Privacy Impact Assessment
for the

Advanced Passenger Information System-Voluntary Rail and Bus Submissions (APIS-VRBS)

February 19, 2009

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

Reviewing Official
John W. Kropf
Acting Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

This is a supplemental Privacy Impact Assessment (PIA) update to the previous Advanced Passenger Information System (APIS) PIA (August 8, 2007) to discuss the current state of voluntary rail and bus submission (VRBS) arrangements between U.S. Customs and Border Protection (CBP) and Amtrak and certain bus carriers to facilitate the transmission of passenger and crew manifest data to CBP for purposes of screening passengers and crew in advance of their crossing the border. This PIA encompasses the current system for screening passengers and baggage on passenger railroad service between the United States and Canada, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), Pub. L. No. 110-53 (August 3, 2007), Section 1523(b)(2).

Overview

Background: Mandatory APIS Submissions

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

By receiving the advanced passenger and crew information, CBP is able to perform enforcement and security queries against various multi-agency law enforcement and terrorist databases and identify high-risk passengers and crew members who may pose a risk or threat to travel safety 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.

Voluntary APIS Submissions

In addition to the mandatory submissions provided by both commercial and private air and vessel carriers, CBP receives voluntary APIS submissions from Amtrak and certain bus carriers. To fulfill its border enforcement mission more efficiently, CBP needs to be able to accurately assess the threat risk of individuals entering the United States, including passengers and crew members aboard all rail and bus traffic crossing the border. Under 19 U.S.C. 1431(b), CBP has the authority to collect manifest data from vessels, aircraft, or vehicles entering the United States. CBP is pursuing "All Modes" APIS legislative authority to clarify its broad authority to mandate the transmission of manifest information, including all international rail and bus travel. This PIA update supplements the original APIS PIA and addresses voluntary submissions of manifest data by private bus carriers entering the United States from Mexico and Amtrak trains traveling in either direction across the United States-Canada border (presently, Amtrak does not provide service across the United States-Mexico border).

Northern Border Railroad

The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), Pub. L. No. 110-53 (August 3, 2007), Section 1523, mandates that U.S. Government agencies responsible for railroad security report on their progress in screening passengers and cargo entering the United States from Canada. Currently, Amtrak collects certain manifest data from passengers and crew on all of Amtrak's international service,[1] and, on a voluntary basis, Amtrak provides that manifest information to CBP. This information is not collected for domestic Amtrak train service.

For all international service Amtrak trains arriving in the United States from a Canadian location or departing the United States for a Canadian location, Amtrak currently, voluntarily transmits an advance notice submission of information regarding each individual traveling onboard the train to CBP. This transmission automatically sent using a United Nations Electronic Data Interchange for Administration, Commerce, and Trade (UN EDIFACT) text file through eAPIS, the CBP APIS web portal. The manifest data may include the following information for all individuals aboard the train: complete name, date of birth, gender, country of citizenship, travel document type (e.g., Passport, Merchant Mariner Document, NEXUS or SENTRI Card, Legal Permanent Registration Card, Enhanced Driver's License, etc.), DHS-approved travel document number, DHS-approved travel document country of issuance, DHS-approved travel document expiration date, passenger name record (PNR) or reservation locator number, status on board the train (i.e., passenger or crew member), train point of origin , final destination, date of arrival/departure, rail carrier code (Amtrak), and train number or other official number. This data is generally received by CBP 60 minutes before an arriving train departs from a Canadian location or a train in the United States leaves for a Canadian location.

