U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 30,2006

Via Electronic Delivery

Mr. Jonathan Faull
Director General
European Commission
Brussels, Belgium

Mr. Markus Laurent
Deputy Director General
Ministry of Foreign Affairs
Helsinki, Finland

Dear Jonathan and Markus:

This letter is intended to set forth our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued by the Department of Homeland Security (DHS) on May 11,2004. We seek your concurrence in the interpretations outlined below and look forward to further reviewing these and other issues in the context of future discussions toward a comprehensive, reciprocal agreement based on common principles.

Sharing and Disclosure of PNR

The Intelligence Reform and Terrorism Prevention Act of 2004 required the President to establish an Information Sharing Environment "that facilitates the sharing of terrorism information." Following this enactment, the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to . . . terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the Information Sharing Environment.

Pursuant to Paragraph 35 of the Undertakings (which requires that the Undertakes be consistent with U.S. law and allows DHS to advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings), the U.S. has now advised the EU that the implementation of the Information Sharing Environment required by the Act and the Executive Order may be impeded by certain provisions of the Undertakings that restrict information sharing among U.S. agencies, particularly all or portions of paragraphs 17, 28, 29, 30, 31, and 32.

In light of these developments, nothing in the Undertakings should be interpreted or applied to limit the sharing of PNR data by the Bureau of Customs and Border Protection (CBP) with other elements of the U.S. government responsible for preventing or combating of terrorism and other crimes as set forth in Paragraph 3 of the Undertakings.

CBP will therefore facilitate the disclosure of PNR data to U.S. government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combatting terrorism and

serious transnational crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating.

CBP will ensure that such authorities respect substantially equivalent standards of data protection to that applicable to CBP, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm to CBP that it respects those standards. CBP will inform the EU on the implementation of such facilitated disclosure and respect for the applicable standards before the expiry of the Agreement.

Early Access Period for PNR

While Paragraph 14 limits the number of times PNR can be pulled, the provision puts no such restriction on the "pushing" of data to DHS. The push system is considered by the EU to be less intrusive from a data privacy perspective. The push system does not confer on airlines any discretion to decide when, how or what data to push, however. That decision is conferred on CBP by U.S. law. Therefore, it is understood that if a carrier implements a "push system, Paragraph 14 is consistent with requiring that after the initial push of data, all changes to the PNR are to be transmitted in real time.

In determining when the initial push of data is to occur, CBP has discretion to obtain PNR more than 72 hours prior to the departure of a flight so long as action is essential to combat an offense enumerated in paragraph 3. Additionally, while there are instances in which the government may have specific information regarding a particular threat, in most instances the available intelligence is less definitive and may require the casting of a broader net to try and uncover both the nature of the threat and the persons involved. Paragraph 14 is therefore understood to permit access to PNR outside of the 72 hour mark when there is an indication that early access is likely to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with offenses described in Paragraph 3 of the Undertakings. In exercising this discretion, CBP will act judiciously and with proportionality.

DHS will carry out the necessary tests as soon as its technical requirements are satisfied in order to move, as soon as practicable, to a push system for the transfer of PNR data in accordance with these Undertakings.

Data Retention

Several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. The U.S. expressed grave reservations about the destruction of PNR data at the end of 3.5 years. The Agreement will expire before Paragraph 15 of the Undertakings requires the destruction of any data, and questions of whether and when to destroy PNR data collected since 2004 will be addressed by the United States as part of future discussions; in the absence of formal agreement, the data will be retained only for so long as it has potential relevance to the purposes stated in Paragraph 3 of the Undertakings.

The Joint Review

Given the extensive joint analysis of the Undertakings conducted in September 2006 and the expiration of the agreement prior to the next Joint Review, the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement.

Data Elements

The frequent flyer field may offer addresses, telephone numbers, email addresses; all of these, as well as the frequent flyer number itself, may provide crucial evidence of links to terrorism. Similarly, information about the number of bags carried by a passenger may have value in a counterterrorism context. The Undertakings authorize CBP to add data elements to the 34 previously set forth in Attachment "A" of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3.

The U.S. has consulted under Paragraph 7 with the EU in connection with item 11 of Attachment A regarding CBP's need to obtain the frequent flier number and any data element listed in Attachment A to the Undertakings wherever that element may be found.

Finally, with respect to the filtering and use of sensitive data, the parties agreed that Paragraphs 9 and 10 of the Undertakings are not intended to impose an absolute prohibition on the use of sensitive data but that such data should be accessed only when strictly necessary. An example was given of an intelligence report suggesting that passengers were planning to hide explosives in a cast or prosthetic device; in response to such a report, it would be appropriate to search PNR data for such passengers. Access to such information is authorized by paragraph 34, which provides that the Undertakings must not impede the use of PNR for the protection of the vital interests of the data subject or of other persons or inhibit the direct availability of PNR to relevant authorities for the purposes set forth in Paragraph 3 of the Undertakings. "Vital interests" encompasses circumstances in which the lives of the data subject or of others could be at stake and includes, for example, instances in which a potential terrorist or other attack could endanger the lives of passengers; it also includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay. Notwithstanding these interpretations, "sensitive" data as defined by Attachment C to the Undertakings will not be routinely used by DHS for passenger risk assessment and DHS does not rely on discriminatory racial, ethnic, or religious stereotypes in carrying out its assessments.

Secretary Chertoff has fully reviewed and concurs with the details of this letter.

Sincerely yours,

Stewart Baker
Assistant Secretary for Policy