UPDATE TO
THE 2008 REPORT
CONCERNING PASSENGER NAME RECORD INFORMATION DERIVED FROM FLIGHTS BETWEEN
THE U.S. AND THE EUROPEAN UNION

Privacy Office
U.S. Department of Homeland Security

February 5, 2010

I. Overview

Purpose: In advance of the 2010 Joint Review of the 2007 U.S. – EU Passenger Name Records (PNR) Agreement, the Department of Homeland Security (DHS) Privacy Office updated its December 2008 Report Concerning Passenger Name Records (2008 Report) derived from flights between the U.S. and EU.[1] The purposes of the update are to: (1) review the status of recommendations contained in the 2008 Report and (2) identify key Customs and Border Protection (CBP) program practices and assess whether such practices continue to comply with the 2007 U.S.-EU PNR Agreement.

Scope: Due to the recency of the 2008 review, the Privacy Office limited the scope of the review to updating the status of the recommendations contained in the 2008 Report and identifying key program practices such as scope of the information sharing conducted to assess compliance with the 2007 U.S.-EU PNR agreement. The DHS Privacy Office conducted the review in January 2010 with the cooperation of CBP officials from the following offices: Office of Chief Counsel, Office of Intelligence and Operations Coordination, Office of Field Operations, Freedom of Information Act (FOIA) Branch, CBP Privacy Office, and DHS Office of Policy.

Methodology: To address the first objective, the Privacy Office reviewed the 2005 and 2008 PNR reports, analyzed relevant CBP documents, processes and directives, and interviewed key CBP officials to assess the implementation status of the recommendations. To address the second objective, the Privacy Office focused on identifying key program policies and practices, such as sharing PNR with external entities, and assessed whether such policies and practices complied with the 2007 U.S. – EU PNR agreement. To do so, the Privacy Office reviewed documents including an accounting of PNR disclosures between August 2008 and January 2010. Additionally, the Privacy Office interviewed key CBP officials from the Office of Intelligence and Operations Coordination, Office of Field Operations, FOIA Branch, and CBP Privacy Office regarding PNR practices, processes, and oversight.

II. Summary of Findings

CBP has taken action to address all six of the recommendations contained in the 2008 Report, which include:

- Publication to the DHS website of a revised Frequently Asked Questions (FAQ) and Privacy Statement reflecting the terms of the 2007 U.S. – EU PNR Agreement;
- Development of a CBP Directive concerning PNR handling to be issued in February 2010; and
- Key improvements to the CBP FOIA Branch practices including a reduction in the backlog of FOIA requests and improvements to address more consistent

[1] A Report Concerning Passenger Name Record Information Derived From Flights between the U.S. and the European Union, December 18, 2008.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf

processing of PNR-related FOIA requests and ensure that individuals requesting their PNR receive information pertaining to them.

The Privacy Office finds that CBP continues to comply with the terms of the 2007 U.S. – EU PNR Agreement.

The Privacy Office also found that key program policies and practices from August 2008 to January 2010, including the scope of how the information is received, used, and disseminated by CBP, continued to comply with the terms of the 2007 U.S. – EU PNR Agreement. Specifically, CBP continues to place filters on the system used to process PNR (using flight numbers and U.S. airport codes) so that it only reviews PNR with a clear nexus to the U.S. and continues to institute automatic masking of sensitive PNR fields. Regarding information sharing practices, the disclosures were found to be appropriate and compliant with the terms of the 2007 U.S. – EU PNR Agreement. CBP appropriately logged the PNR disclosures electronically to make review and reporting easily auditable. There have also been no reports of misuse of PNR to either the DHS Privacy Office or CBP since the 2008 Report.

Further, it should be noted that CBP has made significant progress in encouraging airlines to "push" PNR to CBP. As of January 2010, 13 carriers from the EU have transitioned to the "push" system, an increase of 10 since 2007.

III. Update to 2008 Report Recommendations

In the 2008 Report, the Privacy Office found CBP to be in compliance with the 2007 U.S. – EU PNR Agreement and identified six recommendations for action by CBP aimed at improving its ability to comply with terms of the agreement in the areas of notice, access, and guidance. During the course of the update, CBP provided evidence that it had effectively addressed these recommendations. Accordingly, the Privacy Office considers these recommendations closed. The Privacy Office will continue to monitor compliance with the agreement, continuing to monitor the areas of notice, access, and guidance. The following CBP actions address our December 2008 recommendations.

