Privacy Impact Assessment Update
for the

Advance Passenger Information System
For
Customs and Border Protection's
General Aviation
Notice of Proposed Rulemaking

September 11, 2007

Contact Point
Robert Neumann
Program Manager
US Customs and Border Protection
(202) 344-2605

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

This is an update to the previous Advanced Passenger Information System (APIS) privacy impact assessment (August 8, 2007) to discuss an expansion of the scope of the APIS data collection to include non-commercial aviation. In conjunction with this update, CBP is publishing a Notice of Proposed Rulemaking that amends the CBP regulations contained in 19 CFR Part 122 addressing the advance electronic submission of information for private aircraft arriving in, departing from, continuing and overflying the United States.

Introduction

U.S. Customs and Border Protection (CBP), a component within the Department of Homeland Security (DHS), currently collects from commercial carriers personally identifying information about passengers and crewmembers traveling by air or sea, and arriving in, departing from, (and, in the case of crew, flights overflying or continuing domestically within), the United States. This information, often collected and maintained on what is referred to as the passenger manifest, can be found on routine travel documents that passengers and crew members must provide when processed into or out of the United States; most of the information is included on the Machine Readable Zone (MRZ) of a person's passport. Once collected, the information is transmitted to CBP through the Advanced Passenger Information System (APIS), an electronic data interchange system used by DHS for international commercial air and vessel carriers.

By receiving the advanced passenger and crew information, CBP is able to perform enforcement and security queries against various multi-agency law enforcement and terrorist databases and identify high risk passengers and crew members who may pose a risk or threat to vessel or aircraft security or to national or public security or of non-compliance with U.S. civil and criminal laws, while simultaneously facilitating the travel of legitimate passengers and crew members.

In order to provide the nation, private aircraft operators, and the international traveling public security, and fulfill its border enforcement mission, CBP needs to be able to accurately assess the threat risk of private aircraft and those individuals traveling via private aircraft. Therefore, CBP is issuing a Notice of Proposed Rulemaking to amend its regulations to create security standards that mirror the existing security standards in the commercial environment by requiring the advance electronic transmission of information by private aircraft arriving from, departing, continuing within, or overflying the United States. This PIA updates the original APIS PIA and addresses the proposed expansion of this collection relating to non-commercial aviation. In connection with this PIA update, the NPRM for General Aviation, and the notice and comment

period for the APIS System of Record Notice (published on August 24, 2007 at 72 FR 48349) will be updated accordingly.

Under the proposed regulations, CBP intends to require the pilot of any private aircraft arriving in the U.S. from a foreign port or location or departing the United States for a foreign port or location to transmit notice to CBP, via the Electronic Advanced Passenger web-based eAPIS portal, an advance submission of information regarding each individual traveling onboard the aircraft. This manifest data would include the following information for all individuals aboard the aircraft: full name, date of birth, gender, citizenship, country of residence, status on board the aircraft (*i.e.*, passenger or crew member), travel document type (*e.g.*, passport, alien registration card), passport number (if a passport is required, or approved DHS travel document), travel document country of issuance, travel document expiration date, alien registration number, redress number (if available),[1] and address while in the United States.

Additionally, under the proposed regulations, CBP intends to add data elements to and modify the time frame for existing notice of arrival requirements for private aircraft, and require a new notice of departure requirement. The notice of arrival and notice of departure would include the following information regarding the aircraft: aircraft registration number, type of aircraft, call sign (if available), decal number, place of last departure, date of aircraft arrival (or departure, for departure notice), estimated time of arrival (or departure, for departure notice), estimated time and location of crossing U.S. border/coastline, name of intended airport of first landing[2] (or name of intended foreign airport of first landing, for departure notice), owner/lessee name (first, last and middle, if available), owner/lessee address (number and street, city, state, zip code, country, telephone number, fax number and email address), pilot/private aircraft pilot name, pilot license number, pilot street address (number and street, city state, zip code, country, telephone number, fax number and email address), pilot license country of issuance, operator name (last, first and middle, if available), operator street address (number and street, city, state, zip code, country, telephone number, fax number and email address), transponder code, color, complete itinerary (foreign airports landed at within past 24 hours prior to landing in U.S.), and 24-hour point of contact (*e.g.*, broker, dispatcher, repair shop, etc.) name and telephone number. The notice of arrival and departure information would have to be submitted to CBP through eAPIS in the same transmission as the corresponding departure or arrival passenger manifest information. This data would have to be received by CBP no later than 60 minutes before an arriving private aircraft departs from a foreign location and no later than 60 minutes before a private aircraft departs a United States airport or location for a foreign port or place.

