuits, as well as to reassure our allies, DHS has entered into these negotiations.

The Agreement currently in force provisionally, negotiated in 2007, is not scheduled to sunset until 2014. The Agreement is operationally sound, but it is subject to ratification by the European Parliament, which instead directed the European Commission to renegotiate the Agreement. As a matter of good faith and out of respect for our EU partners and their evolving political structures following enactment of the Lisbon Treaty, Secretary Napolitano subsequently agreed to negotiate a new agreement only if the new text would not degrade the operational effectiveness of the 2007 Agreement and would permit additional security enhancements where necessary. We commenced the latest negotiations on December 4, 2010. As such, the United States is currently in its fourth negotiation over PNR with the EU in nine years—effectively a decade of negotiation.

The Department is committed to concluding a new PNR agreement, first and foremost a security agreement, which upholds vital public interests in both security and privacy. We reached agreement with the European Commission for such a text on May 16, 2011. The text is an improvement over the 2007 Agreement, it protects both security and privacy and U.S. and European interests, it provides all relevant parties with legal certainty, and it is a reliable framework for an enduring deal.

U.S. and EU negotiators worked to respond to the European Parliament's criticism of the 2007 Agreement, to improve passenger security and to provide air carriers a legally certain operating environment. To build support for this approach, DHS has met repeatedly with not only the European Commission, which negotiates on behalf of the EU, but also with key Committees and Members of the European Parliament and representatives of individual Member States. The new agreement is clear, detailed, and transparent – in ways that some critics in Europe felt the previous Agreement was not. The text of the draft agreement defines key terms such as “terrorism,” and “transnational crime” consistently with U.S., EU, and international norms. A data retention period acceptable for U.S. security purposes is maintained, with additional safeguards to ensure privacy and data protection. The new agreement will require travel information to be transmitted to DHS with greater lead time than provided for in the 2007 Agreement, and thus will provide for greater analysis earlier in the passenger travel life-cycle. It also provides for a new method of data transmission (“real-time” push). By restricting data transmission to the minimum necessary while ensuring data accuracy, the real-time push method of sharing data will enhance security and privacy protection at the same time. Lastly, the new agreement will expand opportunities for police and judicial cooperation between the U.S. and EU authorities.

I want to thank this Committee for its interest and support in our negotiations with the EU. With the conclusion of PNR negotiations with the European Commission and, we hope, forthcoming signature and then support from the European Parliament, the United States and EU will have made progress in strengthening the previous PNR Agreement from a privacy and security perspective. Success will be the result of nine months of intense negotiations and build off nine-years of dialogue on how best to facilitate safe transatlantic travel and protect individual privacy.

By all accounts, the new text is stronger than the 2007 Agreement; it addresses all EU concerns raised with the U.S. negotiating team, while also preserving and in some cases improving critical U.S. operational interests. We must build on our historic relationship, values, and interests, as we seek action by the European Commission, the European Council, and the European Parliament to finally conclude this PNR Agreement, which is without a doubt better for enhanced security, as well as for improved data and privacy protections.

Conclusion

Chairman Meehan, Ranking Member Speier, and distinguished Members of the Subcommittee, we look forward to working with you as we explore opportunities to advance our cooperation with our European partners to counter terrorism and

transnational crime. Thank you again for this opportunity to testify. My colleagues and I are happy to answer your questions.