Privacy Impact Assessment
for the

Advance Passenger Information System

APIS

November 18, 2008

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

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

Abstract

CBP is issuing a Final Rule to amend regulations governing the submission of Advanced Passenger Information System (APIS) data to include private aircraft. CBP is publishing a revised PIA and a revised associated System of Records Notice to include these final changes with its existing APIS privacy notices. The previous System of Records Notice for the APIS system was last published at 72 FR 48349, August 23, 2007. On September 18, 2007, CBP published a Notice of Proposed Rulemaking in the Federal Register (72 FR 53393) proposing amendments to CBP regulations concerning the advance electronic transmission of passenger and crew manifests for private aircraft arriving in and departing from the United States, commonly referred to as APIS. A PIA update was published on the DHS web site at the same time discussing the impact of the notice of proposed rule.

Introduction

To implement the statutory mandates provided by the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), CBP, a component within the Department of Homeland Security, currently collects from commercial carriers personally identifying information about passengers and crew members 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 collection of passenger and crew manifest data. The purpose of this collection is to identify high risk passengers and crew members who, for example, may pose a risk or threat to vessel or aircraft safety or to national security, while simultaneously facilitating the travel of legitimate travelers. This information collection also assists CBP officers at ports of entry in directing resources, resulting in more effective and efficient customs and immigration processing.

In order to ensure the security of the nation, private aircraft operators, and the international traveling, and fulfill its border enforcement mission, CBP must accurately assess the threat risk of private aircraft and those individuals traveling via private aircraft. Accordingly, under the authority provided to it by the Tariff Act of 1930, as amended, CBP issued a Notice of Proposed Rulemaking (NPRM) on September 18, 2007, to amend its regulations to create security standards similar to those utilized in the commercial air environment by requiring the advanced electronic transmission of manifest information by private aircraft arriving in and departing from the United States. In connection with that NPRM, on September 11, 2007, CBP published a Privacy Impact Assessment Update for APIS to discuss the proposed expansion of the scope collection of the APIS data collection to include non-commercial aviation.

In accordance with the NPRM published on September 18, 2007, CBP is now issuing a Final Rule that will require the advance electronic submission of information. This PIA incorporates the interim September 11, 2007 PIA Update, and updates the original APIS PIA, issued August 8, 2007, to reflect the collection of data from private aircraft as well as commercial aviation and vessel carriers. Lastly, this PIA, in conjunction with a separate Privacy Impact Assessment for the collection of Rail and Bus information

prepared in response to provisions of the 9/11 Commission Act of 2007, encompasses the full collection of advanced passenger information (whether mandatory or voluntarily provided by carriers) that is received by CBP from carriers or operators, on behalf of the traveling public. The APIS-Rail and Bus PIA will discuss those requirements relating to the voluntary submission of rail and bus manifest information, separately. As a further note, a separate PIA for the Electronic System for Travel Authorization (ESTA) was published on June 2nd, 2008.

The information that is collected will be used to identify high risk passengers and crew members who may pose a risk to border, aviation or public security, may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists, may be inadmissible, may be a person of interest, or may otherwise be engaged in activity in violation of U.S. law, or the subject of wants or warrants. The system allows CBP to facilitate effectively and efficiently the entry and departure of legitimate travelers into and from the United States. Using APIS, officers can quickly reference the results of the advanced research that have been conducted through CBP's law enforcement databases, the Department of State's Passport Records Systems, as well as using the Federal Bureau of Investigations Terrorist Screening Center's Terrorist Screening Database (TSDB), information on individuals with outstanding wants or warrants, and information from other government agencies regarding high risk parties; confirm the accuracy of that information by comparison with information obtained from the traveler and from the carriers; and make immediate determinations as to a traveler's security risk and admissibility and other determinations bearing on CBP's inspectional and screening processes.

Information collected in APIS is maintained for a period of no more than twelve months from the date of collection at which time the data is erased from APIS. During the vetting process, information submitted to APIS is copied to Border Crossing Information (BCI) and as appropriately determined during CBP's admissibility decision regarding the traveler, the Treasury Enforcement Communication System (TECS), which is being revised and will be republished as TECS (no longer an acronym). During physical processing at the border, primary inspection lane and ID inspector are added to APIS and the APIS information is verified. 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 or sea), primary inspection lane, ID inspector, travel document, departure location, airline code, flight number, and the result of the CBP processing.

Additionally, for individuals subject to US-VISIT requirements[1], certain APIS data is copied to the Arrival and Departure Information System (ADIS) for effective and efficient processing of foreign nationals. The SORN for ADIS was published on December 12, 2003 (68 FR 69412) and updated on August 22, 2007 (72 FR 47057). The information copied from APIS to ADIS includes: complete name, date of birth, gender, country of citizenship, passport/alien registration number and country of issuance (for non-immigrants authorized to work), 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.

As noted above, this PIA incorporates the discussions of the previous three PIAs (published March 21, 2005, August 9, 2007, and September 11, 2007) so that there is a consolidated discussion of how the Department collects, maintains, and disseminates APIS information the provision of which is mandated by law. A separate PIA related to rail and bus APIS information, voluntarily provided by carriers to CBP, will be published in the near future.

[1] US-VISIT currently applies to all visitors (with limited exemptions).

System Overview

As charged by Congress, DHS is deploying a fully automated electronic travel system. In support of this requirement, CBP has developed a system that includes an internet-based application and attendant vetting mechanism that will accommodate the entry of information by the pilots of private aircraft (*i.e.*, passenger manifest and arrival/departure notice), the vetting of the application by DHS, and the return notification to grant, deny or restrict landing rights as appropriate.

