DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket Number: DHS–2007–0040]

Privacy Act of 1974; U.S. Customs and Border Protection—Border Crossing Information, Systems of Records

AGENCY: Privacy Office; Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) gives notice that it is establishing a distinct System of Records, Border Crossing Information (BCI). BCI will receive and maintain border crossing information on travelers who are admitted or paroled into the United States, this information includes: Certain biographical information; a photograph; certain itinerary information provided by air and sea carriers and any other forms of passenger transportation, including rail, which is or may subsequently be mandated, or is or may be provided on a voluntary basis; and the time and location of the border crossing. Previously, maintenance of this border crossing information was covered by the Treasury Enforcement Communications System (TECS) ''system of records notice.'' See 66 FR 52984, dated October 18, 2001. As part of DHS's ongoing effort to increase transparency regarding the collection of information at the Department, as well as its efforts to specifically review the personally identifiable information maintained on the TECS information technology platform, DHS and CBP have identified different data sets that call for individual notice so as to provide appropriate routine uses, retention, and exemptions to the Privacy Act.

This system of records notice does not identify or create any new collection of information, rather, the Department is providing additional notice and transparency with respect to the handling of an existing collection of information, by separately noticing its collection as a distinct system of records.

DATES: Comments must be provided prior to August 25, 2008. The new system of records will be effective August 25, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS–2007–0040 by one of the following methods:

- Federal e-Rulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.
- Fax: 1–866–466–5370.
- Mail: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov*, including any personal information provided.
- Docket: For access to the docket to read background documents or comments received go to *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202–572–8790), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of International Trade, Regulations & Rulings, Mint Annex, 1300 Pennsylvania Ave., NW., Washington, DC 20229. For privacy issues contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The priority mission of U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorists' weapons from entering the country while facilitating legitimate travel and trade. BCI will maintain border crossing information on travelers who are admitted or paroled into the United States, this information includes: Certain biographical information; a photograph (if available); certain itinerary information provided by air and sea carriers and any other forms of passenger transportation, including rail, which is or may subsequently be mandated, or is or may be provided on a voluntary basis; and the time and location of the border crossing. Previously, maintenance of this information was covered by the Treasury Enforcement Communications System (TECS) ''system of records notice.'' See 66 FR 52984, dated October 18, 2001. As part of DHS's ongoing effort to increase transparency regarding the collection of information at the Department, as well as its efforts to specifically review the personally identifiable information maintained on the TECS information technology platform, DHS and CBP have identified different data sets that call for individual notices so as to provide appropriate routine uses, retention, and exemptions to the Privacy Act.

This system of records notice does not identify or create any new collection of information; rather, the Department is providing additional notice and transparency with respect to the handling of an existing collection of information, by separately noticing it as a distinct system of records.

CBP is the agency responsible for collecting and reviewing border crossing information from travelers entering and departing the United States. This is consistent with CBP's overall border security and enforcement missions. Upon arrival in the United States, all individuals crossing the border are subject to CBP processing. As part of this clearance process, each traveler entering the United States must first establish his or her identity, nationality, and admissibility to the satisfaction of a CBP officer. Additionally, CBP creates a record of the fact that the individual has been admitted or paroled into the United States at a particular time and port of entry. This record was previously covered by TECS system of records notice and will now be maintained in accordance with the privacy rules of this newly created Privacy Act System of Records Notice, BCI.

The border crossing information identified below may be collected in a number of different ways. For example, information may be collected: (1) From the travel documents presented by the individual at CBP Ports of Entry, such as foreign passports, where no advance notice of the border crossing has been provided to CBP; (2) from carriers who submit information in advance of travel, through the Advance Passenger Information System (APIS) (See DHS/CBP–005, August 23, 2007, 72 FR 48346); (3) from a DHS system that validates a Trusted Traveler Program card, I–551 Permanent Resident Card, or immigration document; (4) from non-federal governmental authorities that have issued valid travel documents approved by the Secretary of the Department of Homeland Security, such as an Enhanced Driver's License (EDL); or (5) from another Federal Agency that has issued a valid travel document, such as Department of State Visa, Passport including Passport Card, or Border Crossing Card data. When a traveler is admitted or paroled into the U.S., a traveler's biographical information, photograph, where available, and crossing details (time and location) will be maintained in accordance with this BCI system of records. The information collected in BCI is authorized pursuant

to the Enhanced Border Security and Visa Reform Act of 2002 (Pub. L. 107–173), Aviation and Transportation Security Act of 2001 (Pub. L. 107–71), the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108–458), the Immigration and Naturalization Act, as amended (8 U.S.C. 215), and the Tariff Act of 1930, as amended (19 U.S.C. 66, 1433, 1454, 1485, 1624 and 2071) and much of the information can be found on routine travel documents that persons, passengers, and crewmembers currently provide to CBP when entering and departing the United States.

