

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

1974, the Department of Homeland Security, U.S. Customs and Border Protection, proposes to add the following system of records to its inventory of records systems, the Non-Federal Entity Data System (NEDS).

II. Current Process for Border Crossing

Upon arrival, all individuals crossing the border are required to submit to inspection and be cleared for admission by CBP. As part of this clearance process, each traveler entering the United States must first establish his or her identity, nationality/citizenship, and admissibility to the satisfaction of a CBP officer. Additionally, CBP records the fact that the individual has been admitted or paroled into the United States. This record is maintained in a newly created Privacy Act System of Records, Border Crossing Information (BCI), which is being concurrently published in today's **Federal Register**. DHS has determined that certain border crossing travel documents enabled with RFID, MRZ and OCR technology will be accepted as proof of identity and citizenship and, further, may be accepted as WHTI-compliant travel documents upon implementation of WHTI.

The purpose of the Non-Federal Entity Data System (NEDS) is to have available to the CBP officer at the border the data related to certain border crossing travel documents. This will enable the CBP officer to quickly access the traveler's biographic information and photograph, when the traveler presents his or her border crossing travel document, to validate the authenticity of the travel document. Certain non-federal governmental authorities will choose to provide CBP with a copy of information derived from their EDL (or other traveler document) database, that denotes identity and citizenship, and can be used by CBP to validate the travel document. The datasets from each issuing authority will be kept separately such that information from one issuing authority is not commingled with another's information.

CBP may electronically validate the following information, where available, and record this information as part of the traveler's border crossing record: Full name (first, middle, and last), date of birth, gender, travel document type (e.g., EDL) and number or identifier, expiration date, issuing country or jurisdiction, country of citizenship, and photograph (when available). Where the issuing entity provides CBP with an advance copy of information from their travel document database, that data will be maintained in NEDS.

Upon arrival at the border, a person presenting proof of identity or citizenship issued by a non-federal governmental authority will have the identifier associated with her or his border crossing travel document read by the appropriate technology, such as an RFID reader, or the document information will be read using the MRZ or will be entered manually by the CBP officer. The identifier associated with this travel document will be transmitted through secure CBP computer networks to NEDS, where the unique number will be associated with the respective biographic information and photograph held in that system. The associated biographic information and photograph is then transmitted back through secure CBP computer networks to the port of entry and inspection terminal where the border crossing travel document was first read for confirmation that the document is a valid document and belongs to the person presenting the document to the CBP officer.

In cases where a traveler presents a federally issued travel document, such as a Visa, Passport or Passport card, or Border Crossing Card (BCC) issued by Department of State, or an I-551 Permanent Resident Card issued by U.S. Citizenship and Immigration Services (USCIS), DHS will validate the travel document through the use of systems or databases other than NEDS. NEDS is only employed when the travel document is issued by a non-federal government authority and that authority has provided CBP with advance information for purposes of validating such documents at the time of a U.S. border crossing. The data housed in NEDS is then used to populate biographical data fields contained in two other CBP systems, BCI (to record the entry of a traveler into the United States) and, where applicable, the Treasury Enforcement Communications System (TECS) (in the event some enforcement action is taken with regard to that traveler).

The traveler information held in NEDS is used by CBP to facilitate implementation of its mandates pursuant to the Enhanced Border Security and Visa Reform Act of 2002, Aviation and Transportation Security Act of 2001, the Intelligence Reform and Terrorism Prevention Act of 2004, the Tariff Act of 1930, as amended (19 U.S.C. 66, 1433, 1459, 1624, and 2071), and the Immigration and Nationality Act, as amended (8 U.S.C. 1185).

The information held within NEDS will be maintained and used in accordance with the individual memorandum of understanding/agreement with each issuing authority.

III. 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, whether they are U.S. citizens, lawful permanent residents, or non-immigrant aliens. The Non-Federal Entity Data System 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 are applicable 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.

In consideration of privacy, CBP has limited the sharing of NEDS data to the statutory disclosures permitted under 5 U.S.C. 552a(b) of the Privacy Act, and has chosen not to publish any routine uses pursuant to 5 U.S.C. 552a(b)(3). This provides an individual possessing an approved travel document, such as EDL, whose data is shared with CBP prior to crossing the border with a similar level of privacy as the individual whose data is shared at the time of crossing with CBP.

DHS is hereby publishing a description of the Non-Federal Entity Data System, 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-008

SYSTEM NAME:

Non-Federal Entity Data System (NEDS).

SYSTEM LOCATION:

These datasets are located at the U.S. Customs and Border Protection (CBP)

National Data Center. Computer terminals receiving the data are located at customhouses, border ports of entry, airport inspection facilities under the jurisdiction of 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 NEDS consist of persons, including U.S. Citizens and Canadian Citizens who have been issued Enhanced Driver's Licenses (EDL) or certain other travel documents by participating authorities, such as certain States, Native American Tribes, and Canadian Provinces and Territories, where the issuing authority has chosen to provide CBP with advance information from their databases regarding the EDL or other travel document. Individuals holding travel documents issued by authorities that do not provide CBP with a copy of this information (or only provide CBP with real-time access to document-specific information in their databases at the time such document is presented for border crossing purposes) are not covered by NEDS, as the information underlying their travel document has not been provided in advance to CBP.

