Privacy Impact Assessment Update
for the

Advanced Passenger Information System (APIS)

DHS/CBP/PIA – 001(e)

June 23, 2011

Contact Point
Robert Neumann
Office of Field Operations
U.S. Customs and Border Protection
202-344-2605

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is updating the Privacy Impact Assessment (PIA) for the Advanced Passenger Information System (APIS) in order to provide further notice of the expansion of routine sharing of APIS with the intelligence community in support of the Department's mission to protect the United States from potential terrorist activities.

Introduction

The Aviation and Transportation Security Act of 2001 and the Enhanced Border Security and Visa Reform Act of 2002 together mandated the collection of certain information on all passenger and crew members who arrive in or depart from (and, in the case of crew members, overfly) the United States on a commercial air or sea carrier. The information required to be collected and submitted to APIS can generally be found on routine entry documents that passenger and crew members must provide when being processed into or out of the United States. The APIS information includes full name, date of birth, citizenship, passport/alien registration card number, passport/alien registration card country of issuance, passport expiration date country of residence, passenger name record locator number, and U.S. destination address (where applicable). The APIS information is collected in advance of a passenger's departure from or arrival into (and in many cases, prior to departure for) the United States. APIS information is also collected for each individual aboard a private aircraft arriving in or departing from the United States.

The purpose of this collection is to perform law enforcement queries and to identify high risk passengers and crew members who may pose a risk or threat to vessel or aircraft safety or to national security, while simultaneously facilitating the travel of legitimate passengers and crew members. This information collection also assists in expediting processing of travelers at ports of entry, resulting in a significant time savings.

Pursuant to the National Security Act of 1947, as amended, the National Counter Terrorism Center (NCTC) "serve[s] as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support," 50 U.S.C. § 404o. In order to enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 27, 2005), which provides that the Head of each agency that possesses or acquires terrorism information shall promptly give access to that information to the Head of each other agency that has counterterrorism functions. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (Pub. L. No. 108-458), as

amended, places an obligation on U.S. government agencies to share terrorism information with the intelligence community, including NCTC. In certain instances, DHS shares the entire dataset with an intelligence community member in order to support the counterterrorism activities of the intelligence community and to identify terrorism information within DHS data. DHS has decided to share the entire APIS database with NCTC under a Memorandum of Understanding (MOU). The MOU permits NCTC to use APIS information to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. The MOU includes a number of safeguards to ensure the data is only used for the purposes explicitly permitted under the MOU, this PIA, and the DHS/CBP – 005 Advance Passenger Information System of Records Notice (SORN), 73 FR 68435, November 18, 2008.[1] The MOU also limits the amount of time the information is maintained at NCTC, ensures proper information technology security is in place during and after transmission of the APIS data to NCTC, requires deletion, requires training for staff accessing APIS, and provides for routine reporting and auditing of NCTC's use of the data.

Reason for the PIA Update

DHS/CBP is updating the existing DHS/CBP/PIA – 001 APIS, first published on March 21, 2005 and updated subsequently on August 9, 2007, September 11, 2007, November 18, 2008, and February 19, 2009,[2] to account for the routine sharing of APIS data with the intelligence community, including NCTC. DHS has entered into a MOU with NCTC in order to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. DHS and NCTC have placed specific safeguards in MOU to ensure that the data is used appropriately and in accordance with the existing SORN, DHS/CBP – 005 Advance Passenger Information System of Records, November 18, 2008, 73 FR 68435, and this PIA.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

There is no change in the collection of APIS records. As noted in the DHS/CBP/PIA-001(c) 2008, APIS includes the following from all travelers (passengers and crew):

- Complete name;
- Date of birth;

[1] Available at: http://edocket.access.gpo.gov/2008/E8-27205.htm.
[2] Available at: http://www.dhs.gov/files/publications/gc_1281020492905.shtm.

- Gender;
- Country of citizenship;
- DHS-approved travel document type (e.g., Passport, Merchant Mariner Document, Nexus Air Card, Alien Registration Card, etc.,);
- Travel document number and country of issuance;
- Travel document expiration date;
- Country of residence;
- Status on board the aircraft or vessel (whether individual is crew or non-crew);
- U.S. destination address (except for passengers who are U.S. citizens or lawful permanent residents, commercial crew, and persons in transit);
- Place of birth and address of permanent residence (commercial flight crew only);
- Passenger name record (PNR) locator number (commercial passengers);
- Pilot license/certificate number and country of issuance, (commercial and private flight crew only);
- Vessel information (name, country of registry, IMO number, and voyage number);

Uses of the System and the Information

DHS/CBP has not changed the uses of the information.

Retention

The DHS retention period for APIS has not changed. The information initially collected by APIS is used for entry screening purposes and is retained in APIS for no more than twelve months.

