U.S. Department of Homeland Security
U.S. Customs and Border Protection
Washington, DC 20229

Frequently Asked Questions
U.S. Customs and Border Protection
Receipt of Passenger Name Record (PNR) Data

June 21, 2013

United States (U.S.) law requires airlines operating flights to, from, or through the United States to provide the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), with certain passenger reservation data, referred to as Passenger Name Record (PNR) data, which assists CBP in securing the U.S. borders and facilitating safe and efficient international travel. This practice has been widely accepted around the world and is increasingly replicated by foreign border authorities, although some commentators in Europe have questioned the privacy impact of this requirement. The European Union (E.U.) has determined that U.S. laws, in conjunction with DHS/CBP policies regarding the protection of personally identifiable information (PII) and the U.S.-E.U. PNR Agreement signed in December 2011 (2011 Agreement), provide an adequate basis upon which to permit transfers of PNR data to the U.S. consistent with applicable E.U. law.

The updated 2011 Agreement is available at:

http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf.

For a comprehensive explanation of the manner in which DHS/CBP generally handles PNR data, please refer to the Automated Targeting System (ATS) System of Records Notice (SORN), 77 Fed. Reg. 30297 (May 22, 2012) at:

http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

The Privacy Impact Assessment (PIA) for ATS at:

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

1. Why is my Passenger Name Record being transferred to U.S. Customs and Border Protection prior to traveling to, from, or through the United States?

The purpose of collecting PNR information in advance of your arrival or departure is to enable CBP to make accurate, comprehensive decisions regarding which passengers require additional inspection at the port of entry based on law enforcement and other information. Collecting this information in advance provides the traveler two advantages. First, it affords CBP adequate time to research possible matches against derogatory records to eliminate false positives. Second, it

expedites travel by allowing CBP to conduct mandatory checks prior to a flight's arrival in the U.S., rather then making you, and everyone else on your flight, stand in line while we manually conduct the review after you arrive.

DHS/CBP uses PNR strictly for the purposes of preventing, detecting, investigating, and prosecuting:

- Terrorist offenses and related crimes; and
- Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.

PNR is also used where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court and to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

2. What U.S. and E.U. laws allow for the transfer of PNR data?

By statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49d), each air carrier operating passenger flights in foreign air transportation to, from, or through the U.S. must provide CBP with electronic access to PNR data to the extent it is collected and contained in the air carrier's reservation and/or departure control systems.

The E.U. has determined that this statute, in conjunction with DHS/CBP policies regarding the protection of PII and the 2011 Agreement, provide an adequate basis upon which to permit transfers of PNR data to the U.S. consistent with applicable E.U. law. Please note that the 2011 Agreement applies to carriers operating passenger flights between the E.U. and the U.S., as well as those carriers incorporated or storing data in the E.U. and operating passenger flights to, from, or through the United States. For further information regarding this agreement, please refer to the link to the 2011 Agreement provided above.

3. What type of information about me will CBP receive when my PNR is submitted?

Most information contained in PNR data can be obtained by CBP officers at the U.S. port of entry by examining your airline ticket and other travel documents pursuant to CBP's normal border search authority.

Every time you make a reservation for travel, information about that reservation is put into the airline's reservation system. The information, or PNR, provided to CBP may differ depending on the particular air carrier collecting the data since air carriers do not all collect the same set of information. The PNR collected by air carriers and submitted to CBP generally includes the traveler's name, contact details, details of the travel itinerary (such as date of travel, origin and destination, seat number, and number of bags) and details of the reservation (such as travel agency and payment information). The PNR may include other information voluntarily provided by a customer during the booking process (such as affiliation with a frequent flier program).

