International Civil Aviation Organization

FALP/6-IP/9
10/5/10
English only

INFORMATION PAPER

FACILITATION PANEL (FALP)

SIXTH MEETING

Montréal, 10 to 14 May 2010

Agenda Item 3: Report of the API/PNR Working Group

U.S. POSITION REGARDING PNR DATA PROVISION METHODOLOGIES

(Presented by U.S. Customs and Border Protection)

1. INTRODUCTION

1.1 Attached, for information for FALP/6 participants, is an informational paper to the ICAO Secretariat and member States on the U.S. Position regarding PNR data provision methodologies.

2. ACTION BY THE FAL PANEL

2.1 Informational only.

3. U.S. PNR STATUS

3.1 The United States has used airline reservation data, also known as Passenger Name Records (PNR), to successfully identify transnational criminals and terrorists attempting to transit the United States since 1992.

3.2 Over the last nearly twenty years, the analysis of PNR data has become an integral part of our effort to manage the U.S. border securely, efficiently and fairly and has significantly reduced wait times at our border crossings.

3.3 Pursuant to the Aviation and Transportation Security Act of 2001, the U.S. Customs Service, now known as U.S. Customs and Border Protection (CBP), issued an Interim Final Rule in 2002, mandating that carriers that store PNR data make such information available by electronic means.

3.4 PNR data holds information that can be used in identifying persons involved in transnational crimes and terrorism.

3.5 When PNR is available, CBP officers use it to identify travelers that potentially pose a greater risk of terrorism or serious transnational crimes, based on intelligence and the analysis of current and past law enforcement cases.

3.6 In this way, PNR helps CBP to identify known threats earlier and previously unknown threats by uncovering travel practices known to be indicative of illicit activity.

3.7 2007, CBP signed an agreement with the European Union (EU) agreeing to a set of 19 data categories that can be provided by carriers traveling between the United States and the European Union.

3.8 The 19 data categories include such information as traveler's name, contact details, details of the travel itinerary (such as data of travel, origin and destination) and details of the reservation (such as travel agency and payment information).

3.9 CBP currently receives, on a fairly consistent basis, the PNR record locator code, date of ticket issuance, ticket number, first and last name, airline, flight number, date of travel, historical changes of the reservation, city of departure, city of arrival, and at least one form of contact information (phone number or email address), at 72-hours prior to travel. This information is then updated a number of times prior to departure to ensure CBP decisions are based on current information.

3.10 The precise data received is dependent on the carrier's business practices and reservation system and may vary between flights and passengers on each flight. The variance in PNR data impacts CBP's ability to perform consistent screening across all travelers destined to or departing from the United States.

3.11 CBP's Automated Targeting System – Passenger (ATS-P) maintains PNR information received from commercial air carriers and uses that information to assess risk associated with travelers seeking to enter, exit, or pass through the United States.

3.12 The system utilizes scenario-based targeting rules in order to identify "unknown" potential higher-risk individuals.

3.13 Two examples of how PNR data aided in identifying persons involved in terrorist activity:

3.13.1 2009 - The PNR of a German traveler does not match watch-lists or scenario-based rules, however, a match is made between a phone number in the traveler's PNR and the phone number of a previously-encountered terrorist subject. CBP officers at a U.S. port of entry are advised to conduct a secondary examination, which subsequently provided the National Targeting Center with sufficient derogatory history to deny entry for engaging in terrorist activity.

3.13.2 2006 – ATS-P identifies an individual traveling to the U.S. from a Middle Eastern country, holding a valid student visa. PNR review identifies possible ties to other students with confirmed terrorist ties. A secondary search of the individual reveals instructions on building improvised explosive devices (IEDs), martyrdom, video will and testimony. The subject was interviewed by the Federal Bureau of Investigations (FBI) and charged with making false statements.

3.14 Referencing the examples in paragraphs 3.13.1 and 3.13.2, having critical information beginning at 72 hours prior to a flight's departure has become vital to making accurate assessments.

4. PNR STANDARIZATION

4.1 CBP has written several programs to allow it to recognize and process the various PNR formats used by carriers and their systems. Oftentimes these formats change as carriers modify their systems or business practices. This may result in fields or even entire flights being added or dropped unintentionally.

4.2 A standardized format would be welcomed, from both a technical and a compliance perspective.

4.3 CBP is participating in the PNRGOV working group organized by the International Air Transport Association (IATA) and the World Customs Organization (WCO), the goal of which is to establish a standardized message format to be utilized when sharing PNR data between carriers and participating governments.

4.4 Having a standardized PNR message format will allow carriers and governments to predict the framework of the message structure and therefore more efficiently program their systems to accommodate requirements during systems upgrades or future regulations.

4.5 CBP receives PNR through two primary submission methods, “Push” and “Pull”.

4.6 From a security and border management perspective, either technology solution can meet the United States’ needs, however, many carriers have been reluctant to invest in IT reforms to support a “push” method.

4.7 CBP’s operational experience illustrates that it must be able to receive additional PNR data outside of scheduled transmissions under either a push or pull system. This capability allows CBP to respond to emerging threats and flight path irregularities. As a result, unscheduled data transfers must be available rapidly on a 24/7 basis.

5. LESSONS LEARNED

5.1 The recent events associated with the failed car bombing in New York City and other high-profile terrorist incidents since the Fall of 2009 are evidence of the need to receive reliable and comprehensive PNR data.

5.2 CBP believes that having the most up-to-date PNR information is critical. The data needs to be provided in time and format for appropriate screening and action if necessary.

5.3 As contracting parties, including the United States, increase their reliance on PNR for identifying crime and terrorism, variations in messaging structure and any resulting disruptions will increasingly become an untenable vulnerability.

5.4 CBP will continue to assist member States by providing concepts and ideas on the management of PNR data and how best to utilize this data for targeting purposes.

— END —