Recommendation #1: Update the PNR Frequently Asked Questions (FAQ) and Privacy Statement to reflect the 2007 U.S. – EU PNR *Agreement.*

*CBP Action Taken***:** CBP updated the PNR FAQs and Privacy Statement to reflect the 2007 U.S. – EU PNR Agreement. This document can be found at www.cbp.gov under "Travel" (available directly at http://www.cbp.gov/xp/cgov/travel/clearing/pnr/).

Recommendation #2: CBP should fully staff the FOIA/PA program office to reduce any backlog or delay in processing.

CBP Action Taken: Since the December 2008 review, the CBP FOIA Branch has taken significant steps to reduce its backlog. According to CBP FOIA Branch

officials, it reduced its backlog to less than two percent of its highest 2008 levels.[2] This was primarily accomplished through the use of temporary contractor staff. Currently, the CBP FOIA Branch is experiencing an increase in the number of requests as a result of referrals from the U. S. Citizenship and Immigration Services (USCIS) and the new administration's policy on transparency. The CBP FOIA Branch did not identify any extraordinary issues in addressing the current workload volume.

Recommendation #3: CBP should provide more comprehensive training to new and existing staff on FOIA, Privacy Act, DHS policy, the relevant CBP System of Records Notices and applicable exemptions, as well as the use of the Information Technology systems that maintain the information. In particular training is needed on the various search capabilities of the systems involved.

*CBP Action Taken***:** Issues related to inconsistencies in applying exemptions to PNR requests and the need for training on various search capabilities for the source system have been addressed in that all requests related to the Automated Targeting System - Passenger (ATS-P), the system that processes PNR, are processed by a FOIA specialist in the CBP FOIA Branch who has dedicated responsibilities to PNR. This specialist has received advanced training in the search methods available in ATS as well as other traveler-related systems involving border crossing records. Additionally, the specialist's supervisor has had the same training and reviews the materials prior to the disclosure.

Recommendation #4: CBP should develop standard operating procedures that outline which systems are searched and how the search is conducted.

CBP Action Taken: Although the CBP FOIA Branch did not document standard operating procedures, it addressed the intent of the recommendation by providing additional training, assigning a dedicated specialist to process all requests related to ATS-P and PNR, and training the supervisor. After reviewing the PNR requests and responses, CBP found that in most instances individuals were responding to CBP stating that the PNR was not useful, and what was needed was the border entry-exit records. To reduce the number of individuals responding to CBP for additional information and to provide additional transparency to requesters, the CBP FOIA Branch began processing PNR FOIA requests to include border entry-exit records from other DHS systems.

Recommendation #5: CBP should ensure that only PNR information pertaining to the individual requesting the information and no other individual's passenger reservation information, consistent with the ATS SORN, is disclosed.

CBP Action Taken: This recommendation was addressed by the Privacy Office in guidance issued on redacting documents to ensure the greatest level of first party

[2] For further details on DHS FOIA practices see the 2009 FOIA Annual Report, http://www.dhs.gov/xlibrary/assets/foia/privacy_rpt_foia_2009.pdf

access to records while restricting access to third parties, consistent with the spirit and letter of the FOIA and the Privacy Act. Further, as noted in actions taken on the above recommendations, many of these issues are also addressed by having a dedicated FOIA specialist that is well-trained in PNR requirements process all PNR-related requests.

Recommendation # 6: For ease of use, the Privacy Office Recommends DHS, in coordination with CBP, issue a single set of guidance consistent with the SORN and the 2007 Agreement, for use of all DHS offices and components which have or may obtain access to PNR.

CBP Action Taken: CBP developed a Directive on use of PNR in order to provide a consolidated formal framework for the appropriate use, handling and disclosure of PNR stored in ATS-P and to clearly set forth the policy concerning access to PNR. This Directive is to be issued in February 2010.

IV. Ongoing PNR-Related Activities Demonstrate Continued Compliance with the 2007 Agreement

The Privacy Office reviewed ongoing key program policies and practices from August 2008 to January 2010, including the scope of the information reviewed by CBP and information sharing practices with external entities. The Privacy Office found that CBP policies and practices continue to comply with the terms of 2007 U.S. – EU PNR Agreement. Much of the information contained in our 2008 Report remains unchanged, such as the purpose for PNR and the use of data elements in the 19 categories described in the 2007 U.S. – EU PNR Agreement. There have also been no reports of misuse of PNR to either the Privacy Office or CBP since the 2008 Report, and CBP has put in place measures to review account access to PNR on a bi-yearly basis to ensure appropriate access to systems containing PNR.