Pursuant to the new regulations, both the manifest and notice of arrival/departure must be transmitted in the same transaction via electronic submissions through the Electronic Advanced Passenger Information System (eAPIS) web portal or by a CBP-approved alternative transmission medium. The pilot would be responsible for submitting this information, but could authorize another party to submit the information on his or her behalf.

Pilots of private aircraft arriving in the United States from a foreign port or location are required to transmit notice to CBP through a CBP-approved electronic data interchange system no later than 60 minutes prior to departure from a foreign port or location. Aircraft that are not originally destined for the United States but are diverted to the U.S. due to an emergency are required to transmit an arrival manifest no later than 30 minutes prior to arrival. The data elements required for the notice of arrival report include the following: aircraft tail number, type of aircraft, call sign (if available), CBP issued decal number (if available), place of last departure, date of aircraft arrival, estimated time of arrival, estimated time and location of crossing U.S. border/coastline, name of intended U.S. airport of first landing, owner/lessee name and address, pilot name and address, pilot license number and country of issuance, operator name and address, aircraft color(s), complete itinerary, and 24-hour Emergency point of contact. After CBP receives the submitted arrival notice information, CBP will send a message to the submitter of the manifest information before departure from a foreign airport indicating that the information has been received and specifying whether landing rights have been granted at the requested airport, granted at a different airport designated by CBP, or denied.

Additionally, private aircraft pilots arriving in the United States are responsible for submitting passenger manifest information no later than 60 minutes prior to departure from a foreign port or location that provides identifying information for all individuals on board the aircraft. The manifest data must be provided simultaneously with the notice of arrival information and must 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), DHS-approved travel document type, travel document number, travel document country of issuance, travel document expiration date, alien registration number (if applicable), and address while in the United States. The pilot collecting the manifest information is required to compare the manifest information with the information on the DHS-approved travel document presented by each individual attempting to travel onboard the aircraft to ensure that the manifest information is correct, that the travel document appears to be valid for travel purposes, and that the traveler is the person to whom the travel document was issued. If additional passengers not included in the manifest board the aircraft after the manifest data was submitted to CBP, the pilot is responsible for submitting a corrected manifest. The pilot is required to await CBP approval of the corrected manifest before departing; any previously-granted landing approval is invalidated. If a subsequent arrival manifest is submitted less than 60 minutes prior to departure, the private aircraft pilot must resubmit the arrival manifest and receive approval from CBP for the amended manifest containing the added or amended information before allowing the aircraft to depart the foreign location. After receipt of the manifest information, CBP will perform an initial security vetting of the data and grant, deny, or restrict landing rights appropriately. If landing rights are restricted or denied, the pilot will be provided with appropriate instructions and contact information.

Lastly, pilots of private aircraft departing the United States to a foreign port or location must submit a departure manifest and a departure notice to CBP no later than 60 minutes prior to departure. The data elements required for the notice of departure report include the following: aircraft tail number, type of aircraft, call sign (if available), CBP-issued decal number (if available), place of last departure, date of aircraft departure, estimated time of departure, estimated time and location of crossing U.S. border/coastline, name of intended foreign airport of first landing, owner/lessee name and address, pilot name and address, pilot license number and country of issuance, operator name and address, aircraft color(s), complete itinerary, and 24-hour Emergency point of contact. The manifest data must be provided simultaneously with the notice of departure information and must 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), DHS-approved travel document type, travel document number, travel document country of issuance, travel document expiration date, alien registration number (if applicable), and address while in the United States. As with the arrival manifest, the pilot collecting the manifest information is required to compare the manifest information with the information on the DHS-approved travel document presented by each individual attempt to travel onboard the aircraft to ensure that the manifest information is correct, that the travel document appears to be valid for travel purposes, and that the traveler is the person to whom the travel document was issued. If a departure manifest is submitted to CBP before all individuals arrive for transport, the pilot must resubmit and amended manifest with all required information; any clearance previously granted would be invalidated. If changes are submitted less than 60 minutes prior to departure, the pilot would be required to receive a new clearance from CBP before departing.

The process of receiving electronic clearance to depart is substantially the same as that in reporting arrival. Upon the transmission of the notice of departure and departure manifest to CBP, the private aircraft pilot must await CBP's confirmation of receipt of the manifest data and await CBP's clearance to depart the United States.

Whether collected in conjunction with the arrival or departure of private aircraft, commercial aircraft, or vessels, the purpose of this collection is to identify high risk passengers and crew members who may pose a risk or threat to aircraft or vessel 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. As mentioned above, this information collection also assists CBP officers in properly directing resources, resulting in efficient and effective customs and immigration processing at ports of entry. In keeping with the requirements of Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act, the mandatory collection of information required by APIS is the subject of this Privacy Impact Assessment.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is to be collected?

The information to be collected from all travelers (passengers and crew members) consists of:

- Complete name

- Date of birth
- 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 (whether individual is crew or non-crew)
- U.S. destination address (except for commercial aviation passengers who are U.S. citizens or lawful permanent residents, commercial aviation 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 and crew only)
- Pilot license/certificate number and country of issuance, (commercial and private flight crew only)

In addition to collecting information directly from the traveler, the commercial carrier also must transmit to CBP the following supplementary information:

- For arrivals, the airport/port where the passengers and crew members began their air transportation to or from the United States
- For departures from the United States, the foreign airports/port of final arrival
- For passengers and crew members destined for the U.S., the location where the passenger and crew member will be processed through customs and immigration formalities
- For passengers and crew members that are transiting through (and crews on flights overflying) the U.S. and not clearing customs and immigration formalities, the foreign airport/port of ultimate destination

