Privacy Impact Assessment
for the

Advance Passenger Information System

APIS

<<Publication

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

CBP is issuing a Final Rule to amend regulations governing the submission of Advanced Passenger Information System (APIS) data. CBP is publishing a PIA and an associated System of Records Notice and Notice of Proposed Rulemaking for Privacy Act exemptions for APIS. The APIS database was previously covered by the Treasury Enforcement Communications System (TECS) System of Records Notice last published at 66 FR 52984, October 18, 2001. On July 14, 2006, CBP published a Notice of Proposed Rulemaking in the Federal Register (71 FR 40035) proposing amendments to CBP regulations concerning the advance electronic transmission of passenger manifests for commercial aircraft arriving in and departing from the United States, and of passenger and crew manifests for commercial vessels departing from the United States, commonly referred to as APIS.

Introduction

The Advanced Passenger Information System (APIS) was developed by the former U.S. Customs Service (Customs) in 1988, in cooperation with the former Immigration and Naturalization Service (INS) and the airline industry. Air carriers and vessels collected passengers' biographical data and transmitted the data to the Customs Service while the flight or the vessel was en route. The Customs Service Data Center used APIS data to perform a check against the combined Federal law enforcement database known as the Interagency Border Inspection System (IBIS). Through the voluntary APIS program, these checks were performed in advance of arrival and quickly referenced once the passengers arrived in the United States. This resulted in a significant time savings for the processing of passengers and carriers.

As a voluntary program, APIS participation grew widely, making it nearly an industry standard. After a period of voluntary participation, the Federal government implemented requirements governing the advance electronic transmission of passenger and crew member manifests for commercial aircraft and commercial vessels in accordance with several statutory mandates. In the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border

Security and Visa Reform Act of 2002 (EBSA), Congress made mandatory the collection of certain information on all passenger and crew members who arrive in, depart from, or transit through the United States on a commercial air or vessel carrier, and, in the case of crew members, those who continue domestically on a foreign carrier or over fly the United States. 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 passengers and crew members. This information collection also assists in customs and immigration processing at ports of entry, resulting in a significant time savings.

To implement the mandatory collection of APIS information under ATSA and EBSA, the Customs Service issued an interim regulation (19 CFR 122.49a)[1], mandating the transmission of APIS data for all inbound commercial air carriers. The INS issued a Notice of Proposed Rulemaking (NPRM) 68 FR 292 on January 3, 2003, expanding these requirements to outbound commercial air carriers and inbound and outbound commercial vessel carriers. With the creation of the Department of Homeland Security (DHS), the inspection and patrol functions of the former INS were incorporated in the U.S. Customs Service, which was renamed United States Customs and Border Protection (CBP) under DHS. CBP is now responsible for border enforcement activities, including the collection of APIS information.

To carry out its statutory responsibilities, on April 7, 2005 (70 FR 17280), CBP issued a final rule to require the submission by commercial air and vessel carriers of certain carrier and biographical data to CBP through APIS prior to a passenger's or crew member's arrival in and departure from the United States and with respect to crew, prior to overflying the United States. The 2005 Final Rule also provided a website for small commercial air and vessel carriers, which did not have the means to transmit data through APIS, to submit this information in the required time frame. At that time and in conjunction with that final rule, CBP published a Privacy Impact Assessment for APIS. This PIA document updates the original APIS PIA and addresses new functionality that is being implemented to enhance APIS.

On July 14, 2006, CBP published a Notice of Proposed Rulemaking in the Federal Register (71 FR 40035) proposing amendments to the 2005 Final Rule

[1] 66 FR 67482 (December 31, 2001), as amended 67 FR 42712 (June 25, 2002)

concerning the advance electronic transmission of passenger manifests for commercial aircraft arriving in and departing from the United States, and of passenger and crew manifests for commercial vessels departing from the United States, in accordance with the mandate from the Intelligence Reform and Terrorism Prevention Act. In accordance with the NPRM published July 14, 2006, for air travel, CBP is now issuing a Final Rule that will now allow three options for transmission of manifest data by air carriers for aircraft departing from or en route to the United States, two employing an interactive method and one a non-interactive method: (1) transmission of passenger manifests in batch form by an interactive method no later than 30 minutes prior to the securing of the aircraft doors (APIS-30); (2) transmission of individual passenger manifest information as each passenger checks in for the flight, up to, but no later than, the time the flight crew secures the aircraft doors (APIS interactive Quick Query or AQQ); and (3) transmission of passenger manifests in batch form by a non-interactive method no later than 30 minutes prior to the securing of the aircraft doors (APIS 30 "non-interactive"). For vessel travel, CBP will require vessel carriers to transmit passenger and crew manifests for vessels departing from the United States no later than 60 minutes prior to departure. For vessels departing from foreign ports destined to arrive at a U.S. port, CBP is retaining the current requirement to transmit passenger and crew arrival manifest data at least 24 hours and up to 96 hours prior to the vessel's entry at the U.S. port of arrival.