4. Is sensitive data included in the PNR data transfer?

Sometimes, information that could be considered sensitive could be included in the PNR data transfer. Such sensitive PNR data could include certain information revealing the passenger's racial or ethnic origin, religion, or health. CBP uses electronic filters to automatically mask PNR data identified as sensitive that may be included in the PNR when it is transferred from reservation and/or air carrier departure systems in the E.U. to CBP. This information is not used or seen by any CBP personnel except under exceptional circumstances where the life of an individual could be imperiled or seriously impaired, in which case additional approval and security steps must be taken.

5. What if I'm just transiting the U.S.? Will CBP still be given my PNR?

If you travel on flights arriving in or departing from the U.S. (even if you are simply transiting through the U.S.), CBP may receive PNR data concerning you. Airlines create PNR data in their reservation systems for each itinerary booked for a passenger. Such PNR data may also be contained in the air carrier departure control systems.

6. Who will have access to my PNR data?

CBP and DHS officials responsible for identifying illicit travel and preventing and detecting terrorism and certain transnational crimes will have access to PNR data derived from flights to, from, or through the United States. This PNR data may be provided to other government authorities, as described below.

7. Will my PNR data be shared with other authorities?

PNR data received by CBP in connection with flights to, from, or through the United States may be shared with other government authorities consistent with the purposes identified above in response to FAQ 1 and with the routine uses included in the ATS SORN and other exemptions under the Privacy Act. E.U. PNR data is only exchanged with foreign government authorities after a determination that the recipient's intended use(s) is consistent with the terms of the 2011 Agreement, if applicable, and DHS/CBP policy, and that the recipient has the ability to protect the information.

CBP will ensure in writing that the requesting authority will apply safeguards to the PNR which are comparable to those applied by CBP to ensure that access is granted in accordance with all applicable laws, regulations, DHS policies, and international agreements/arrangements.

8. How long will CBP store my PNR data?

PNR data derived from flights to, from, or through the United States will be kept by CBP for a period of five years in an active file. After the first six months, the PNR will be "depersonalized," with names, contact information, and other personally identifiable information masked in the record. After the five year active period, PNR will be maintained for up to ten years in a dormant database, which requires additional approvals for access. However, PNR

information that is linked to a specific enforcement record will be maintained by CBP until the enforcement record is archived.

9. How will my PNR data be secured?

CBP will keep PNR data from flights to, from, or through the United States secure and in confidence. Careful safeguards, including appropriate data security and access controls, will ensure that the PNR data is not used or accessed improperly.

10. May I request a copy of, or make a correction to, my PNR data that is collected by CBP?

Yes. Any individual, regardless of citizenship who wishes to seek access to his or her PNR held by DHS can do so under the Freedom of Information Act (FOIA). FOIA provides members of the public with access to records, subject to certain exemptions, about the operations and activities of the U.S. federal government. A final agency decision may be judicially challenged under U.S. law. Individuals seeking access to PNR records may submit a FOIA request to CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

The Privacy Act of 1974 (5 U.S.C. 552a) protects the PII the federal government keeps on United States citizens and lawful permanent residents in "Systems of Records." PII is information kept by an agency that can be used to identify an individual when retrieved by name or some other personal identifier, and must be kept in a system of records. The Privacy Act regulates how the government can disclose, share, provide access to, and maintain the personal information that it collects. DHS, as a matter of policy, extends the administrative rights of the Privacy Act, including the rights of access and amendment, to all persons, regardless of citizenship when dealing with mixed systems (systems housing information about both U.S. citizens and foreign nationals). DHS allows persons, including foreign nationals, to seek access and request amendment under the Privacy Act to certain information maintained in ATS-P, including PNR.

Requests for access to PII contained in ATS-P may be submitted to the FOIA Headquarters Office, above. Requests for information should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked “Privacy Act Access Request.” The request should include a general description of the records sought and must include the requester’s full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

However, certain information maintained in ATS-P, such as information pertaining to the rule sets or accounting of a sharing with a law enforcement or intelligence entity in conformance with a routine use, may not be accessed, pursuant to 5 U.S.C. § 552a (j)(2) or (k)(2). In cases where CBP denies access to PNR data pursuant to an exemption under the Privacy Act, such a determination can be administratively appealed to the Chief Privacy Officer of DHS, who is responsible for both privacy protection and disclosure policy for DHS.