Data obtained through the APIS transmission is copied to the Border Crossing Information (BCI) system, another subsystem of TECS,[3] during the process of vetting an individual traveler or crew member. The information copied from APIS into BCI includes: complete name, date of birth, gender, date of arrival, date of departure, time arrived, means of arrival (air/sea), primary inspection lane, ID inspector, travel document, departure location, airline code and flight number (as appropriate), related vessel documentation (if appropriate, to include: port of entry, entry date, port of departure, departure date and status on board the vessel), and result of the CBP processing. The data copied from APIS into BCI will be retained in accordance with the record retention period for BCI.

[3] The PIAs and SORNs for both DHS/CBP/BCI and DHS/CBP/TECS can be found at www.dhs.gov/privacy.

Data regarding individuals subject to US-VISIT requirements is obtained through the APIS transmission and is copied to the Arrival and Departure Information System (ADIS)[4] including: the above information and U.S. destination address, passport number, expiration date of passport, country of issuance (for non-immigrants authorized to work), alien registration number, country of residence, U.S. destination address, and expiration date of passport. The copied data is retained in accordance with the retention schedules approved for ADIS.

NCTC will be allowed to retain APIS records for up to 180 days in order to identify terrorism information, in support of its counterterrorism mission and in support of the mission of DHS. APIS records will be deleted by NCTC within 180 days of receipt unless a nexus to terrorism has been identified for a particular record. NCTC may retain APIS data containing terrorism information in accordance with NCTC authorities and policies, applicable law, and the terms of the MOU.

Internal Sharing and Disclosure

No changes have been made to internal sharing. Non-United States Citizen (USC) data from APIS is systematically shared with US-VISIT in order to build the ADIS system to identify immigrants and non-immigrants.

External Sharing and Disclosure

DHS has entered into a new sharing agreement with NCTC in order to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. This sharing is conducted pursuant to routine use H of the APIS SORN, which states that DHS may share APIS information with "a federal, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive."

NCTC will process all APIS records within 180 calendar days of receipt from DHS to determine whether a nexus to terrorism exists. NCTC will immediately purge all APIS records that do not constitute terrorism information no more than 180 calendar days from receipt. This process will be audited as required under the MOU. NCTC will review, retain, and disseminate APIS records it has determined have a nexus to terrorism in accordance with procedures approved for NCTC by the Attorney General in accordance with Section 2.3 of Executive Order 12333, and additional terms specified in the MOU.

The MOU has strict safeguards to protect PII provided to NCTC. These protections include a routine oversight of NCTC's use of the data by DHS personnel detailed to NCTC. In

[4] The PIA and SORN for DHS/NPPD/US-VISIT/ADIS can be found at www.dhs.gov/privacy.

addition, training has been provided to NCTC users on the appropriate use of PII. DHS/CBP will provide annual and periodic training to appropriate NCTC personnel on proper interpretation of the data contained in APIS and on proper treatment of data from certain categories which require special handling, such as asylum, refugee, and U.S. Person data.

NCTC may not disseminate to third parties information derived from APIS data, unless that data was identified as containing terrorism information. NCTC shall maintain an electronic copy and accounting of the APIS data that was disseminated, to whom, and the purpose for the dissemination.

Additionally, this external sharing, outside of DHS, is being appropriately logged pursuant to subsection (c) of the Privacy Act, which requires the Department to maintain a log of when records have been shared outside of DHS. In accordance with the APIS SORN,5 DHS has exempted this accounting for disclosure required by subsection (c) from the access provisions of subsection (d).

Notice

The APIS SORN was last published in the *Federal Register* on November 18, 2008, 73 FR 68435, and remains accurate and current. Routine Use H covers this sharing.

Individual Access, Redress, and Correction

No changes have been made to access, redress, and correction.

DHS allows persons, including foreign nationals, to seek administrative access under the Privacy Act to certain information maintained in APIS. Requests for access to PII contained in APIS that was provided by the commercial air or vessel carrier or private pilot regarding the requestor may be submitted to:

U.S. Customs and Border Protection
FOIA Division
799 9th Street NW, Mint Annex
Washington, DC 20229-1177

However, records and information maintained in APIS pertaining to the results of the vetting of the traveler may not be accessed.

Requests for access 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

[5] Available at: http://edocket.access.gpo.gov/2008/E8-27205.htm.

submitted under penalty of perjury.

Individuals, including foreign nationals, may also seek redress through the DHS Traveler Redress Program ("TRIP"). See the DHS/ALL – 005 Redress and Response Records SORN, 72 FR 2294, January 18, 2007).[6] Persons who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through DHS TRIP. DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs such as airports, seaports and train stations, or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in APIS and other data stored in other DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

Technical Access and Security

The new sharing of information with NCTC will be conducted in conformance with existing information technology security protocols, including encryption.

Technology

No changes.

Responsible Officials

Kim Mills, Director, Traveler Entry Programs, Office of Field Operations, U.S. Customs and Border Protection, U.S. Department of Homeland Security, (202) 344-3007.

Laurence Castelli, CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, U.S. Department of Homeland Security, (202) 325-0280.

Approval Signature

Final Signed Version on File with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security

[6] Available at: http://edocket.access.gpo.gov/2008/E8-27205.htm.