---

[1] The redress number is the number assigned by DHS to an individual processed through the redress procedures described in 49 CFR Part 1560, Subpart C.

[2] As listed in 19 CFR 122.24, if applicable, unless an exemption has been granted under 19 CFR 122.25, or the aircraft was inspected by CBP Officers in the U.S. Virgin Islands.

Lastly, although unrelated to data collection, the new regulations clarify landing rights procedures and departure clearance procedures as well as expressly setting forth CBP's authority to restrict aircraft from landing in the United States based on security and/or risk assessments; or, based on those assessments, to specifically designate and limit the airports from where aircraft may land or depart.

Reason for the PIA Update

In accordance with the Section 222 of the Homeland Security Act of 2002, this PIA update is required by the proposed amendment of CBP regulations that intend to expand the electronic collection of APIS data elements to include General Aviation.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

The proposed regulations mandate the electronic collection of APIS data from a new category of persons; previously, no advance electronic personally identifying information was collected with regard to travelers (passengers or crew members (including pilots) as discussed in this PIA update, the APIS PIA, and the APIS System of Records Notice) arriving in the U.S. by private aircraft. For every individual on the aircraft, arriving and departing, the data elements to be collected will include: full name, date of birth, gender, citizenship, country of residence, status on board the aircraft (*i.e.*, passenger or crew member), travel document type (*e.g.*, passport, alien registration card), travel document country of issuance, travel document expiration date, alien registration number, redress number (if available),[1] and address while in the United States. Additionally, incident to the transmission of the manifest via eAPIS, the email address of the pilot will be collected.

The proposed regulations will require the advance electronic collection of additional data elements pertaining to the private aircraft, including: aircraft registration number, type of aircraft, call sign (if available), decal number, place of last departure, date of aircraft arrival, estimated time and location of crossing U.S. border/coastline, name of intended airport of first landing,[2] owner/lessee name (first, last and middle, if available), owner/lessee address (number and street, city, state, zip code, country, telephone number, fax number and email address), pilot/private aircraft pilot name, pilot license number, pilot street address (number and street, city state, zip code, country, telephone number, fax number and email address), pilot license country of

[1] The redress number is the number assigned by DHS to an individual processed through the redress procedures described in 49 CFR Part 1560, Subpart C.

[2] As listed in 19 CFR 122.24, if applicable, unless an exemption has been granted under 19 CFR 122.25, or the aircraft was inspected by CBP Officers in the U.S. Virgin Islands.

issuance, operator name (last, first and middle, if available), operator street address (number and street, city, state, zip code, country, telephone number, fax number and email address), transponder code, color, complete itinerary (foreign airports landed at within past 24 hours prior to landing in U.S.), and 24-hour point of contact (e.g., broker, dispatcher, repair shop, etc.) name and telephone number.

The proposed collection of these elements will increase the amount of PII collected from passengers of private aircraft because a broader population will now be covered by the APIS rule. Additionally, with this rule CBP will be collecting information on owner/lessee of the private aircraft and additional types of personally identifiable information for pilots. Given the variance in operating environment of commercial aircraft as compared to a private aircraft this additional information is required to enable CBP to meet its border enforcement and security mission as mandated by the Homeland Security Act of 2002.

Uses of the System and the Information

There are no new uses of data currently being collected for APIS based on this update. As described in the previous PIA, the information that is collected is used to perform counterterrorism, law enforcement, and public security queries to identify risks to the aircraft, to its occupants, or the United States, and to expedite CBP processing.

Retention

Data retention for APIS is unchanged as a result of this update. As described in the previous PIA, information initially collected by APIS is used for entry screening purposes and is retained for no more than twelve (12) months.

Data obtained through the APIS transmission is copied to the Border Crossing Information System, (BCIS), a subsystem of the Treasury Enforcement Communications System (TECS), during the process of vetting an individual traveler or crew member. The information copied from APIS into BCIS 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, and result of the CBP processing. The data copied from APIS into the BCIS database of TECS will be retained in accordance with the record retention period for TECS. The Systems of Record Notice (SORN) for TECS was last published on October 18, 2001 (66 FR 52984).