Bus Carrier Submissions

Through efforts by CBP at ports in the vicinity of Nogales, Arizona, CBP has established a program that permits private bus carriers to voluntarily submit advanced passenger and crew information to CBP. APIS sender accounts have been created for 31 different bus carriers and/or their third party submitters. Similar to Amtrak, bus carriers collect the passenger information, convert it into a US EDIFACT text file, and submit it through eAPIS, the CBP APIS web portal. The manifest data may include the following information for all individuals aboard the bus: complete name, date of birth, gender, travel document type (e.g., passport, permanent resident card), approved DHS travel document number, travel document country of issuance, status on board the train (i.e., passenger or crew member), point of origin, final destination, carrier code (assigned by CBP), manifest number (assigned by carrier – akin to a flight number), date of departure, and date of arrival. This data is generally received by CBP 60 minutes before a bus departs from a Mexican location for the United States.

[1] Maple Leaf Train 63 inbound from Canada – Eastern service area; Maple Leaf Train 64 outbound from the United States; Adirondack Train 68 inbound from Canada – Eastern service area; Adirondack Train 69 outbound from the United States; Train #510 outbound from the United States – Western service area; and Train #517 inbound from Canada.

Section 1.0 Characterization of the Information

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

1.1 What information is collected, used, disseminated, or maintained in the system?

Northern Border Railroad

The information collected from passengers and crew members by Amtrak and transmitted to APIS may consist of:

- Complete name
- Date of birth
- Gender
- Country of citizenship
- Travel document type (e.g., Passport, Merchant Mariner Document, NEXUS or SENTRI Card, Legal Permanent Registration Card, Enhanced Driver's License, etc.)
- DHS-approved travel document number
- DHS-approved travel document country of issuance
- DHS-approved travel document expiration date
- Passenger name record (PNR) or reservation locator number

In addition to collecting information directly from the traveler, Amtrak also transmits to CBP the following supplementary trip information:

- Status on board the train (i.e., passenger or crew member)
- Train point of origin
- Final destination
- Date of arrival/departure
- Rail carrier code (Amtrak)
- Train number or other official number

This information is transmitted in UN EDIFACT form automatically via eAPIS, CBP's APIS web portal. Once this information is transmitted to CBP, it is stored in APIS and maintained for one year.

Bus Carrier Submissions

The information collected from passengers and crew members by bus carriers and transmitted to APIS may consist of:

- Complete name
- Date of birth
- Gender
- Travel document type (e.g., passport, permanent resident card)

- Approved DHS travel document number
- Travel document country of issuance
- Status on board the train (i.e., passenger or crew member)

In addition to collecting information directly from the traveler, the bus carriers also transmit to CBP the following supplementary manifest information:

- Point of origin
- Final destination
- Carrier code (assigned by CBP)
- Manifest number (assigned by carrier – akin to a flight number)
- Date of departure
- Date of arrival

This information is transmitted in UN EDIFACT form automatically via eAPIS, CBP's APIS web portal. Once this information is transmitted to CBP, it is stored in APIS and maintained for one year.

During physical processing at the border, CBP verifies the Amtrak or bus passenger and crew manifest data, adds the primary inspection lane and inspector ID to this information, and maintains it as Border Crossing Information (DHS/CBP-007, July 25, 2008, 73 FR 43457). Finally, information is maintained in the Treasury Enforcement Communications System[2] (TECS) (TREAS/CS.244 October 18, 2001, 66 FR 52984) regarding the results of CBP processing the information to determine whether the traveler may pose a risk to border, rail or public security; may be a terrorist or suspected terrorist; may be 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?

Amtrak and bus carriers collect the information from their internal records and from passengers and crew members who intend to arrive in and/or depart from the United States. Amtrak or the bus carrier then submits this information to CBP. Additionally, during physical processing at the border, primary inspection lane and inspector ID are added to the API data and this information is verified using travel documents provided by the crew or passenger, and then maintained in the Border Crossing Information (BCI) System.

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

The manifest data provided by Amtrak allows CBP to facilitate the entry and departure of legitimate travelers into and from the United States. Using this data, 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 whether the traveler presents a security risk or may be engaged in activity in violation of U.S. law, and make admissibility and other determinations bearing on CBP's inspectional and screening processes.

