9111-14 (non-Treasury)

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2013-0038]

Privacy Act of 1974; Department of Homeland Security U.S. Customs and Border Protection - 007 - Border Crossing Information System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security, U.S. Customs and Border Protection proposes to update and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security, U.S. Customs and Border Protection - 007 - Border Crossing Information System of Records." This system of records allows U.S. Customs and Border Protection to collect and maintain records on border crossing information for all individuals who enter, are admitted or paroled into, and - where available - exit from the United States, regardless of method or conveyance. This border crossing information includes certain biographical information; a photograph; certain itinerary information mandated or provided on a voluntary basis by air, sea, bus, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing.

This system of records notice was previously published in the Federal Register on July 25, 2008 (73 FR 43457). A Final Rule exempting portions of this system from certain provisions of the Privacy Act was published on February 3, 2010 (75 FR 5491).

As part of DHS's ongoing effort to increase transparency regarding its collection of information, DHS/CBP is updating (1) the categories of individuals to include persons entering Canada from the United States, (2) the categories of records to include border crossing data from Canada, (3) the sources of information to include data provided by the Canada Border Services Agency (CBSA), and (4) the routine uses to include the sharing of border crossing information with Canada. Additional routine uses were edited for clarity and for ease of use and understanding. In addition, DHS/CBP made non-substantive edits to the exemptions to ensure clarity.

DHS/CBP is updating this system of records notice to provide notice of the Beyond the Border (BTB) Entry/Exit Program with Canada. Through the Entry/Exit, the United States and Canada will exchange border crossing information about certain third-country nationals, permanent residents of Canada, and lawful permanent residents of the United States, at all automated land border ports of entry.

The exemptions for the existing system of records notice (July 25, 2008, 73 FR 43457) will continue to apply for this updated system of records notice and DHS will include this system in its inventory of record systems.

DATES AND COMMENTS: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. In particular, comments are requested concerning the application of the exemptions to the newly added categories of individuals, categories of records, routine uses, and sources of information for this system. This updated system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2013-0038 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 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, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Laurence E. Castelli (202-325-0280), Privacy Officer, U.S. Customs and Border Protection, 90 K Street NE, Washington, DC 20229. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) proposes to update and reissue a current DHS system of records titled, "DHS/CBP- 007 - Border

Crossing Information (BCI) System of Records."

The priority mission of CBP is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. To facilitate this mission, CBP maintains border crossing information for all individuals who enter, are admitted or paroled into, and—where available—exit from the United States, regardless of method or conveyance. This border crossing information includes certain biographical information; a photograph; certain itinerary information mandated or provided on a voluntary basis by air, sea, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing. This border crossing information resides on the TECS information technology platform. As part of DHS's ongoing effort to increase transparency regarding its collection of information, DHS/CBP is updating this system of records to provide notice to the public about the update and expansion of the (1) categories of individuals, (2) categories of records, (3) sources of information for this system, and (4) routine uses. DHS/CBP previously published this system of records notice in the Federal Register on July 25, 2008 (73 FR 43457).

As part of DHS/CBP's overall border security and enforcement missions, CBP is the agency responsible for collecting and reviewing border crossing information from travelers entering and departing the United States. 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, as applicable, to the satisfaction of a CBP officer. Additionally, CBP creates a record of an individual admission or parole into the United

States at a particular time and port of entry. CBP also collects information about individuals as they exit the United States for law enforcement purposes and to document the border crossing.

To further CBP's immigration and law enforcement missions, as well as facilitate cross-border travel, CBP is expanding the sharing of border crossing information collected from individuals as part of the Beyond the Border Entry/Exit Program. The program is divided into three phases. The first phase was a 90-day pilot program that tested the ability of DHS/CBP to match the data received from the Canada Border Services Agency (CBSA) to DHS/CBP existing entry records. Following the completion of the data match, DHS/CBP destroyed all data received through the pilot program.

The Beyond the Border Entry/Exit program is now entering the second phase, during which both countries intend to exchange border crossing information for third-country nationals, permanent residents of Canada, and lawful permanent residents of the United States at all automated land border ports of entry. CBP will not share information for U.S. citizens, Canadian citizens, asylees, refugees, individuals who have obtained a T, U, or Violence Against Women Act (VAWA) visa, or when the individual's citizenship is unknown. Individuals with a T, U, or VAWA visa fall under the U.S. government's victim protection visa program, which includes victims of human trafficking and domestic violence.

A future third phase is planned to allow CBP and CBSA to exchange entry data including U.S. citizens entering the U.S. and Canadian citizens entering Canada at any land port of entry between the U.S. and Canada. This exchange of border crossing entry

information will assist both countries so that the record of an entry into one country establishes an exit record from the other, ultimately supporting each country in their immigration and law enforcement missions, as well as facilitating cross-border travel.

CBP may collect the border crossing information stored in this system of records through a number of ways. For example, CBP may collect information from: (1) travel documents, such as foreign passport, presented by the individual at CBP ports of entry when the individual provided no advance notice of the border crossing to CBP; (2) carriers who submit information in advance of travel through the Advance Passenger Information System (APIS) (DHS/CBP-005 - Advance Passenger Information System (November 18, 2008, (73 FR 68435)); (3) information stored in DHS/CBP-002 - Global Enrollment System (GES) January 16, 2013 (78 FR 3441), as part of a trusted or registered traveler program; (4) 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); (5) 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; or (6) the CBSA pursuant to the Beyond the Border Entry/Exit Program. When a traveler is admitted, paroled into, or departs from the United States, the traveler's biographical information, photograph (when available), and crossing details (time and location) will be maintained in accordance with this BCI system of records.