In accordance with the 2005 Final Rule, CBP mandates that air and vessel carriers collect and provide CBP with personally identifiable information about passengers and crew members traveling by air or sea, and arriving in, or departing from (and, in the case of crew, on flights overflying), the United States—this information is often collected and maintained on what is referred to as the manifest. The information that is required to be collected and submitted to APIS can be found on routine travel documents that passengers and crew members must provide when processed into or out of the United States and most of the information is included on the Machine Readable Zone (MRZ) of most passports.

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 the Border Crossing Information System (BCIS), a subsystem of TECS. 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 BCIS 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[2], 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 last published on December 12, 2003 (68 FR 69412). 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 in the past, the purpose of this collection is to 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

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

criminal laws, while simultaneously facilitating the travel of legitimate passengers and crew members. As mentioned above, this information collection also assists in customs and immigration processing at ports of entry, resulting in a significant time savings. 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
Information collected and maintained

1.1 What information is to be collected?

The information to be collected from passengers and crew members by air and vessel carriers consists of:

- Complete name
- Date of birth
- Gender
- Country of citizenship
- Passport/alien registration number and country of issuance
- Passport expiration date
- Country of residence
- Travel document type (e.g., Passport, Merchant Mariner Document, Nexus Air Card, Alien Registration Card, etc.,)
- U.S. destination address (except for U.S. citizens, lawful permanent residents, crew and persons in transit)
- Place of birth and address of permanent residence (flight crew only),
- Passenger name record (PNR) locator number
- Pilot certificate number and country of issuance, (flight crew only, if applicable)

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

- For arrivals 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, and status on board (whether an individual is crew or non-crew)Status on board

Information also is collected about the particular 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

During physical processing at the border, primary inspection lane and ID inspector are added to APIS 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 From whom is information collected?

The information will be collected by the air or vessel carrier from its internal records and from

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

The air or vessel carrier will then submit this information to CBP.

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?

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. 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?

Most of the information collected is contained in the machine-readable zone (MRZ) of an official travel document such as a passport or alien registration card. When a 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 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 member 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 airport of ultimate destination, and 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.

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

1.5 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; the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), Public Law 107-173, 116 Stat. 543; 49 U.S.C. 44909 (applicable to carriers operating passenger flights in foreign air transportation to the United States); 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 19 U.S.C. 1431 and 1644a (requiring manifests for vessels and aircraft).

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

This Final Rule does not change the types of information CBP collects, but rather CBP is altering the time frame in which the information is collected. Accordingly, inasmuch as CBP already collects the information from various travelers, no additional qualitative privacy risks were identified. 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

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, 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 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 law enforcement, immigration control functions, and national security mission. 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 the Treasury Enforcement Communications System (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. 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 will enable CBP to screen all passengers and crew arriving from or departing for foreign points, to the United States, to discover travelers that 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. 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 Does the system analyze data to assist users in identifying persons of concern that were previously unknown to law enforcement, or patterns of activity indicating issues of concern?

No. The APIS system itself does not conduct such analysis; however the APIS data residing in the system may be accessed by other systems (such as ATS) which do conduct such analysis. APIS is a system that formerly resided within the Treasury Enforcement Communications System (TECS), a law enforcement database. (The most recent System of Records Notice for TECS can be found at 66 FR 53029 (October 18, 2001). APIS comprised a subset of the data collected and maintained within TECS. The data particular to APIS was accessed through functionality that is separate from data within TECS. APIS is now being published as a separate system of records pursuant to the Privacy Act. (*see*, 72 FR xxxxx July xx, 2007).

The APIS data is cross-referenced or compared against other law enforcement data maintained in TECS. TECS provides access to the National Crime Information Center (NCIC), which allows users to interface with all 50 states via the National Law Enforcement Telecommunications System (NLETS). TECS also contains the names of individuals on the consolidated Terrorist Screening Center terrorist watch list.