Once the traveler has crossed, the information is submitted to BCI to provide a record of the traveler's

[2] CBP is in the process of publishing a new notice for this system and will thereafter refer to it only as TECS.

crossing. (73 FR 43457, dated July 25, 2008).

1.4 How is the information collected?

Amtrak collects the passenger information from the passenger when the ticket purchase is made. If purchased over the phone, a reservation agent at a call center collects the information and enters it into the Amtrak system. If the passenger purchases the ticket at the station, the information is entered by a station ticket agent. If purchased online, the information is entered by the passenger via the Internet. Crew information is collected from the crew and kept on file. Amtrak then adds the supplementary trip information, converts it to a UN EDIFACT text file, and electronically submits it via eAPIS, the CBP APIS web portal. Amtrak transmits this information 60 minutes before a scheduled departure, as well as manually transmitting this information in the event of a delayed departure.

Like Amtrak, bus carriers collect the passenger information from the passenger when the ticket is purchased at the station and entered by the bus carrier representative. Crew information is collected from the crew and kept on file. Bus carriers, or their third party submitters, then add the supplementary trip information, convert it to a US EDIFACT text file, and electronically submit it via eAPIS, the CBP APIS web portal. The bus carrier generally transmits this information 60 minutes before a scheduled departure, as well as manually transmitting this information in the event of a delayed departure.

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

1.5 How is the information 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, BCI, and TECS.

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, and/or agreements define the collection of information?

Pursuant to 19 U.S.C. 1431(b), CBP has the authority to require manifest information for all vehicles crossing the border, including trains and buses. CBP is pursuing "All Modes" APIS legislative authority to clarify its broad authority to mandate the advance transmission of manifest information. Amtrak collects this information under its authority provided by 49 U.S.C. 24709 and voluntarily provides the information to CBP. Bus carriers provide this information to CBP on a voluntary basis.

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

This PIA does not change the types of information CBP collects pursuant to existing regulations, but rather notifies the public of the additional voluntary submissions CBP accepts, expanding the pool of people from which such information is collected. Accordingly, inasmuch as CBP already collects the information

from various travelers pursuant to existing regulatory requirements, 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 Information

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

2.1 Describe all the uses of information.

CBP accepts these voluntary submissions to screen passengers and crew members, arriving in the United States from foreign travel points and departing the United States, to identify those persons who may pose a risk to border or public security; may be a terrorist, 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 in 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 TECS, its screening and targeting systems, and the Automated Targeting System (ATS), against information from the Federal Bureau of Investigation's 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 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).

After CBP has determined to admit or parole the traveler into the United States, the border crossing information, including the traveler's biographical data, is transmitted to BCI. 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 recent 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. 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 inclusion of voluntary Amtrak and bus passenger manifest data expands the collection of information maintained in APIS, but data does not give rise to new analysis techniques. Further, APIS itself does not conduct any data mining analysis; however the APIS data residing in the system may be accessed by other systems, such as the Automated Targeting System (DHS/CBP-006, August 6, 2007, 72 FR 43650), which do conduct such analysis.

APIS data is accessible through TECS, a law enforcement database. (The most recent System of Records Notice for TECS can be found at 66 FR 53029 (October 18, 2001). This Amtrak and bus passenger manifest data provided to APIS is cross-referenced or compared against other law enforcement data maintained in TECS, and produces an indication of matches where they exist. TECS provides access to the National Crime Information Center, which allows TECS users to interface with criminal databases from all 50 states via the National Law Enforcement Telecommunications System. TECS also uses APIS to match names against the names of individuals on the Federal Bureau of Investigation's Terrorist Screening Center's Terrorist Screening Database (TSDB).

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

Rail and bus carriers provide APIS data to CBP on a voluntary basis; CBP does not purchase this data. By providing this information in advance, rail and bus carriers allow CBP to conduct pre-screening to facilitate the clearance of legitimate travelers and ensure that the carriers are not transporting individuals that present a risk to border, transportation or public security; may be a terrorist, suspected terrorist, or affiliated with or suspected of being affiliated with terrorists; may be inadmissible; may be a person of interest; may otherwise be engaged in activity in violation of U.S. law; or the subject of wants or warrants.

