



Homeland Security

March 31, 2010

Mr. Reinhard Priebe
Director
Directorate F: Security
European Commission
Directorate-General justice, Freedom and Security
B-1049 Brussels, Belgium

Subject: *DHS Response to the European Commission's Report on the Joint Review of the U.S. – EU Passenger Name Record Agreement*

Dear Mr. Priebe:

DHS appreciates the opportunity to comment on the European Commission's (EC) draft *Report on the Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security*. We recognize and appreciate the substantial efforts made by the EU Delegation during the course of the Joint Review to objectively gather facts, review documentation, observe DHS/U.S. Customs and Border Protection (CBP) operations they relate to PNR, as well as the thoughtful follow-up questions presented to the DHS team by the EU Delegation.

The DHS team reviewed the draft report and submits this letter, which as we understand under the terms of the Agreement and as identified in the draft report, will be published as an Appendix to this report. DHS finds the EC draft report findings to be largely consistent with the 2010 EU-US Joint Review and the reviews conducted by the DHS Privacy Office as reflected in the 2008 and 2010 reports, specifically as they relate to the finding of substantial efforts made toward full implementation of the Agreement and compliance with the terms of the Agreement.

As with any program, DHS agrees with the Commission that continued improvements are always advisable, and the PNR program at DHS is no different. Nonetheless, DHS would like to clarify and respond to certain areas of the report where the Commission found that "improvement seems necessary and advisable" and made specific recommendations to DHS to address these areas. These areas include:

1. the Secure Flight Program;
2. the Immigration Advisory Program and the Regional Carrier Liaison Group;
3. push vs. pull;
4. monitoring and use of the override and ad hoc pull functions;
5. tracking requests for access to EU PNR;
6. sensitive terms;
7. purpose limitation and serious transnational crime; and
8. international cooperation.

1. Secure Flight Program

The DHS Transportation Security Administration's (TSA) Secure Flight program has a regulatory requirement as prescribed in the Final Rule published on October 28, 2008, for all carriers, both U.S. and foreign, that provide service to, from, and over the United States, to provide limited passenger information (referred to as Secure Flight Passenger Data (SFPD)) 72 hours prior to travel. In order to meet requirements regulated within the Secure Flight Final Rule, DHS allows carriers to provide this information through their existing PNR Push/Pull protocol; thus significantly reducing the number of required data transmissions. In these instances CBP will pass three data elements to the Secure Flight program for vetting (full name, date of birth, and gender). SFPD is maintained by the Secure Flight system for a period of seven days, upon completion of the identified travel itinerary. The Secure Flight data is deleted from the Secure Flight system after that time period.¹

SFPD collected by the DHS TSA under Secure Flight is security information the carriers are required to collect and provide to the government to fulfill regulatory requirement associated with operating in the United States, similar to Advance Passenger Information (API) collected by CBP; therefore it is dissimilar to PNR data which is originally collected by carriers for commercial purposes. Notwithstanding its transmission through a PNR Push/Pull protocol from the carriers, these data elements are SFPD, not PNR. DHS provided for this option to reduce the number of times the airlines would need to send data to DHS.

Further, it should be noted that when DHS issued the Secure Flight notice of proposed rulemaking in August 2007, the DHS Office of Policy specifically briefed the Directorate General for Justice, Freedom and Security at a high level on the scope of the Secure Flight program to ensure there were no issues with the Agreement.

Based on this additional information, DHS respectfully requests that conclusions and recommendations concerning the Secure Flight Program be removed from this report as we believe that this discussion falls outside the scope of the Agreement. Should the Commission still find this discussion to be relevant to the report, we request that this additional context regarding the relationship of the Secure Flight Program and the Agreement be provided since these issues were not discussed in detail during the joint review.