Information also is collected about the commercial flight or voyage, including:

- Date of arrival/departure
- Airline carrier code
- Flight/voyage number
- Vessel name and country of registry/flag
- International Maritime Organization number or other official number

In addition to information collected directly from the traveler, the pilot of a private aircraft must also transmit to CBP the following information pertaining to the private aircraft:

- Aircraft tail number
- Type of aircraft
- Call sign (if available)
- CBP-issued decal number (if available)
- Place of last departure (ICAO airport code, when available)
- Date of aircraft arrival/departure
- Estimated time of arrival/departure
- Estimated time and location of crossing U.S. border/coastline

- Name of intended airport of first landing (ICAO airport code, when available)
- Owner/lessee name (first, last and middle, if available, or business entity name, if applicable)
- Owner/lessee address (number and street, city, state, zip code, country, telephone number, fax number and email address)
- Pilot/private aircraft pilot name (last, first, and middle, if available)
- Pilot street address (number and street, city, state, zip code, country, telephone number, fax number and email address)
- 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)
- Aircraft color(s)
- Complete itinerary (for arrivals, foreign airport landings 24 hours prior to landing in U.S.; for departures, intended foreign airport destinations 24 hours following departure)
- 24-hour Emergency point of contact (e.g., broker, dispatcher, repair shop or other third party knowledgeable about particular flight) name and telephone number

During physical processing at the border, primary inspection lane and inspector ID are recorded in BCI and the APIS data is verified.

Finally, information is maintained in APIS regarding the results of CBP processing the information to determine whether the traveler may pose a risk to border, aviation or public security, may be a terrorist or suspected terrorist, inadmissible, or may otherwise be engaged in activity in violation of U.S. law.

1.2 What are the sources of the information in the system?

Private aircraft pilots, commercial air or vessel carriers will collect and provide information to CBP from its internal records and from

- Passengers and crew members who intend to arrive and/or depart the United States
- Crew members on commercial aircraft who overfly the United States
- Crew members on foreign commercial aircraft who intend to arrive on a flight from an international departure location which will continue domestically within the United States

The private aircraft pilot and /or commercial air or vessel carrier will then submit this information to CBP, as applicable.

Additionally, during physical processing at the border, primary inspection lane and ID inspector are added to APIS and the APIS information is verified using travel documents provided by the crew or passenger.

1.3 Why is the information being collected, used, disseminated, or maintained?

Pursuant to the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), the collection of the traveler's passport data is mandatory for law enforcement and national security purposes. Additionally, sections, 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, and 1644a of the Tariff Act of 1930, as amended (19 U.S.C. 1431 et seq.),

give the Secretary of Homeland Security broad authority regarding the entry and clearance of civil aircraft and sea going vessels. The purpose of the collection is to screen passengers and crew members arriving from foreign travel points and departing the United States to identify those passengers who may pose a risk to border, aviation or public security, may be a terrorist or suspected terrorist, inadmissible, or may otherwise be engaged in activity in violation of U.S. law.

APIS also allows CBP to facilitate effectively and efficiently the entry and departure of legitimate travelers into and from the United States. Using APIS, officers can quickly reference the results of the advanced research that has been conducted through CBP's law enforcement databases, confirm the accuracy of that information by comparison of it with information obtained from the traveler and from the carriers, and make immediate determinations as to a traveler's security risk, admissibility and other determinations bearing on CBP's inspectional and screening processes.

1.4 How is the information collected?

For commercial air and vessel travelers, most of the information collected is contained in the machine-readable zone (MRZ) of a DHS-approved official travel document, such as a passport or alien registration card. When a commercial traveler (passenger or crew) checks in for an international flight or vessel voyage, the carrier representative will swipe the traveler's travel document through a document reader designed to electronically capture specific information and populate the carrier's computer screen. The carrier will also collect and transmit to CBP the U.S. destination address (except for U.S. citizens, lawful permanent residents, crew and persons in transit through the United States) and country of residence, which is not contained in the MRZ.

In addition to collecting information directly from the commercial traveler, the carrier also must transmit to CBP the following supplementary information: foreign airport/port where the passengers and crew members began their air transportation to the United States and in the case of departures from the United States, the foreign airport/port of final arrival; for passengers and crew members destined for the U.S., the location where the passenger will be processed through customs and immigration formalities; and for passengers and crew members that are transiting through (and for crew on flights overflying) the U.S. and not clearing customs and immigration formalities, the foreign port of ultimate destination, and crew member's status on board. Finally, information also is collected from the carrier about the particular flight or voyage, such as date of arrival/departure, airline carrier code, flight number, departure location, arrival location, and vessel country of registry.

When a non-commercial air traveler checks in for an international flight, the pilot collecting the manifest information will examine the travel document presented by the traveler to ensure that the information is correct, that travel document appears to be valid for travel purposes, and that the traveler is the person to whom the travel document was issued. In addition to collecting information directly from the traveler, the pilot must also transmit to CBP additional information noted above in 1.1. Both the notice of arrival/departure and manifest information must be transmitted by the private pilot in the same transmission via electronic submissions through the Electronic Advance Passenger Information System (eAPIS) web portal or by a CBP-approved alternative transmission medium.

During physical processing at the border, primary inspection lane or equivalent and ID inspector are added to APIS and the APIS information is verified using the documents provided by the passenger or crew.

1.5 How will the information collected from individuals or derived from the system be checked for accuracy?

Upon a traveler's or crew member's arrival into or prior to their departure from the United States, a CBP officer verifies that the data transmitted by the carrier is the same as that on the traveler's travel documents. If discrepancies are found, a CBP officer can correct the data at the port of entry/exit and update the information in APIS and BCI.