BCI shall contain border crossing information, as that term is explained above, for all individuals who are admitted or paroled into the United States, regardless of method or conveyance, and information for all individuals who depart the United States by air or sea and, in certain circumstances, by land. In certain circumstances in the land environment, CBP will collect the individual's biographic data, either directly from an approved travel document presented by the traveler and/or by verifying the traveler's border crossing information against electronic records supporting certain documents, such as EDLs, determined by the Secretary of DHS to denote citizenship and identity in conformance with IRTPA. For certain air and sea carriers and any other forms of passenger transportation, including rail, which are or may subsequently be mandated to provide APIS, or provide such information on a voluntary basis, CBP will confirm the individual's data against such information previously submitted by carriers.

For information collected from certain travel documents, for example a foreign or U.S. Passport, the CBP Officer will swipe the Machine Readable Zone (MRZ) to populate the border crossing record for an individual.

For records first collected through APIS, the BCI record will contain all the data of the APIS record (including complete name, date of birth, travel document type (e.g., passport), travel document number and travel document country of issuance) as well as information pertaining to the instance of the border crossing (for example, airport or place of embarkation, where the person began their travel to the United States; for persons destined for the U.S., the location where the person underwent CBP clearance). Such data will also be maintained in accordance with the APIS SORN, DHS/CBP–005 August 23, 2007 72 FR 48349.

For records first collected through the Non-Federal Entity Data System (NEDS), a new system of records being published concurrently in today's **Federal Register**, biographic data elements and photographs collected by the authority issuing the travel document will be transferred from NEDS, displayed in TECS, and then recorded in BCI as border crossing information at the time an individual is admitted or paroled into the United States. In the instance of data being transferred from NEDS, the biographical data and photograph will be first collected from the traveler by the issuing authority of the respective travel document and then provided to CBP, which will store a copy of that data in the system of records described by the NEDS SORN. At the time of arrival at the border, the travel document, either through a CBP Radio Frequency Identification (RFID) Reader reading a unique RFID number from the RFID chip contained in the travel document, or through the CBP Machine Reader reading the MRZ of the travel document, will be used to retrieve the biographical data and photograph associated with the travel document from NEDS and populate a record in BCI, following admission/parole, to permit CBP to electronically verify identity and citizenship, to perform law enforcement queries to identify security risks to the United States and to expedite CBP processing upon arrival in and prior to departure from the United States. Upon admission/parole of the individual by CBP at the United States border or its functional equivalent, a record of the crossing will be created in BCI. Prior to admission/parole and during the process of inspecting the individual, information relating to identity and citizenship is compiled by the CBP in TECS, as part of the screening process to determine admissibility.

For records where traveler-specific information is accessed from a non-federal authority's travel document database at the time of the traveler's crossing, the biographical data and photograph will be first collected from the traveler by the issuing authority of the respective travel document and the issuing authority will maintain its own travel document database; the data from such issuing authorities will not reside in NEDS. At the time of arrival at the border, the travel document, either through a CBP RFID Reader reading the RFID number from the RFID chip contained in the travel document, or through the CBP Machine Reader reading the MRZ of the travel document, will be used to access that traveler's biographic data and photograph, displaying it in TECS; upon admission to the United States, that data will be recorded in BCI. CBP also uses this information to perform law enforcement queries to identify security risks to the United States and to expedite CBP border processing.

For records where the information is provided by another component of DHS or another federal government authority, such as the State Department's Visa and Passport database or USCIS Permanent Resident Card data, the information will be transferred from the federal authority's or DHS's system of records, displayed in TECS, and then used to create a record in BCI at the time of admission or parole into the United States. Technically, in the case of information obtained from the Department of State and Citizenship and Immigration Services (CIS), the information is maintained on the TECS IT Platform to improve the efficiency of the processing time at the border, but the information follows the State Department's or USCIS's system of records notices until the individual is admitted or paroled into the United States, at which point the information will by handled consistent with the BCI system of records notice, or that of any other DHS systems (such as TECS) in which it may be recorded.