2. Immigration Advisory Program and the Regional Carrier Liaison Group

DHS would also like to clarify statements made in the draft report concerning the Immigration Advisory Program (IAP) and the Regional Carrier Liaison Group (RCLG), which are not, as the draft report indicates, new programs. IAP has its origins in a 2004 arrangement between CBP and the Government of Poland; it has since expanded to nine locations in seven countries. IAP enables CBP to work with foreign governments and commercial airlines based on its analysis of PNR and API to facilitate and promote safe travel between the United States and the participating nations. The program operates based on an arrangement negotiated between DHS/CBP and the appropriate agency in the EU Member

¹ For additional information about the Secure Flight Program, see http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_secureflight2008.pdf.

state where it operates. The Regional Carrier Liaison Groups (RCLG) began in 2006 for non-IAP locations to assist carriers with questions regarding U.S. admissibility-related matters. CBP officers assigned to the RCLG make recommendations to the carriers whether to board or to deny boarding to a passenger who would otherwise be inadmissible to the U.S. RCLGs are staffed solely by CBP officers.

IAP and RCLG require no new data collection or analysis. The National Targeting Center – Passenger (NTC-P) identifies suspected high-risk passengers through the same automated screening process it uses for non-IAP flights, but when the program is present at an airport the team will be notified of potential concerns prior to departure. Once IAP officers determine that an identified passenger is expected to be found inadmissible to the United States, they may recommend to the carrier that it not board the passenger. This program has been very well received by host governments and overseas carriers, as it identifies and terminates illicit activity at an earlier stage, and saves money and time otherwise spent on processing those who are ineligible to enter the United States.

It is important to note that at both IAP and non-IAP locations PNR is not used as the sole basis to recommend to a carrier that a passenger not be boarded. It acts merely as a pointer to a potential concern and any decision to make such a recommendation would only be made after the CBP officer at an IAP location or a CBP officer assigned to a RCLG cross checks the information against API data and/or the physical travel documents in order to verify the identity of the passenger.

In an IAP location, the CBP Officer will interview the passenger and make a recommendation to the carrier that the passenger not be boarded and take appropriate actions in concert with local authorities, as appropriate. In a non-IAP location, the CBP Officer assigned to the RCLG would communicate to the carrier based on API data to recommend that a passenger not be boarded because the individual would most likely be ineligible to enter the U.S., thus enabling the carrier to make a decision on whether to board the passenger. The final decision to board or not board lies with the carrier.

The only distinction between IAP and non-IAP locations is the lack of a physical presence of the CBP Officer; nevertheless it should be noted that the recommendation to not board is always made by a CBP Officer, the final decision is always made by the carrier. Use of the RCLGs at non-IAP locations provides the same benefits identified for IAP locations as it identifies travelers ineligible to enter the U.S. at an earlier stage, and saves the air carriers money and time otherwise spent on processing the travelers return trip if they were to arrive in the U.S. and be found inadmissible.

DHS views the use of PNR in this regard as consistent with the terms of the Agreement. However, we believe that the IAP and RCLG program fall outside the scope of the Agreement and respectfully request that conclusions and recommendations concerning the IAP and RCLG be removed from this report. Should the Commission still find this discussion to be relevant to the report, we request that this additional context regarding the relationship of the IAP and RCLG and the Agreement be provided since these issues were not discussed in detail during the joint review.

3. Push vs. Pull Issues

DHS agrees with the EC's recommendation that more work needs to be done to move all carriers transmitting EU PNR to DHS to a push method. However, DHS would like to remind the EC, as acknowledged in the Agreement, that transitioning to a push method is ultimately a responsibility of the carriers and DHS cannot compel these changes. Recognizing the carriers' needs to reduce costs in both technology enhancements and costs associated with the PNR Push protocol, DHS will continue to provide advice to carriers and their system providers on how best to achieve a functional PNR Push protocol. It should be noted that as indicated in our March 3, 2010 response to the Delegation's follow-up questions, DHS added two additional carriers in February 2010. As stated by several members of the DHS team during the February 2010 Joint Review, DHS welcomes the assistance of the EC in encouraging more carriers to migrate to the Push protocol.

4. Monitoring and Use of Override and Ad hoc Pull Functions

DHS agrees that it should continue to monitor access to, and use of the override and ad hoc pull functions and ensure that access to these functions is limited. As discussed extensively during the course of the review and explained in more detail in the March 3, 2010 letter, these functions are necessary for DHS to meet its mission needs. We recognize that it is equally important to ensure that use of these functions is necessary and proper.