Additionally, CBP audits and tracks the sufficiency and error rates of individual carrier or private aircraft pilot transmissions to APIS and may assess penalties against any submitter that fails to properly transmit APIS data within system parameters on a recurring basis or incur large error rates in the review of their transmissions. CBP also performs periodic audits and routine maintenance on its information technology systems to ensure that system protocols and programming remain intact and operational.

1.6 What specific legal authorities/arrangements/agreements define the collection of information?

The collection of manifest information on all passengers and crew members was mandated by Congress in the Aviation and Transportation Security Act of 2001 (ATSA), Public Law 107-71, 115 Stat. 597, as codified 49 U.S.C. 44909 (applicable to carriers operating passenger flights in foreign air transportation to the United States); the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), Public Law 107-173, 116 Stat. 543; 8 U.S.C. 1221 (applicable to commercial flights and vessels arriving in and departing from the United States); and CBP's general statutory authority including the Tariff Act of 1930, as amended, in particular 19 U.S.C. 1431, 1433, 1644 and 1644a (providing authority to CBP to mandate the electronic collection of manifest data from vessels and aircraft entering and departing the U.S.).

1.7 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

Inasmuch as CBP already collects this information from various travelers in the commercial air and vessel travel environments, no additional qualitative privacy risks were identified. The expansion of APIS reporting to the private aircraft environment increases the number of persons whose privacy may be impacted by APIS but does not change the type of privacy risks associated with giving personally identifiable information to the operator of the aircraft for transmission to CBP. While there are no specific (non-contractual) penalty provisions pertaining to the private aircraft pilot for the misuse of passenger information, the vast majority of private aircraft pilots are either employed in that capacity by their passenger(s) or his or her corporation and would risk the loss of their job for such misuse. CBP already deploys extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of CBP employees. CBP's physical security measures include maintaining the information systems and access terminals in controlled space protected by armed individuals. Access to information is restricted by role, responsibility, and geographic location of the employee accessing the information.

Section 2.0 Uses of the system and the information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The purpose of the information collection is to screen passengers and crew members arriving from foreign travel points and departing the United States to identify those persons who may pose a risk to border, vessel, aviation or public security, may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists, may be inadmissible, may be a person of interest, or may otherwise be engaged in activity in violation of U.S. law, or the subject of wants or warrants.

At the same time, the system allows CBP to facilitate effectively and efficiently the entry and departure of legitimate travelers and crew members traveling into, from, and through the United States. Using APIS, officers can quickly reference the results of the advanced research conducted through the law enforcement databases and make immediate determinations as to a traveler's security risk, admissibility and other determinations bearing on CBP's inspectional and screening processes.

CBP will use the information collected and maintained through the APIS to carry out its immigration control functions and law enforcement and national security missions. CBP uses this system to ensure the entry and departure of legitimate travelers and crew members, identify, investigate, apprehend and/or remove individuals unlawfully entering the United States, prevent the entry of inadmissible individuals, and detect violations of U.S. criminal and civil laws.

The information will be cross-referenced with data maintained in CBP's other enforcement databases, notably TECS, and its screening and targeting systems, notably the Automated Targeting System (ATS), and against information from the Federal Bureau of Investigations Terrorist Screening Center's Terrorist Screening Database (TSDB), information on individuals with outstanding wants or warrants, and information from other government agencies regarding high risk parties to assist in the enforcement of U.S laws at the border. The data will be shared with enforcement systems, as appropriate, when related to ongoing investigations or operations or as otherwise authorized by law and policy. A real time image of the data will reside in the ATS as part of the screening functions performed by that system to assist, in part, in the detection of identity theft and fraud (*e.g.*, multiple border transit locations occurring simultaneously employing the same identity).

Certain information is also copied to the Arrival and Departure Information System (ADIS) for the effective and efficient processing of foreign nationals who are subject to the US-VISIT requirements. US-VISIT currently applies to all visitors (with limited exemptions). The APIS data is maintained in ADIS to identify lawfully admitted non-immigrants who remain in the United States beyond the period of authorized stay.

Certain APIS data is maintained and examined in order to view an individual's travel history. In addition to maintaining an individual's travel record, this data is aggregated with information from other law enforcement databases to assist CBP employees in making determinations with regard to a traveler's security risk, admissibility and other determinations bearing on CBP's inspectional and screening processes. APIS enables CBP to screen all passengers and crew arriving in or departing the United States, to discover travelers who may pose a risk to border, vessel, aviation or public security, may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists, may be inadmissible, may be a person of interest, or may otherwise be engaged in activity in violation of U.S. law, or the subject of wants

or warrants. CBP uses the information collected through APIS to compare with information collected in other law enforcement databases to identify possible matches, and employs this APIS data in other systems such as ATS, to help DHS officers identify patterns of activity for the purpose of assisting law enforcement efforts.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The APIS system itself does not analyze data; however the APIS data residing in the system may be accessed by other systems (such as ATS) which do conduct such analysis. The APIS data is cross-referenced or compared against other law enforcement data maintained in TECS. (The most recent Systems of Records Notice for TECS can be found at 66 FR 53029 (October 18, 2001)). TECS provides access to the National Crime Information Center (NCIC), which allows TECS users to interface with criminal record databases from all 50 states via the National Law Enforcement Telecommunications System (NLETS). TECS also contains the names of individuals in the Terrorist Screening Center's Terrorist Screening Database (TSDB).