Before requesting corrections be made to your PNR, please ask for a copy of the record through the processes described above to determine what information is actually in your PNR record(s). Keep in mind that PNR is usually information that you (or your representative) supplied yourself – so there is very little probability that the PNR we have is incorrect. Requests for amendment should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting amendment to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Amendment Request." The request must include the requester's full name, current address, and date and place of birth. Your request should identify each particular record in question, state the amendment or correction that you want, and state why you believe that the record is not accurate, relevant, timely, or complete. You may submit any documentation that you think would be helpful. The request must be signed and either notarized or submitted under penalty of perjury.

11. Whom do I contact in the U.S. regarding this program?

Access Requests: If you wish to seek access to PNR data about you that is held by CBP, you may mail a request to the CBP FOIA Headquarters Office through the procedures in FAQ 11.

For further information regarding the procedures for making such a request, you may refer to Title 19, Code of Federal Regulations, Part 103 or www.dhs.gov/foia.

Concerns, Complaints, and Correction Requests:

The DHS Traveler Redress Inquiry Program (TRIP), accessible at www.dhs.gov/trip, provides a means for all individuals, regardless of citizenship, to appeal a security determination and to seek correction of erroneous information that may result in travel delays or misidentification. TRIP does not involve individual access to one's records, but rather provides a structured method of review.

Questions, concerns, or comments of a general or specific nature regarding CBP or its handling of PNR may be directed to the CBP INFO Center. You may contact the CBP INFO Center in any one of three ways:

Online - Through the "Questions" tab at: www.cbp.gov

Telephone- During the hours of 8:30 a.m. to 5:00 p.m. Eastern Time:
(877) 227-5511 (toll-free call for U.S. callers)
(202) 325-8000 (international callers)
(866) 880-6582 (TDD)

Mail - U.S. Customs & Border Protection
OPA/CBP INFO Center
1300 Pennsylvania Avenue N.W., MS: 1345
Washington, DC 20229

In order to verify your identity, you will need to provide as much identifying information as possible (such as your full name, current address, and date and place of birth) or send us a clear copy of your passport photo page as well as your signed request for a review or redress regarding your PNR information or your experience. If you are unable to provide proof that you are the subject of the record you are requesting, we may be unable to respond to your request.

Decisions by CBP regarding such requests may be reviewed by the Chief Privacy Officer of the Department of Homeland Security, Washington, DC 20528-0550; Email at privacy@hq.dhs.gov; Phone: (202) 343-1717; and Fax: (202) 343-4010. An inquiry, complaint, or request for correction of PNR data may also be referred by an E.U. passenger to the Data Protection Authority (DPA) within their E.U. Member State for further consideration as may be deemed appropriate.

12. Whom do I contact if my complaint is not resolved?

In the event that a complaint cannot be resolved by CBP, the complaint may be directed, in writing, to the Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528-0550; Email at privacy@hq.dhs.gov; Phone: (202) 343-1717; and Fax: (202) 343-4010. The Chief Privacy Officer shall review the situation and endeavor to resolve the complaint.

Complaints received from the European Union Member States on behalf of an E.U. resident, to the extent such resident has authorized the DPA to act on his or her behalf shall be handled on an expedited basis.

13. What is the role of the Chief Privacy Officer of the Department of Homeland Security?

Pursuant to the Homeland Security Act of 2002, as amended (6 U.S.C. § 142) and Section 802 of the Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53), the DHS Chief Privacy Officer is statutorily obligated to ensure that personally identifiable information is handled in a manner that complies with relevant law. He or she exercises oversight of compliance with the PNR agreement to ensure strict compliance by DHS and to verify that proper safeguards are in place. He or she is independent of any directorate within DHS. His or her determination is binding on the Department.