Data regarding individuals subject to US-VISIT requirements is obtained through the APIS transmission is also copied to the Arrival and Departure Information System (ADIS) including: complete name, date of birth, gender, citizenship, country of residence, status on board the vessel, U.S. destination address, passport number, expiration date of passport, country of issuance (for non-immigrants authorized to work), alien registration number, port of entry, entry date, port of departure, departure date, country of residence, status on board the vessel, U.S. destination address, and expiration date of passport. The copied data is retained in accordance with the

retention schedules approved for ADIS. The SORN for ADIS was published on December 12, 2003 (68 FR 69412) and updated on August 22, 2007 (72 FR 47057). The PIA for ADIS was originally published on December 18, 2003 and updated on August 1, 2007.[1]

Internal Sharing and Disclosure

There are no new data disclosures within CBP as a result of this update.

External Sharing and Disclosure

After receipt of the manifest information, the CBP system performs an initial security vetting of the data and sends to the pilot or manifest submitter, by a non-interactive transmission back to the e-mail address from which the manifest was submitted, one of three possible responses: either an approval or grant of landing rights, a denial of landing rights, or a restriction of landing rights by directing the aircraft to a specific airport for arrival.

Message information conveyed to pilots may not be disclosed to any passenger, crew member, or other person without DHS permission and the pilots must undertake appropriate measures to protect the information from unauthorized access and dissemination. Pursuant to the Air Transportation Security Act (ATSA), specifically, title 49 United States Code (U.S.C.) § 114, and 19 U.S.C. § 1644a, DHS may subject pilots to applicable civil, administrative and criminal sanctions for the unauthorized disclosure of message information.

To make determinations relating to landing rights, DHS uses the consolidated terrorist watch list of known and suspected terrorists maintained by the Terrorist Screening Center (TSC) of the Department of Justice (DOJ) to vet passengers and crew members traveling on flights to and from the United States and on cruise vessels departing from the United States. The transmission of incomplete passenger data may prevent proper vetting of the passenger by the system. This will generate a "not-cleared" response.

Through an analysis of the data provided by the pilot's transmission, DHS will be able to identify passengers that are designated as selectee or no-fly. This and other information will be used in determining whether landing rights or clearance will be granted, restricted or denied. DHS is evaluating the advisability of disclosing to the pilot the identity of individual passengers that are selectee or no-fly matches so that the pilot may better understand potential threats to the security of the aircraft. Accordingly, DHS is soliciting public comments on the economic costs and benefits of notifying a pilot about an individual selectee or no-fly match being aboard the aircraft. DHS is also seeking comments on any operational and privacy concerns associated with sharing such information.

[1] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_inc1.pdf;
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_adis_2007.pdf

Notice

Notice will be provided by this PIA update, as well as the related Notice of Proposed Rulemaking. CBP strongly recommends that the pilot inform each passenger that his or her personal data has been reported to APIS. Through the notice of proposed rulemaking, CBP is seeking comments on, and will evaluate methods for providing a Privacy Act Statement to individual passengers. The General Aviation population, however, is unique in that many passengers are fractional owners, family members, or close associates of the pilot, and may travel without the benefit of formal reservation, ticketing, or check-in procedures such that individual notice is exceedingly difficult or impractical.

DHS is seeking comment on the privacy impacts of the expansion of the population that will be covered by this rule. Presently, the Advanced Passenger Information System (APIS) System of Records Notice (SORN) published in the Federal Register on August 23, 2007 (72 FR 48349) would cover this population. The APIS SORN currently covers the collection of APIS information in both the commercial and private aircraft context. Comments will be considered and addressed in the development of this final rule, additionally any updates to the APIS SORN required by the rule or DHS's analysis of the comments from this NPRM will be incorporated into the APIS SORN prior to the collection of personally identifiable information under the rule.

Individual Access, Redress, and Correction

No changes have been made to individual access, redress and correction as a result of this update. As described in the previous PIA, CBP has a FOIA/Privacy Act Branch in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems (including APIS). If a traveler (passenger or crew) believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to the FOIA/Privacy Act Branch at the following address: FOIA/Privacy Act Branch, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229, fax (202) 344–2791. Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue. Individuals may provide additional information to CBP to ensure that the information maintained by CBP is accurate and complete. The FOIA/Privacy Act Branch will respond in writing to each inquiry.

Technical Access and Security

No changes have been made to technical access and security as a result of this update. CBP will evaluate the need for increased auditing to ensure that APIS and eAPIS are not abused or manipulated in any way.

Technology

No technology has changed as a result of this update.

Responsible Official

Laurence E. Castelli, Chief

Privacy Act Policy and Procedures Branch

U.S. Customs and Border Protection

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security