2.3 If the system uses commercial or publically available data please explain why and how it is used.

The APIS system does not use commercial or publically available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

As with any collection of personally identifiable information, there is a risk of misuse of the information. To mitigate this risk, access to data in APIS is controlled through passwords and restrictive access rules. Users are limited to the roles that define authorized use of the system. Procedural and physical safeguards are utilized such as accountability and receipt records. Management oversight is in place to ensure appropriate assignment of roles and access to information. With regard to private pilots who submit information, on behalf of others, to APIS, misuse of this information is mitigated through restricting the pilot's access following submission of the data. Where it becomes necessary for further communication with the pilot, a message informing the pilot of a telephone number, at which to call DHS, will be provided in lieu of permitting further access to the APIS transmission.

In order to become an authorized user, an officer must have successfully completed privacy training and hold a full field background investigation. Finally, an officer must not only complete the above, but must have a "need-to-know" for the information.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

APIS retains the following information collected in connection with travelers:
Complete name, date of birth, 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 (whether individual is crew or non-crew), U.S. destination address (except for commercial aviation passengers who are U.S. citizens or lawful permanent residents, commercial aviation 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 and crew only), pilot license/certificate number and country of issuance, (commercial and general flight crew only, if applicable).

APIS retains the following information collected from commercial air or vessel carriers in connection with specific flights/voyages:
Date of arrival/departure, airline carrier code, flight/voyage number, vessel name and country of registry/flag, International Maritime Organization number or other official number. Additionally, in connection with arrivals, APIS retains the airport/port where the passengers and crew members began their air transportation to or from the United States; for departures from the United States, the foreign airports/port of final arrival. For passengers and crew members destined for the U.S., APIS retains the location where the passenger and crew member will be processed through customs and immigration formalities. For passengers and crew members that are transiting through (and crews on flights overflying) the U.S. and not clearing customs and immigration formalities, the foreign airport/port of ultimate destination.

APIS retains the following information collected in connection with private aircraft transportation:
Aircraft tail number, type of aircraft, call sign (if available), CBP-issued decal number (if available), place of last departure (ICAO airport code, when available), date of aircraft arrival/departure, estimated time of arrival/departure, estimated time and location of crossing U.S. border/coastline, name of intended airport of first landing (ICAO airport code, when available), owner/lessee name (first, last and middle, if available, or business entity name, if applicable), owner/lessee address (number and street, city, state, zip code, country, telephone number, fax number and email address), pilot/private aircraft pilot name (last, first, and middle, if available), pilot street address (number and street, city, state, zip code, country, telephone number, fax number and email address), 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), aircraft color(s), complete itinerary (for arrivals, foreign airport landings 24 hours prior to landing in U.S.; for departures, intended foreign airport destinations 24 hours following departure), 24-hour Emergency point of contact (e.g., broker, dispatcher, repair shop or other third party knowledgeable about particular flight) name and telephone number.

3.2 What is the retention period for the data in the system?

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 BCI, another subsystem of TECS, 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.

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) 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 and , 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. 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.[2]

3.3 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

CBP is working with the U.S. National Archives and Records Administration (NARA) to develop a retention and disposition schedule for APIS records that will meet program requirements.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Information is required to be retained in APIS for a period of 12 months to permit the cross-referencing and review by CBP analysts of historical data relating to an individual's air or sea travel. This retention is consistent both with CBP's border search authority and with the border security mission mandated for CBP by Congress. This information, in conjunction with other information as noted above (ADIS, BCI), is maintained for longer than the 12 month period for immigration and border security purposes and in accordance with the published system of records notices.

[2] 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

Section 4.0 Internal sharing and disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The information collected by and maintained in APIS may be shared with all component agencies within DHS on a need to know basis consistent with the component's mission. This may include U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, US-VISIT, Intelligence and Analysis, and the Transportation Security Administration. Access to APIS information within DHS is role-based according to the mission of the component and need to know in performance of its official duties.

As discussed previously, data submitted to APIS is copied to the BCI database, another subsystem of TECS, during the process of vetting a passenger or crew member. The information copied to and maintained in the BCI database 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 the result of the CBP processing.

For individuals subject to US–VISIT requirements, certain APIS data are copied to the Arrival and Departure Information System (ADIS) for effective and efficient processing of foreign nationals. This information includes: complete name, date of birth, gender, citizenship, country of residence, U.S. destination address, passport number, expiration date of passport, country of issuance (for non-immigrants authorized to work), alien registration number, and country of residence.

The purpose of sharing data within DHS is to provide the DHS counter-terrorism, intelligence, law enforcement and public security communities with information from or about suspected or known violators of the law and other persons of concern, in a timely manner. This objective supports CBP's and DHS' law enforcement, counter-terrorism, and public security missions. All component agencies of DHS that have a need to know may have access to the relevant border crossing information that includes advanced arrival and departure data collected pursuant to the APIS regulations.

4.2 How is the information transmitted or disclosed?

The information may be transmitted either electronically or as printed materials to authorized personnel. CBP's internal data sharing of the data submitted to APIS is required to comply with statutory requirements for national security and law enforcement systems. Access terminals, mainframe processors, and databases are all maintained in DHS controlled space protected by armed guards. Hard copies of information are protected by sealed envelope and shared via official intra-agency courier. All information is kept secure, accurate, and controlled. Authorized personnel must possess a mission or job related need and intended use before access may be granted.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

In order to mitigate the privacy risks of personally identifiable information being inappropriately used, the information is shared only with DHS personnel who have a need to know the information as part of the performance of their official employment duties. Internal DHS access to APIS data is controlled by CBP through the use of strict access controls for the users, passwords, background checks for individuals accessing the data, as well as system audits that track and report on access to the data. Additionally, any individual with access has gone through privacy training.