As we discussed during the course of the Joint Review, the override function was introduced in October 2009 to enable DHS to view PNR of flights with a U.S. nexus that may not have an indication of the stop in the PNR itself (e.g., fuel stops, emergency situations). Access to the functionality itself is granted by a senior level authority and the CBP officer must affirmatively acknowledge he has both authority and need to access the information. The affirmative acknowledgement reminds the user that he may access only PNR that has a nexus to the U.S. This new override functionality is reviewed by CBP in the same way general access to PNR is reviewed. Audits of the override process introduced in October 2009 will be conducted by CBP semi-annually. The first audit will be completed in April 2010. The semi-annual audit enables CBP to identify if officers with such access are using the function appropriately or exceeding the functions purpose.

DHS also ensures officers having a working need for access to the ad hoc process by requiring authorization from a senior level authority within DHS. On March 7, 2010, CBP Assistant Commissioner of Field Operations signed the PNR Directive which specifies officer responsibilities as they relate to conducting ad hoc requests. DHS continues to maintain the highest regard when conducting ad hoc requests and makes every effort to ensure such requests are based on immediate need to know and relative to immediate targeting interests. In addition, CBP currently requires officers to acknowledge they have a purpose for the ad hoc request when using the system. ATS-P maintains a log of all ad hoc requests and CBP will conduct periodic audits to ensure valid ad hoc queries are being conducted. Through the internal audits CBP also identifies any accounts that should no longer have the ad hoc access and immediately terminates said access.

5. Tracking Freedom Of Information Act (FOIA) Requests

DHS concurs with the finding that substantial progress has been made in the processing of FOIA requests by CBP that include PNR. The new categories implemented by CBP in December 2009 provide additional insight as to the types of requests that are received, including through identification of the "Traveler" category. While it is important to continue to identify metrics that provide meaningful reporting to our stakeholders including the Congress, the public, and our sharing partners, given the recent implementation of new categories in December 2009 and the likelihood a single FOIA request may involve multiple traveler related records, we do not believe it would be efficient for CBP to further refine the Traveler category at this time. Nevertheless, the CBP FOIA Branch remains committed to processing requests expeditiously.

6. Sensitive Terms

DHS concurs with the recommendation of maintaining an active relationship with the European Commission to maintain a current list of sensitive data within the ATS-P system to ensure appropriate filtering of EU PNR data. However, we also feel it is important to clarify that this review is the first time the Commission has requested we assess the relevance of the current list.

7. Immigration and Serious Transnational Crimes

There are several references in the draft report that suggest DHS may be using EU PNR for purposes unrelated to serious transnational crime. We believe this finding is premised on differing views between DHS and the EC review team on two items: 1) what constitutes a serious transnational crime; and 2) what is considered a decision based on PNR. With respect to what constitutes a serious transnational crime DHS looks at the potential impact of the violation and whether the offense includes a cross border component. With regard to the decisions made based on PNR (i.e., the "use"), DHS believes all of its uses comply with the terms of the 2007 agreement and is happy to discuss differences in the two aforementioned items with the EC.

8. International Cooperation

DHS agrees that bi-directional sharing of analytical information benefits all law enforcement communities and is committed to identifying procedures seen as productive, while at the same time ensuring privacy rights are maintained, that can be used to share analytical information. DHS also encourages Member States police and judicial authorities, as well as Europol and Eurojust, to establish an analytical information sharing relationship with CBP and explore the collection of PNR, which the EC acknowledges in its report has valuable information for law enforcement.

As you are aware, DHS and the EU have identified improving this bi-directional flow of information as a priority under the January 21, 2010 Toledo Declaration on Aviation Security adopted by Secretary Janet Napolitano, former European Commission Vice-President Barrot and the Spanish Presidency represented by Interior Minister Rubalcaba. The status of work

under this declaration will be reviewed at the U.S.-EU Justice and Home Affairs Ministerial,
April 8-9, 2010 in Madrid.

Thank you again for the opportunity to comment on the report. Should you have any
questions or concerns about this letter, please contact me on 1-(703) 235-0780.

Sincerely,

A handwritten signature in cursive script, appearing to read "Mary Ellen Callahan", followed by a horizontal line extending to the right.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security