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

As with any collection of personally identifiable information (PII), 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

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

3.1 What information is retained?

All the data listed in 1.1 is retained in APIS.

3.2 How long is the information retained?

The information initially collected by APIS is used for entry screening purposes and is retained for no more than 12 months. Data obtained through the APIS transmission is copied to BCI during the process of vetting an individual traveler or crew member and will be retained in accordance with the record retention period for BCI. If an individual is required to go through secondary inspection or some other enforcement action is taken, then that information will be maintained in TECS pursuant to that retention schedule.

Data regarding individuals subject to US-VISIT requirements is obtained through the APIS transmission and is also copied to the Arrival and Departure Information System (ADIS). The copied data is retained in accordance with the retention schedules approved for ADIS.

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

CBP is working with the NARA to develop a retention and disposition schedule for APIS records that will meet program requirements.

3.4 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 trip information and rail or bus 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

The following questions are intended to define the scope of sharing within DHS.

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

The inclusion of rail and bus data does not alter internal sharing of APIS information. 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, the DHS Office of 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 BCI, a subsystem of TECS, during the process of vetting a passenger or crew member. The information copied to and maintained in BCI includes: complete name, date of birth, gender, date of arrival, date of departure, time arrived, means of arrival (air/vessel/rail/bus), primary inspection lane, inspector ID, travel document, departure location, rail code and train number, and the result of the CBP processing.

For individuals subject to US–VISIT requirements, certain APIS data is copied to 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 or DHS-approved travel document number, expiration date of travel document, 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 train, U.S. destination address, and expiration date of passport.

One of the objectives of sharing data within DHS is to provide the DHS counterterrorism, 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, counterterrorism, and public security missions. All component agencies of DHS that have a need to know may have access to the relevant border crossing information, which 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 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 PII 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 and local government, and the private sector.

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

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 counterterrorism 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 United States, each of the 50 states, the District of Columbia, U.S. insular possessions and territories, and a majority of foreign nations with which the United States maintains diplomatic relations.

All APIS information collected is subject to being shared for reasons of general law enforcement; counterterrorism purposes; and border, aviation, vessel, rail, bus and public security.

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. Similarly, when an Enhanced Drivers License (EDL) is used for the purpose of establishing identity and citizenship, the relevant information will be compared an image within the Non-Federal Entities Data System (NEDS) as a means of confirming the information as supplied by the EDL issuing non-Federal authority. This confirmation of identity allows CBP to make a more informed decision regarding admissibility.

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.

PII is shared outside the Department according to the provisions of the Privacy Act (5 U.S.C. 552a) and the routine uses listed in the APIS SORN (last published November 18, 2008) for the purposes listed above. See 5.1.

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, MOUs and other written arrangements, which define 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.

CBP currently has MOUs 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. CBP intends to initiate discussions with the Canadian government concerning an arrangement that will facilitate the sharing of rail and bus APIS data, while ensuring that appropriate protections are in place for such information.

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 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, of which APIS is a subsystem. 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, explain the privacy risks 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 (i.e., MOU) and Interconnection Security Agreement (ISA) 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 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 information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

CBP collects this information directly from Amtrak and the bus carriers and will provide notice through publication of this privacy impact assessment for APIS. CBP will also publish an updated 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.

Amtrak provides notice via their Web site, www.amtrak.com[3], that passengers must provide this information in order to travel across the border, and that their information will be provided to CBP for pre-screening purposes.