Section 5.0 External sharing and disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations and the private sector.

5.1 With which external organizations is the information shared, what information is shared, and for what purpose?

All APIS information collected is subject to being shared for reasons of border, vessel, aviation and public security, general law enforcement, intelligence and counter-terrorism purposes. The information, as warranted by specific request or Memorandum of Understanding, will be shared on a "need to know" basis, particularly with appropriate Federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order or license, where DHS believes the information would assist enforcement of civil or criminal laws. Presently, this external sharing includes every counter-terrorism, intelligence and law enforcement agency in the Federal government, as well as those Federal agencies mandated to ensure compliance with laws or regulations pertaining to entry into or exit from the U.S., each of the Fifty States, the District of Columbia, U.S. insular possessions and territories, and a majority of foreign nations with which the U.S. maintains diplomatic relations. Of particular note are Memoranda of Understanding providing for law enforcement sharing of APIS information with the Department of State [relating to Visa and other admissibility requirements], the Department of Justice (Federal Bureau of Investigation) [relating to general law enforcement], the Department of the Treasury [relating to currency and financial enforcement], the Department of Commerce [relating to export and trade controls], and the Department of Health and Human Services [relating to public health and security].

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Information collected by APIS is mandatory for law enforcement and national security purposes and the sharing of this data by CBP, for reasons of border, vessel, aviation and public security, general law enforcement, intelligence and counter-terrorism purposes, is consistent with these purposes. CBP currently has Memoranda of Understanding and other written arrangements with various law enforcement agencies, including those within the Departments of Justice, Treasury, State, and Commerce, and internationally with Canada, that have access to APIS. These MOUs address the access and use of APIS data by those agencies.

All sharing outside the Department is covered by an appropriate routine use(s), which are set forth in detail in the System of Records Notice (SORN) for the APIS system, which has been updated contemporaneous with the publication of the Final Rule concerning private aircraft obligations to provide APIS [cite].

5.3 How is the information shared outside the Department and what security measures safeguard its transmission.?

The information may be transmitted either electronically or as printed materials to authorized personnel. CBP's external data sharing of the data submitted to APIS is required to comply with statutory requirements for national security and law enforcement systems. All information is kept secure, accurate and controlled. Additionally, Memoranda of Understanding and other written arrangements, defining roles and responsibilities, have been executed between CBP and each agency that regularly accesses APIS. Lastly, information that is shared with other agencies, Federal, state, local, tribal, or foreign, outside of the context of any MOU or other prior written arrangement requires a written request by the agency specifically identifying the type of information sought and the purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the Chief, Privacy Act Policy and Procedures Branch, Regulations & Rulings, Office of International Trade, CBP, insofar as the request and use are consistent with the Privacy Act, the published routine uses for APIS, and the receiving agency agrees to be restricted from further unauthorized sharing of the information. All three requirements—use consistent with purpose for collection, sharing consistent with a statutory or published routine use, and acceptance of the restriction barring unauthorized dissemination outside the receiving agency—and the legal responsibility clause for wrongful dissemination contained in the Paperwork Reduction Act (44 U.S.C. section 3510) are stated as conditions pertaining to the receiving agencies acceptance and use of the shared information. These conditions are stated in the written authorization provided to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

Recipients of APIS data are required by the terms of their sharing arrangement (including an MOU) to employ the same or similar precautions as CBP in the safeguarding of information that is shared with

them. CBP requires all external users of APIS (that is, external to CBP) to receive the same or equivalent training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in APIS. CBP training is available online, once a user has met the background requirements for access to TECS. The training module must be completed prior to a user accessing other functionality within the TECS environment.

5.4 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

When sharing information with third parties, the same specifications related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. The reason for the interface request and the implications on privacy related concerns are two factors that are included in both the initial and ongoing authorization, the written arrangement (MOU) and Interconnection Security Agreement that is negotiated between CBP and the external agency that seeks access to CBP data. The written arrangement specifies the general terms and conditions that govern the use of the functionality or data, including limitations on use. The Interconnection Security Agreement ("ISA") specifies the data elements, format, and interface type to include the operational considerations of the interface. The written arrangements and ISAs are periodically reviewed and outside entity conformance to use, security, and privacy considerations is verified before Certificates to Operate are issued or renewed.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of the information collected, the right to consent to uses of said information, and the right to decline to provide such information.

6.1 Was notice provided to the individual prior to collection of information?

CBP collects certain information directly from commercial air and vessel carriers by regulation and has provided notice through publication of the previous APIS Final Rule (*see* 70 FR 17820 April 7, 2005), as well as the privacy impact assessment and its privacy policy for APIS, published simultaneously on April 7, 2005 (70 FR 17857). Additionally, CBP collects information directly from private aircraft pilots and has provided notice through publication of the Final Rule, published in the federal register on the same date as this PIA. CBP, through its APIS system of records notice, provides the traveling public with access to individual information and a more complete understanding of how and where information pertaining to them is collected and maintained.