As noted above, the APIS data is used by the Automated Targeting System (ATS).

2.3 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 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 TECS.

Additionally, CBP audits and tracks the sufficiency and error rates of individual carrier transmissions to APIS and may assess penalties against carriers

that fail 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.

2.4 Privacy Impact Analysis: Given the amount and type of data being collected, 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 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.

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

3.1 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 for no more than twelve months.

Data obtained through the APIS transmission is copied to BCIS, a subsystem of 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.

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.

3.2 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: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

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 flight/voyage information and air/sea travel. This retention is consistent both with CBP's border search authority and with the border security mission mandated for CBP by Congress.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

The information collected by and maintained in APIS may be shared with all component agencies withinDHS 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 are copied to the BCIS database, a subsystem of TECS during the process of vetting a passenger or crew member. The information copied to and maintained in the BCIS 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, 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, 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.

4.2 For each organization, what information is shared and for what purpose?

One of the objectives of sharing data within DHS is to provide the DHS counter-terrorism, 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.

4.3 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.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified 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

5.1 With which external organizations is the information shared?

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. 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].

Presently, this external sharing includes every counter-terrorism 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.

5.2 What information is shared and for what purpose?

All APIS information collected is subject to being shared for reasons of border, aviation and public security, general law enforcement and counter-terrorism purposes.

All relevant passport data is compared with an image within TECS of the Passport Records System from the Department of State as a means of confirming the identity of the person crossing the border. This confirmation of identity allows CBP to make a more informed decision regarding admissibility

5.3 How is the information transmitted or disclosed?

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.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes, 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 that have access to APIS. These MOUs address the access and use of APIS data by those agencies.

5.5 How is the shared information secured by the recipient?

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.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

CBP requires all external users of APIS (that is, external to CBP) to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in APIS. This 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.

5.7 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

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Previously, this information was maintained within TECS and was covered by a system of records notice published for TECS. CBP collects this information directly from the relevant carriers by regulation and has provided notice through publication of the APIS Final Rule (*see* 70 FR 17820; the NPRM (*see* 68 FR 292), as well as the privacy impact assessment and its privacy policy for APIS, published simultaneously on April 7, 2005 (70 FR 17857). Clearance for the arrival or departure of a commercial vessel or aircraft may be contingent upon the submission of passenger and crew manifest information to CBP through APIS. CBP is publishing a new system of records notice in order to permit the traveling public greater access to individual information and a more complete understanding of how and where information pertaining to them is collected and maintained.

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, 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 with the travel document from which APIS data is derived may result in penalties to the carrier 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.

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 they are required to provide APIS data. For this purpose, CBP will be providing notice through publications on its website such as “Know Before You Go” [www.cbp.gov/xp/cgov/travel/vacation/kbyg/], this PIA, and the several Federal Register publications relating to this regulation.

Section 7.0 Individual Access, Redress and Correction

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

DHS allows persons, including foreign nationals, to seek 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 carrier regarding the requestor may be submitted to the FOIA/Privacy Act Branch,

Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: (202)344-1850 and fax: (202)344-2791). 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.

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 at 72,FR XX, published July XX, 2007. 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 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 5.5C, 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.

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

With respect to information collected from a traveler (passenger and crew) and submitted through the traveler's air or vessel carrier, APIS is not exempt from the amendment provisions of the Privacy Act, in the course of any access or amendment process by that person, or his or her agent, to whom the biographical or travel data associated with this SORN pertains.

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 FOIA/Privacy Act Branch (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 (72 FR xxxxx, July x, 2007), CBP provides access and amendment in APIS to the data obtained from the carrier 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 relevant carrier 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

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

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.

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 Does the system use "roles" to assign privileges to users of the system?

Yes. 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.

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

In order to gain access to the APIS information, a user must not only have a need to know, but must also have 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.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

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.

8.6 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.

8.7 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 a bi-annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the system (APIS being a subsystem under TECS). The TPAAC 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 scenarios to retain access to TECS and more specifically, APIS. This training is regularly updated.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

APIS, as a former component 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.

8.9 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

9.1 Was the system built from the ground up or purchased and installed?

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 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Integrity, privacy, and security are 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 What design choices were made to enhance privacy?

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 72, FR XXX (July xx, 2007).

Additionally, access to APIS data 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.

Reviewing Official:

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

Approval Signature Page

_____

Hugo Teufel III

Chief Privacy Officer
Department of Homeland Security