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

No. CBP does not require individuals provide this information to Amtrak or the bus carriers. However, Amtrak has made provision of this information a requirement for all persons traveling on Amtrak international service trains crossing the northern border. Bus carriers have also made provision of this information a requirement for all persons traveling aboard their buses across the United States border. For both Amtrak and bus travel to the United States, the only legitimate means of declining to provide the

[3] To view the notice, go to www.amtrak.com, click on "Terms of Transportation", then "Carriage of Passengers" and finally "Tickets, ID, Safety and Security."

subject information is to choose not to enter or depart the United States.

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

Once API data is provided by Amtrak or a bus carrier to CBP, individuals do not have the right to consent to particular uses of the information by CBP. Individuals may only choose whether or not to enter, transit, or depart from the United States by rail or bus. Amtrak and bus carriers voluntarily provide passenger and crew manifest information to CBP; the manifest is composed primarily of data derived from the travel documents. 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. 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.

U.S. citizens who refuse to provide passenger and crew manifest data to Amtrak or a bus carrier may be subject to action by Amtrak or the bus carrier. Amtrak or the bus carrier may decline to transport the person. However, if Amtrak or the bus 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: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is a risk that individuals will not know that they must provide this information to Amtrak or the bus carrier or that the passenger crew manifest data is submitted to and maintained in the APIS system of records. For this purpose, CBP will be providing notice through publications on its Web site such as "Know Before You Go" [www.cbp.gov/xp/cgov/travel/vacation/kbyg/] and this PIA. Amtrak provides further notice through their Web site, www.amtrak.com under their "Terms of Transportation."

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 that 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 the APIS system of records. Requests for access to the requestor's PII contained in APIS, that was provided by the carrier 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 requester/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.

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, at the following address: 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. CBP will respond in writing to each inquiry.

Individuals and foreign nationals may also seek redress through the DHS Traveler Redress Program ("TRIP") (see 72 FR 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 believes he/she 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 antiterrorism 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 are not the actual subject of a watchlist record but are identified as such due to the same or similar biographical information.

The upgrade, which essentially permits an annotation in TECS, including the subsystem APIS, allows CBP officers at ports of entry to reduce the likelihood of inspections on subsequent trips based on the fact that a travelers' name, birth date, or other biographical information matches that of a high-risk individual, once CBP has verified that the traveler is not the actual person of interest. No action is needed from the traveler. There is no additional data collected on the traveler to facilitate this process beyond what is

normally collected during a secondary type examination.

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 carrier, APIS, including the voluntarily provided manifest data from Amtrak or a bus carrier, 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, the Customer Service Center will explain the procedures for amendment. 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 formal redress is provided, what alternatives are available to the individual?

Redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

As set forth in the APIS SORN published in the Federal Register, 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

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 counterterrorism, law enforcement and public security officers, IT specialists, program managers, analysts, contractors, and supervisors of these persons.

8.2 Will Department Contractors 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 program or system.

All users of the APIS system are required to complete and pass a bi-annual TECS Privacy Act Course (TPAC) to maintain their access to the system (APIS being a subsystem under TECS). The TPAC presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and PII. 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.

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

APIS, a subsystem under 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?

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.

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 the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy risks identified with respect to access and security relate to the 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, Radio Frequency Identification (RFID) technology, biometrics and other technology.

9.1 What type of project is the program or system?

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?

This project is in the formative stages, pre- formal authorization language, regulatory language, or appropriation. Project development lifecycle is undetermined.

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

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.

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:
  - o 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.
  - o 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 counterterrorism, law enforcement, and public security missions.
  - o 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:

o APIS security processes, procedures, and infrastructure provide protection of data, including data about individuals that are stored in APIS.

o 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:

o 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 SORN under the Privacy Act will be published for APIS. The current SORN for APIS is published in the Federal Register.

Responsible Officials

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

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Regulations & Rulings, Office of International Trade, U.S. Customs and Border Protection, Department of Homeland Security, (202) 325-0280.

Approval Signature

Original signed and on file with the DHS Privacy Office
John W. Kropf
Acting Chief Privacy Officer
Department of Homeland Security