With regard to the collection of data from private aircraft participants, CBP strongly recommends that the pilot inform each passenger that his or her personal data has been reported to APIS. In conjunction with the notice of proposed rulemaking, CBP sought comments on the advisability and methods for providing a Privacy Act Statement to individual passengers, but no comments were received. Therefore, CBP continues its evaluation of this matter, noting however, that the private aircraft population 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.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No. Information must be provided pursuant to applicable statutes for all persons on covered flights/voyages. The only legitimate means of declining to provide the subject information is to choose not to enter, transit through, or depart (and in the case of crew, fly over) the United States.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No. Individuals do not have the right to consent to particular uses of the information. Individuals may only choose whether or not to enter, transit, or depart from (and in the case of crew, fly over) the United States. APIS data is collected by CBP from the relevant carrier or private aircraft operator, and is composed primarily of data derived from the travel documents, particularly from the MRZ of most passports. These are the same documents that, upon arrival, all travelers are required by law to present to CBP for purposes of establishing eligibility for admission to the United States. Failure of a traveler to provide the carrier/pilot with the travel document from which APIS data is derived may result in penalties to the carrier/pilot for failure to comply with the APIS regulations and, separate penalties if the traveler is transported to the United States. Foreign travelers declining to provide access to APIS data shall be deemed inadmissible to the United States. An individual may withdraw his or her application for admission, or be subject to removal proceedings.

United States citizens who refuse to provide APIS data to the air or vessel carrier may be subject to action by that particular carrier. A carrier may decline to transport the person. However, if the carrier allows the passenger to board without providing the required information, the person will be subject to additional security checks upon arrival. Travelers aboard private aircraft who refuse to provide APIS data to the pilot may be refused transportation. The pilot of a private aircraft departing the United States, or departing a foreign place for the United States, who fail to comply with the APIS requirements are subject to a civil penalty of $5,000 for the first violation and $10,000 for each subsequent violation as prescribed in 19 U.S.C. 1436(b) and 19 CFR 122.166(a)(c)(1). The pilot may also be subject to criminal penalties for violations under 19 U.S.C. 1436(c). In addition, the U.S. government has established protocols and procedures to defend and protect its airspace against potential threats if it is unable to identify the intention of any aircraft.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

There is a risk that individuals will not know that air and vessel carriers and private aircraft pilots are required to provide APIS data to CBP concerning passengers and crew. For this purpose, CBP will be

providing notice through publications on its website such as "Ready, Set … Go" [www.cbp.gov/xp/cgov/travel/vacation/kbyg/], this PIA, and the several Federal Register publications relating to this regulation. As previously stated, with regard to the collection of data concerning private aircraft, CBP strongly recommends that the pilot inform each passenger that his or her personal data will be reported to APIS. In conjunction with the notice of proposed rulemaking, CBP sought comments on the advisability and methods for providing a Privacy Act Statement to individual passengers, but no comments were received. Therefore, CBP continues its evaluation of this matter, noting that the private aircraft population 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.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

DHS allows persons, including foreign nationals, to seek administrative access under the Privacy Act to certain information maintained in APIS. Requests for access to personally identifiable information contained in APIS, that was provided by the commercial air or vessel carrier or private pilot regarding the requestor may be submitted to the Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: 877-CBP-5511). However, records and information maintained in APIS pertaining to the results of the vetting of the traveler may not be accessed.

Requests 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.

Individuals and foreign nationals may also seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007). 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 TRIP. 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 – like airports, seaports and train stations or at U.S. land borders. Through 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.

To address situations where a traveler has the same or similar name as someone on a watchlist, CBP has developed procedures to identify these travelers as such.

Specifically, a system upgrade was developed in TECS in February 2006 that benefits anti-terrorism security measures, as well as the customs and immigration process for international travelers. The enhancement, which is virtually transparent to travelers, strives to alleviate additional screening procedures for travelers who have been misidentified due to the same or similar biographical information as watch-listed individuals. .

The upgrade, which is essentially an annotation in CBP's TECS database, allows CBP officers at ports of entry to eliminate inspections on subsequent trips in cases where travelers' names, birthdates, or other biographical information matches those of high-risk individuals once CBP has verified that the individual is not the person of interest. No action is needed from the passenger. There is no additional data collected on the passenger beyond what is normally collected during a secondary type examination. TECS will suppress the records from appearing on subsequent encounters with the traveler. However, travelers may continue to be subject to inspection for other reasons unassociated with such misidentification

In addition, the Freedom of Information Act (FOIA) (5 U.S.C. 552) provides a means of access to information, including APIS data, for all persons, irrespective of the individual's status under the Privacy Act. With respect to data for which APIS is the actual source system, the APIS SORN is published in the Federal Register. FOIA requests for access to information for which APIS is the source system may be directed to CBP in the manner prescribed by regulations at Title 19, Code of Federal Regulations, Part 103.

7.2 What are the procedures for correcting erroneous information?

CBP has an Executive Communications 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 Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: 877-CBP-5511) 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 Customer Service Center will respond in writing to each inquiry.

7.3 How are individuals notified of the procedures for correcting their information?

With respect to biographical or travel information collected from a traveler (passenger and crew) and submitted through a private pilot or the traveler's air or vessel carrier, APIS is not exempt from the amendment provisions of the Privacy Act. However, records and information maintained in APIS pertaining to the vetting of the traveler are exempt from the amendment provisions of the Privacy Act.

Requests for redress should be directed to CBP's Customer Service Center (see section 7.2. above).

7.4 If no redress is provided, are alternatives are available?

Redress is provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

As set forth in the APIS SORN (DHS/.CBP-005) published in the Federal Register, CBP provides access and amendment in APIS to the data obtained from the carrier or pilot about a person, or obtained directly from the individual at the time of physical processing at the border. In doing so, CBP seeks to permit all persons to be able to obtain copies of the APIS data that the carrier or private pilot submitted to CBP pursuant to regulatory requirements. As noted above in paragraph 7.1, individuals may also seek access to such information submitted to APIS pursuant to the FOIA, and as a matter of CBP policy, redress may also be requested in the manner described above in paragraph 7.2.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Access to the system is granted and limited to a need to know basis. All parties with access to the system are required to have full background checks. The universe of persons with access includes CBP Officers, DHS employees, Federal counter-terrorism, law enforcement and public security officers, IT specialists, program managers, analysts, contractors, and supervisors of these persons. The system, using the existing infrastructure for APIS, will assign roles based on the individual's need to know, official duties, agency of employment, and appropriate background investigation and training.