CATEGORIES OF RECORDS IN THE SYSTEM:

NEDS will contain the following information, to the extent provided to CBP by the participating document-issuing authority:

- Full Name (first, middle, and last)
- Date of birth
- Gender
- Citizenship
- Digital Image (Photograph)
- Travel document type, e.g. Enhanced Driver's License (EDL)
- Issuing jurisdiction
- Expiration date
- Optical character read (OCR) identifier
- RFID tag number(s)

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The legal authority for NEDS is the Enhanced Border Security and Visa Reform Act of 2002, Pub. L. 107-173, 116 Stat. 543 (2002), Aviation and Transportation Security Act of 2001, Pub. L. 107-71, 115 Stat. 597 (2001), Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 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, 1459, 1624 and 2071, as well as the memoranda of understanding/agreement entered into with participating issuing authorities who are providing the data with which NEDS is populated.

PURPOSE:

CBP collects this information to expedite CBP processing upon an individual's arrival in and, in certain instances, prior to the individual's departure from the United States. This information will allow CBP, upon presentation of the travel document at the border, to electronically verify identity and citizenship, determine admissibility and perform law enforcement queries to identify security risks to the United States. This information is maintained in accordance with this system of records notice and applicable memoranda of understanding/agreement with the issuing authorities.

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

The use of this information is limited, principally to the verification of travel document information used to denote identity and citizenship so as to determine admissibility to the United States. To the extent data derived from NEDS is subsequently transferred to other systems of record (e.g., upon presentation of a travel document in conjunction with a border crossing), that data may be used in a manner consistent with the system of records notice published for the receiving system of records.

In consideration of privacy, CBP has limited the sharing of NEDS data to the statutory disclosures permitted under 5 U.S.C. 552a(b) of the Privacy Act, and has chosen not to publish routine uses pursuant to 5 U.S.C. 522a(b)(3). This provides an individual possessing an approved travel document, such as EDL, whose data is shared with CBP prior to crossing the border with a similar level of privacy protection as the individual whose data is shared with CBP at the time of such crossing.

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 for current data and

offsite at an alternative data storage facility for historical logs and system backups.

RETRIEVABILITY:

The data is retrievable by name, optical character recognition identifier, RFID tag number, or personal identifier from an electronic set of data.

SAFEGUARDS:

All NEDS 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.

NEDS information is secured in full compliance with the requirements of the DHS IT Security Program Handbook. 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 NEDS. 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.

NEDS 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 may be authorized to have access to NEDS data, is limited and confined only to those entities that have a need for the data in the performance of official duties.

RETENTION AND DISPOSAL:

NEDS data is subject to a retention requirement. The information collected and maintained in NEDS is used for border crossing purposes and is retained in NEDS for the duration of the validity of the travel document, that is from the date of issuance by the issuing authority until the date of expiration on the document, or, to the extent more restrictive, in accordance with the terms of any memorandum of understanding/agreement between CBP and the issuing authority. Information contained in NEDS will be retained and updated as information is provided by the issuing authority, so as to ensure timeliness, relevancy, accuracy, and completeness.

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 NEDS. To determine whether NEDS 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>.

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.

While DHS provides this mechanism for seeking notification and access to such information, requesters are encouraged in the first instance to contact the authority which issued the

travel document to request access to this information, as DHS may nonetheless be required to coordinate any release with such authorities.

CONTESTING RECORD PROCEDURES:

Requests to amend records 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). 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—such as, airports, seaports and train stations or at U.S. land borders. Through TRIP, a traveler can request correction of erroneous information 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 <http://www.dhs.gov/trip>.

Additionally, while DHS provides this mechanism for contesting records, requesters are encouraged in the first instance to contact the authority which issued the travel document to request access to this information, as DHS may nonetheless be required to coordinate any requests with such authorities.

RECORD SOURCE CATEGORIES:

The system contains certain data received on individuals who have chosen to obtain a travel document that is designated by the Secretary of Homeland Security as denoting identity and citizenship for purposes of entering the United States and has been issued by an authority which has provided CBP with advance information from its relevant travel document database.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: July 18, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-17126 Filed 7-24-08; 8:45 am]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY**U.S. Citizenship and Immigration Services****Agency Information Collection Activities: Form I-817, Extension of an Existing Information Collection; Comment Request**

ACTION: 30-Day Notice of Information Collection Under Review; Form I-817, Application for Family Unity Benefits; OMB Control No. 1615-0005.

The Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) has submitted the following information collection request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. The information collection was previously published in the **Federal Register** on May 13, 2008, at 73 FR 27549, allowing for a 60-day public comment period. USCIS did not receive any comments for this information collection.

The purpose of this notice is to allow an additional 30 days for public comments. Comments are encouraged and will be accepted until August 25, 2008. This process is conducted in accordance with 5 CFR 1320.10.

Written comments and/or suggestions regarding the item(s) contained in this notice, especially regarding the estimated public burden and associated response time, should be directed to the Department of Homeland Security (DHS), and to the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), USCIS Desk Officer. Comments may be submitted to: USCIS, Chief, Regulatory Management Division, Clearance Office, 111 Massachusetts Avenue, Suite 3008, Washington, DC 20529. Comments may also be submitted to DHS via facsimile to 202-272-8352 or via e-mail at rfs.regs@dhs.gov, and to the OMB USCIS Desk Officer via facsimile at 202-395-6974 or via e-mail at oir_submission@omb.eop.gov.

When submitting comments by e-mail please make sure to add OMB Control