BCI does not constitute a new collection of biographic information by DHS or CBP. DHS and CBP are providing additional notice and transparency with respect to the functionality of an existing operational process. The information storage functions of BCI were previously handled as a sub-module within TECS and covered by the TECS ''system of records notice.'' See 66 FR 52984.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. DHS extends administrative Privacy Act protections to all persons where information is maintained in the same system on U.S. citizens, lawful permanent residents, and non-immigrant aliens. BCI involves the

collection of information that will be maintained in a system of records.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that apply to each system to make agency recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the agency.

DHS is hereby publishing a description of the Border Crossing Information, system of records. In accordance with 5 U.S.C. 552a(r), a report concerning this record system has been sent to the Office of Management and Budget and to the Congress.

DHS/CBP–007

SYSTEM NAME:

Border Crossing Information (BCI).

SYSTEM LOCATION:

This computer database is located at the U.S. Customs and Border Protection (CBP) National Data Center currently, but will move to a DHS Data Center in the future. Access to the border crossing data is available from locations throughout the Department of Homeland Security and other locations at which DHS authorized personnel may be posted to facilitate DHS's mission. Terminals may also be located at appropriate facilities for other participating government agencies, which have obtained system access pursuant to a Memorandum of Understanding.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by BCI consist of persons, including U.S. Citizens, Lawful Permanent Residents, and non-immigrant aliens who lawfully cross the United States border by air, land or sea, regardless of method of transportation or conveyance.

CATEGORIES OF RECORDS IN THE SYSTEM:

The database is comprised of personally identifiable information pertaining to persons, including travelers and crew members who arrive in and are admitted/paroled, and, in certain circumstances, depart from (when departure information is available) the United States (including those entering the United States only for purposes of transiting through the country). The information that may be stored in BCI includes:

- Full name (First, Middle, and Last)
- Date of birth
- Gender
- Travel document type (e.g., passport information, permanent resident card, Trusted Traveler Program card, etc.), number, issuing country or entity, and expiration date
- Photograph (where available)
- Country of citizenship
- RFID tag number(s) (if land/sea border crossing)
- Date/time of crossing
- Lane for clearance processing
- Location of crossing
- Secondary Examination Status
- License Plate number (or Vehicle Identification Number (VIN), if no plate exists; only for land border crossings)

Where applicable, information derived from an associated APIS transmission, will be stored with an individual's border crossing record including: The airline carrier code, flight number, vessel name, vessel country of registry/flag, International Maritime Organization number or other official number of the vessel, voyage number, date of arrival/departure, foreign airport/port where the passengers and crew members began their air/sea transportation to the United States; for passengers and crew members destined for the United States, the location where the passenger and crew members will undergo customs and immigration clearance by CBP; and for passengers and crew members that are transiting through (and crew on flights over flying) the United States and not clearing CBP, the foreign airport/port of ultimate destination, and status on board (whether an individual is crew or non-crew); and for passengers and crew departing the United States, the final foreign airport/port of arrival. To the extent APIS may be transmitted by private aircraft operators and carriers operating in the land border environment, either voluntarily or pursuant to a future legal mandate, similar information may also be recorded in BCI with regard to such travel. In the land border environment for both arrival and departure (when departure information is available), the License Plate number of the conveyance (or VIN number where no plate exists) is also collected.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The legal authority for BCI is the Enhanced Border Security and Visa Reform Act of 2002, Pub. L. No. 107–173, 116 Stat. 543 (2002), Aviation and Transportation Security Act of 2001, Pub. L. No. 107–71, 115 Stat. 597 (2001), Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, 118 Stat. 3638 (2004), The Immigration and Nationality Act, 8 U.S.C. 1185 and 1354 and The Tariff Act of 1930, as amended, 19 U.S.C. 66, 1433, 1454, 1485, 1624 and 2071.

PURPOSE:

CBP collects and maintains this information to assist in screening persons arriving in or departing from the United States to determine identity, citizenship, and admissibility and identify persons who may be or are suspected of being a terrorist or having affiliations to terrorist organizations, have active warrants for criminal activity, are currently inadmissible or have been previously deported from the United States, or have been otherwise identified as potential security risks or raise a law enforcement concern. For non-immigrant aliens, the information is also collected and maintained in order to ensure that the information related to a particular border crossing is available for providing any applicable benefits related to immigration or other enforcement purposes. Lastly, CBP maintains this information in BCI to retain a historical record of persons crossing the border for law enforcement, counterterrorism, and benefits processing.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To appropriate Federal, state, local, tribal, or 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 CBP believes the information would assist enforcement of civil or criminal laws or regulations;

B. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in response to a subpoena, or in connection with criminal proceedings;

C. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance

of the official duties of the officer making the disclosure;

D. To an agency, organization, or individual for the purposes of performing audit or oversight operations as authorized by law; but only such information as is necessary and relevant to such audit or oversight function.