In order to gain access to the APIS information, a user must not only have a need to know, but must also have an appropriate background check and completed annual privacy training. A supervisor submits the request to the Office of Information Technology (OIT) at CBP indicating the individual has a need to know for official purposes. OIT verifies that the necessary background check and privacy training has been completed prior to issuing a new user account. User accounts are reviewed periodically to ensure that these standards are maintained. Every six months a user must request and his or her immediate supervisor must reauthorize access to APIS. Reauthorization is dependent upon a user continuing to be assigned to a mission role requiring APIS access and the absence of any derogatory information relating to past access.

8.2 Will contractors to DHS have access to the system?

Yes, subject to the same background, training, need-to-know, and confidentiality requirements as employees.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All users of the APIS system are required to complete and pass the annual TECS Privacy Act Course (TPA) to maintain their access to the system (APIS being a subsystem under TECS). The TPA presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the user's understanding of appropriate controls put in place to protect privacy as they are presented. A user must pass the test to retain access to TECS and more specifically, APIS. This training is regularly updated.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

APIS, as a subsystem of TECS, is approved through the TECS Certification and Accreditation under the National Institute of Standards and Technology. The last certification was in January 2006.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

APIS transactions are tracked and can be monitored. This allows for oversight and audit capabilities to ensure that the data are being handled consistent with all applicable laws and regulations regarding privacy and data integrity. APIS maintains audit trails or logs for the purpose of reviewing user activity. APIS actively prevents access to information for which a user lacks authorization as defined by the user's role in the system, location of duty station, and/or job position. Multiple attempts to access information without proper authorization will cause APIS to suspend access automatically. Misuse of APIS data can subject a user to discipline in accordance with the CBP Code of Conduct, which can include being removed from an officer's position.

8.6 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Privacy risks identified with respect to access and security were in appropriate use and access of the information. These risks are mitigated through training, background investigations, internal system audit controls, the CBP Code of Conduct and Disciplinary system, and the practice of least privileged access.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

APIS is a border security system which permits the advance vetting of persons intending to cross the U.S. border. The data collected within APIS is maintained using an existing data module that is part of TECS, an established law enforcement and border security database within CBP.

9.2 What stage of development is the system in and what project development lifecycle was used?

APIS is an operational system in current production. This PIA represents an update to a prior document to address an expansion of the types of individuals within the traveling public, who are subject to its collection requirements. Integrity, privacy, and security were analyzed as part of the decisions made for APIS in accordance with CBP security and privacy policy from the inception of APIS, as demonstrated by the successful transition through the systems development lifecycle (SDLC), certification and accreditation, and investment management processes. Particular areas that were identified as needing to be addressed during the development included: use of accurate data, system access controls, and audit capabilities to ensure appropriate use of the system.

9.3 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

As a border security system, the purpose of APIS is to facilitate the vetting of individuals prior to their boarding an aircraft or sea vessel to travel to the United States. Since a consequence of an individual's interaction with APIS is that they might be prevented from boarding a conveyance or traveling to the United State, privacy concerns are inherent in the operation of APIS. As such, user access controls were developed in order to ensure that only the minimum number of individuals with a need to know the information are provided access to the information. Audit provisions in conjunction with policies and procedures were also put in place to ensure that the system is properly used by CBP officers and other authorized users within DHS and other government agencies.

The system is designed to provide the following privacy protections:

- Equitable risk assessment:
    - APIS provides equitable treatment for all individuals. Equitable risk assessment is provided because APIS interfaces with the same databases for every traveler in seeking to identify matches.
    - APIS applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups. APIS is consistent in its comparison of associated data with individuals and is used to support the overall CBP counter-terrorism, law enforcement, and public security missions.
    - APIS supports a national screening policy that is established at the National Targeting Center. CBP policies regarding inspections and responding to potential terrorists and other criminals seeking entry into the United States are documented in various CBP Directives and individuals with access to the system are trained on the appropriate use of the information.

- CBP's secure encrypted network:
    - APIS security processes, procedures, and infrastructure provide protection of data, including data about individuals that are stored in APIS.
    - Encryption and authentication are the technical tools used to protect all APIS data, including data about individuals.
- APIS's role as a decision support tool for CBP officers:
    - As a decision support system, APIS is employed to support but not replace the decision-making responsibility of CBP officers and analysts. The information accessed in APIS is not the conclusion about whether or not to act but merely part of the basis upon which a CBP officer will make his or her decision. Human intervention, professionalism, and training all serve to mitigate the potential privacy threat posed by data comparisons made outside of an operational context.

In order to enhance privacy and transparency, a separate and distinct System of Records Notice under the Privacy Act was published for APIS. The SORN for APIS is published in the Federal Register.

Additionally, access to data through APIS is limited to CBP, DHS, and other counter-terrorism, law enforcement, and public security officers who have gone through extensive training on the appropriate use of the information and CBP screening policies. These officers are trained to review the APIS data and any associated information to identify individuals that truly pose a risk to law enforcement.

Responsible Officials

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of International Trade, Regulations and Rulings, Customs and Border Protection, (202) 572-8790.

John Wagner, Director, Passenger Automation Programs, Office of Field Operations, Customs and Border Protection, (202) 344-2118.

Approval Signature

Original signed and on file with the DHS Privacy Office

Hugo Teufel III

Chief Privacy Officer
Department of Homeland Security