Listed below are ongoing key program practices in the following areas: scope of PNR reviewed, information sharing practices, and progress in moving air carriers from a "pull" to a "push" method of transmitting PNR to CBP.

Scope of PNR Reviewed

- *Nexus to the U.S.:* Filters remain in place for flights with a nexus to the U.S. CBP accomplished this by programming the system to filter PNR for specific flights with a nexus to the U.S. These PNRs are filtered again so that only those records with a U.S. airport code are retrieved. This process allows the system to filter out those PNR for earlier segments of a flight where the traveler's journey ends before arrival at a U.S. airport. For example, Flight #101 has the routing Mumbai – Manchester – JFK. The system looks for PNR on Flight #101 due to the JFK segment, and then filters out the PNRs of travelers who fly only on the Mumbai-Manchester segment.

- In addition, there is an override mechanism in the system that allows CBP to pull PNR that does not have a U.S. airport code. Authority to use the override mechanism is limited. In order for the override mechanism to be used, 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 override function was added since the 2008 Report and was implemented to address specific cases where the U.S. airport is not recorded in the PNR, but the plane stops at a U.S. airport. For example:
  - A flight from Australia to Canada, where the flight stops in Hawaii to refuel, but the Hawaiian airport code is not in the PNR;
  - A flight from France to Tahiti that stops at Los Angeles International Airport for refueling.

  This functionality may also be used if a flight is diverted because of weather or other reasons and must land unexpectedly in the U.S. DHS is reviewing how the new functionality will be implemented, so as of now only a limited number of CBP officers have system permissions to use this capability. This new override functionality is reviewed by the Office of Information Technology (OIT) in the same way general access to PNR is reviewed by OIT.[3]

- *Data Elements:* Data elements in PNR reviewed by CBP remain limited to the 19 categories defined under the 2007 U.S. – EU PNR agreement. As part of that review, CBP did determine that it needs to change the way in which it receives three data categories (i.e. baggage information, seat assignments, and traveler status). CBP will be working with the airlines on the improved transmission of this information.

- *Sensitive Data:* CBP has put in place automatic masking features for sensitive PNR fields. The Privacy Office saw evidence that the masking mechanisms were working when it reviewed FOIA request case files for PNR as part of this 2010 update.

Information Sharing

- From August 2008 to January 2010, CBP reported through the ATS-P disclosure log that 694 PNR were shared either internally within DHS or externally. This includes both EU and non-EU PNR. When a CBP Officer shares PNR, the Officer must create a log showing to whom the information is shared and for what purpose. The Privacy Office reviewed the ATS-P logs of PNR sharing that occurred during the above mentioned time period, and found these sharing instances to be appropriate and compliant with the terms of the 2007 U.S. – EU PNR Agreement.

[3] 2008 EU Report at 4-5, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf

- Of the 694 PNR sharing instances, 216 were related to the EU PNR. Summaries of the recipients and purposes for sharing the EU PNR are detailed below:

    - Recipients of EU PNR
        - 11% internal DHS components
        - 87% Department of Justice and its components
        - 2% other law enforcement agencies

    - Purposes for Sharing EU PNR
        - 75% for terrorism related cases
        - 18% for transnational crimes
        - 7% for use in law enforcement and/or criminal proceedings (the review showed PNR has been used in one criminal judicial proceeding)

- CBP shared PNR four times with the Centers for Disease Control (CDC) to coordinate responses to health concerns associated with international air transportation. None of this PNR was EU PNR. In these instances, DHS shared information specific to individual travelers rather than the entire flight because of the nature of the health situation.

Increase in Carriers Moving from Pull to Push System of Transmitting PNR

- CBP has increased the number of "push" system carriers with flights to and from the EU by over 400%. As of January 2010, 41 carriers have transitioned to the "push" system. Of these, 13 carriers handle flights to and from the EU. As of 2008, only 13 carriers had transitioned to the "push" system, of which three were carriers with flights to and from the EU.
- For those airlines that are continuing to operate "pull" systems, CBP has provided extensive technical guidance on how to implement a "push" system and how best to interface with CBP once that system is established. CBP does not have the authority to force carriers to implement such a "push" system and the responsibility for initiating a transition to "push" remains with the carriers, which must make resources available to migrate their systems. CBP has reached out extensively to the carriers regarding the need to move to a "push" system.

V. Conclusion

Based on the above update, the Privacy Office finds that CBP continues to comply with the terms of the 2007 U.S. – EU PNR Agreement.