E. To a Congressional office, for the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains;

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees;

G. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

H. To the United States Department of Justice (including United States Attorney offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: (1) DHS, or (2) any employee of DHS in his/her official capacity, or (3) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent said employee, or (4) the United States or any agency thereof;

I. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. Sections 2904 and 2906;

J. To an appropriate Federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request;

K. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or for combating other significant public health threats;

L. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

M. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, under the terms of a memorandum of understanding or agreement, where CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law;

N. To appropriate agencies, entities, and persons when (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, harm to the security or integrity of this system or other systems or programs (whether maintained by CBP or another agency or entity), or harm to the individual that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the CBP's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

O. To the news media and the public and as appropriate, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of or is necessary to demonstrate the accountability of officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

The data is stored electronically at the CBP Data Center and in the future at a DHS Data Center for current data and offsite at an alternative data storage facility for historical logs and system backups.

RETRIEVABILITY:

The data is retrievable by name or personal identifier from an electronic database.

SAFEGUARDS:

All BCI records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include all of the following: Restricting access to those with a ''need to know''; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications.

BCI information is secured in full compliance with the requirements of the DHS IT Security Program Handbook as part of the TECS information technology platform. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including BCI, which is maintained on the TECS IT platform. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the

security aspects of their systems. System users must also complete annual privacy awareness training to maintain current access.

BCI transactions are tracked and can be monitored. This allows for oversight and audit capabilities to ensure that the data is being handled consistent with all applicable federal laws and regulations regarding privacy and data integrity. Data exchange, which will take place over an encrypted network between CBP and other DHS components that have access to the BCI data, is limited and confined only to those entities that have a need for the data in the performance of official duties. These encrypted networks comply with standards set forth in the Interconnection Security Agreements required to be executed prior to external access to a CBP computer system.

RETENTION AND DISPOSAL:

BCI data is subject to a retention requirement. CBP will be working with NARA to develop the appropriate retention schedule based on the information below. The information, as collected and maintained in BCI, is used for the purposes described above. For persons CBP determines to be U.S. Citizens (USC) and Lawful Permanent Residents (LPR), information in BCI that is related to a particular border crossing is maintained for fifteen years from the date that the traveler was admitted or paroled into the U.S., at which time it is deleted from BCI. For non-immigrant aliens, the information will be maintained for seventy-five (75) years from the date of admission/parole into the U.S. in order to ensure that the information related to a particular border crossing is available for providing any applicable benefits related to immigration or for other law enforcement purposes. For non-immigrant aliens who become United States citizens or LPRs following a border crossing that leads to the creation of a record in BCI, the information related to border crossings prior to that change in status will follow the 75-year retention period, but all information regarding border crossing by such persons following their change in status will follow the 15-year retention period applicable to USCs and LPRs. However, for all travelers, BCI records that are linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases will remain accessible for the life of the primary records for the law enforcement activities to which they may be or become related, to the extent retention for such purposes exceeds the normal retention period for such data in BCI.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Office of Automated Systems, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

NOTIFICATION PROCEDURES:

DHS allows persons (including foreign nationals) to seek administrative access under the Privacy Act to information maintained in BCI. To determine whether BCI contains records relating to you, write to the CBP Customer Service Center (Rosslyn, VA), 1300 Pennsylvania Avenue, NW., Washington, DC 20229; Telephone (877) 227–5511; or through the ''Questions'' tab at *http://www.cbp.gov.xp.cgov/travel/customerservice*.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, date of birth, and travel document (type and number) used for the crossing. You must sign your request, and your signature must either be notarized or submitted by you under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records, and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

Requests for notification or access must be in writing and should be addressed to the CBP Customer Service Center (Rosslyn VA), 1300 Pennsylvania Avenue, NW., Washington, DC 20229; Telephone (877) 227–5511; or through the ''Questions'' tab at *http://www.cbp.gov.xp.cgov/travel/customerservice.* Requests should conform to the requirements of 6 CFR part 5, subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS and can be found at *http://www.dhs.gov.* 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.

CONTESTING RECORD PROCEDURES:

Requests to amend a record must be in writing and should be addressed to the CBP Customer Service Center (Rosslyn VA), 1300 Pennsylvania Avenue, NW., Washington, DC 20229; Telephone (877) 227–5511; or through the ''Questions'' tab at *http://www.cbp.gov.xp.cgov/travel/customerservice.* Requests should conform to the requirements of 6 CFR part 5, subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS and can be found at *http://www.dhs.gov/foia.* 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.