DHS/CBP is updating the categories of individuals to include persons entering Canada from the United States for all individuals who enter, are admitted or paroled into,

and—where available—exit from the United States, regardless of method or conveyance. This border crossing information includes certain biographical information; a photograph; certain itinerary information mandated or provided on a voluntary basis by air, sea, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP- 007 - Border Crossing Information (BCI) may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security function. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice (SORN).

Through this updated SORN, DHS is requesting comment on the application of these exemptions to the newly added categories of individuals, categories of records, sources of information, and routine uses for this system.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. 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 an individual or by some identifying number, symbol, or other identifying particular

assigned to the individual. The Privacy Act defines an individual to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/CBP- 007 - Border Crossing Information (BCI) System of Records.

In accordance with 5 U.S.C. § 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) - 007

System name:

DHS/CBP - 007 - Border Crossing Information (BCI)

Security classification:

Unclassified, Sensitive, For Official Use Only, Law Enforcement-Sensitive.

System location:

Records are maintained at the CBP Headquarters in Washington, D.C. and field offices.

Categories of individuals covered by the system:

Individuals covered by BCI consist of persons, including U.S. citizens, lawful permanent residents, and immigrant and non-immigrant aliens who lawfully cross the United States border by air, land, or sea, regardless of method of transportation or

conveyance. This system also contains information about certain individuals, excluding known U.S. or Canadian citizens, who enter Canada from the United States.

Categories of records in the system:

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

When applicable, information derived from an associated APIS transmission, including:

- 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;
- for passengers and crew members who 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 private aircraft operators and carriers operating in the land border environment may transmit APIS, either voluntarily or pursuant to a legal mandate, similar information may also be recorded in BCI by CBP with regard to such travel.

In the land border environment for both arrival and departure (when departure

information is available), CBP also collects the License Plate number of the conveyance (or VIN number when no plate exists).

Under the Entry/Exist Program with Canada, records may also include border crossing data from the CBSA, including:

- Name (First, Middle, Last);
- Date of Birth;
- Nationality (citizenship);
- Gender;
- Document Type;
- Document Number;
- Document Country of Issuance;
- Port of entry location (Port code);
- Date of entry, and
- Time of entry.

Authority for maintenance of the system:

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

Purpose(s):

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 to 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 removed from the United States, or have been otherwise identified as potential security risks or raise a law enforcement concern. For immigrant and 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 the Department of Justice (DOJ), including U.S. Attorney Offices, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or 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 any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The U.S. or any agency thereof.

B. To a congressional office from 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.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency or organization for the purpose 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 appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other

systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS' efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, 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 appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To appropriate federal, state, tribal, local, 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, when DHS believes the information would assist enforcement of applicable civil or criminal laws.

I. To the Canada Border Services Agency for law enforcement and immigration purposes, as well as to facilitate cross-border travel, when an individual enters the United States from Canada.

J. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be relevant in countering the threat or potential threat.

K. To a federal, state, tribal, or local agency, other appropriate entity or individual, or foreign governments, in order to provide relevant information related to intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

L. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or when the information is relevant and necessary to the protection of life or property.

M. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purposes of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease, to

combat other significant public health threats, or to provide appropriate notice of any identified health threat or risk.

N. 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 law proceedings.

O. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation.

P. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when DHS is aware of a need to use relevant data for purposes of testing new technology and systems designed to enhance BCI.

Q. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, 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 DHS or is necessary to demonstrate the accountability of DHS's 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, and disposing of records in the system:

Storage:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

Records may be retrieved by name or other personal identifiers listed in the categories of records, above.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

CBP is working with NARA to develop the appropriate retention schedule based on the information below. 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 when the traveler was admitted or paroled into or departed 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 or departure from the United States 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 USCs 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. 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. For all travelers, however, BCI records linked to active law enforcement lookout records, DHS/CBP matches to enforcement activities, and/or investigations or cases will remain accessible for the life of the primary records of the law enforcement activities to which the BCI records may relate, to the extent retention for such purposes exceeds the normal retention period for such data in BCI.

System Manager and address:

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

Notification procedure:

DHS allows persons (including foreign nationals) to seek administrative access under the Privacy Act to information maintained in BCI. However, the Secretary of Homeland Security has exempted portions of this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. DHS/CBP, however, will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any

record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or CBP FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Lane, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

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, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted 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 Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should :

- Explain 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; and
- 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 the above information, the component(s) may 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:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

The system contains certain data received from 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. The system also contains border crossing information received from CBSA.

Exemptions claimed for the system:

No exemption shall be asserted with respect to border crossing information about an individual maintained in the system. In addition to the disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, information in the system may be shared with law enforcement and/or intelligence agencies pursuant to the above routine uses. The Privacy Act requires DHS to maintain an accounting of the disclosures made

pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement activities. The Secretary of Homeland Security, pursuant to 5 U.S.C. § 552a(j)(2), exempted this system from the following provisions of the Privacy Act: sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS has exempted section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(k)(2) as is necessary and appropriate to protect this information.

Dated: May 16, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-12388 Filed 05/24/2013 at 8:45 am; Publication Date: 05/28/2013]