If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program (''TRIP'') (See 72 FR 2294, dated January 18, 2007). DHS TRIP is a single point of contact for individuals 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 DHS TRIP, a traveler can request correction of erroneous data 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 *http://www.dhs.gov/trip.*

RECORD SOURCE CATEGORIES:

The system contains certain data received concerning individuals who arrive in, depart from, or transit through the United States. This system also contains information collected from carriers that operate vessels, vehicles, aircraft and/or trains that enter or exit the United States, including private aircraft operators.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

No exemption shall be asserted with respect to information maintained in the system at it relates to the border crossing, to the extent that such information was provided by the individual or carrier or an issuing authority in connection with a border crossing.

This system, however, may contain records or information pertaining to the accounting of disclosures made from BCI to other law enforcement or intelligence agencies (Federal, State, Local, Foreign, International or Tribal) in accordance with the published routine uses or statutory basis for disclosure under 5 U.S.C. 5(b). For the accounting of these disclosures only, in accordance with 5 U.S.C. 552a(j)(2), and (k)(2), DHS will claim the original exemptions for these records or information from subsection (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information.

Dated: July 18, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–17123 Filed 7–24–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket Number: DHS–2007–0016]

Privacy Act of 1974; U.S. Customs and Border Protection—Non-Federal Entity Data System, Systems of Records

AGENCY: Privacy Office; Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, U.S. Customs and Border Protection, Department of Homeland Security proposes to add the following system of records to its inventory of records systems, the Non-Federal Entity Data System. Certain States, Native American Tribes, Canadian Provinces and Territories, and other non-Federal Governmental Authorities may make available travel documents, such as Enhanced Driver's Licenses (EDLs), that may be deemed by the Secretary of DHS as denoting identity and citizenship for purposes of the Western Hemisphere Travel Initiative (WHTI), upon implementation, as mandated by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, 118 Stat. 3638 (2004). It is anticipated that all such documents will utilize facilitative technology such as Radio Frequency Identification (RFID), and contain a Machine Readable Zone (MRZ) using Optical Character Recognition (OCR) technology. In certain instances, other non-federal and foreign government authorities may provide to CBP biographical information and photographs that have been voluntarily submitted to the issuing entity by individuals choosing to apply for such travel documents, with the understanding that this information will be provided to DHS and CBP. DHS will use this information to facilitate the validation of travel documents when an individual crosses the border.

DATES: Comments must be provided by August 25, 2008. The new system of records will be effective August 25, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0016 by one of the following methods:

- Federal e-Rulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.
- Fax: 1–866–466–5370.
- Mail: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov*, including any personal information provided.
- Docket: For access to the docket to read background documents or comments received go to *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202–572–8790), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of International Trade, Regulations & Rulings, Mint Annex, 1300 Pennsylvania Ave., NW., Washington, DC 20229. For privacy issues contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The priority mission of U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. In response to this mission, Congressionally mandated, and as part of its efforts to secure the border, CBP and the Department of Homeland Security (DHS) plan to implement the Western Hemisphere Travel Initiative (WHTI), which eliminates a historical exemption that allowed certain travelers, notably U.S. and Canadian citizens, to enter the United States from within the Western Hemisphere without presenting a valid passport or other approved travel document. In advance of full WHTI implementation, DHS is working to close existing security gaps at the earliest possible opportunity, such as the implementation of new procedures for U.S. and Canadian citizens entering the U.S. that became effective January 31, 2008, and to prepare new secure travel document requirements that are expected to go into effect upon full WHTI implementation on June 1, 2009.

To facilitate border crossing for their citizens, certain states, Native American tribes, Canadian provinces and territories and other non-federal governmental authorities may make available to CBP biographical information and photographs associated with travel documents, such as Enhanced Driver's Licenses (EDLs). EDLs utilize facilitative technology such as RFID and contain a Machine Readable Zone (MRZ) using Optical Character Recognition (OCR) technology; they denote both identity and citizenship for border-crossing purposes. In certain instances, non-federal governmental authorities are choosing to provide to CBP biographical information and photographs that applicants for EDLs or similar travel documents have provided voluntarily to the issuing entity, with the understanding that such information will be stored by CBP for purposes of facilitating the document holder's crossing of the border. When a traveler presents such a document for purposes of entering the United States, CBP may validate this document and the information provided by the traveler, against the information provided to CBP by the issuing authority. Therefore, in accordance with the Privacy Act of