9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0021]

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 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(BCI) 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 (when available) exit from the United States, regardless of method or conveyance. Border crossing information includes certain biographic and biometric information; photographs; certain mandatory or voluntary itinerary information provided 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 May 28, 2013 (78 FR 31958). A Final Rule exempting portions of this system from certain provisions of the Privacy Act was published on February 3, 2010, and remains in effect (75 FR 5491). The Department of Homeland Security/U.S. Customs and Border Protection is updating the categories of records to include the capture of biometric information including digital fingerprints, photographs, and iris scans at the border as part of the Department's ongoing effort to better reflect the categories of records in its collection of information. U.S. Customs and Border Protection also is updating the system of records notice to include the collection of records, including photographs of scars, marks, tattoos, and palm prints from individuals in connection with the biometric sharing between the Integrated Automated Fingerprint Identification System/Next Generation Identification of the Department of Justice /Federal Bureau of Investigation and the Department of Homeland Security Automated Biometric Identification System information technology platform. Finally, U.S. Customs and Border Protection is updating the categories of records collected from an associated Advance Passenger Information System transmission to accurately represent collection of personally identifiable information at the border.

The Department of Homeland Security/U.S. Customs and Border Protection is updating this system of records notice to provide notice of the collection of biometric information from U.S. citizens and certain aliens upon arrival to, and departure from, the United States.

The exemptions for the existing system of records notice published May 28, 2013 (78 FR 31958) continue to apply for this updated system of records for those categories of records listed in the previous BCI System of Records Notice. However, U.S. Customs and Border Protection will issue an updated notice and Final Rule to address that certain records ingested from the Advance Passenger Information System (APIS) (see DHS/CBP-005 Advance Passenger Information System (APIS) SORN, 80 FR 13407 (March 13, 2015)) will continue to be covered by the exemptions claimed for those records in that system pursuant to 5 U.S.C. 552a(j)(2) and 5 U.S.C. 552a(k)(2). The Department of Homeland Security will include this system in its inventory of record systems.

DATES: This updated system will be effective upon the public display of this notice. Although this system is effective upon publication, DHS will accept and consider comments from the public and evaluate the need for any revisions to this notice.

ADDRESSES: You may submit comments, identified by docket number DHS-2015-0021 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: Karen L. Neuman, 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: John Connors (202) 344-1610, Privacy Officer, U.S. Customs and Border Protection, Privacy and Diversity Office, 1300 Pennsylvania Avenue, Washington, D.C. 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, 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 System of Records." CBP is updating categories of records for this system of records notice (SORN) to better reflect the categories of records in the DHS/CBP Border Crossing Information system.

CBP's priority mission 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 about all individuals who enter, are

admitted or paroled into, and (when available) exit from the United States regardless of method or conveyance. Border crossing information includes certain biographic and biometric information; photographs; certain mandatory or voluntary itinerary information provided by air, sea, bus, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing. Border crossing information resides on the TECS (not an acronym) information technology platform. DHS/CBP is updating this system of records to provide notice to the public about the update and expansion of the categories of records as part of DHS's ongoing effort to better reflect the categories of records in its collection of information. DHS/CBP previously published this system of records notice in the Federal Register on May 28, 2013 (78 FR 31958).

CBP is responsible for collecting and reviewing border crossing information from travelers entering and departing the United States as part of DHS/CBP's overall border security and enforcement missions. All individuals crossing the border are subject to CBP processing upon arrival in the United States. Each traveler entering the United States is required to establish his or her identity, nationality, and admissibility, as applicable, to the satisfaction of a CBP officer during the clearance process. To manage this process, CBP creates a record of an individual's admission or parole into the United States at a particular time and port of entry. CBP also collects information about U.S. citizens and certain aliens (in-scope travelers pursuant to 8 CFR § 215.8, "requirements for biometric identifiers from aliens on departure from the United States") upon departure from the United States for law enforcement purposes and to document their border crossing.

DHS is statutorily mandated to create and integrate an automated entry and exit system that records the arrival and departure of aliens, verifies alien identities, and authenticates alien travel documents through the comparison of biometric identifiers (8 U.S.C. 1365(b)). Certain aliens may be required to provide biometrics (including digital fingerprint scans, palm prints, photographs, facial and iris images, or other biometric identifiers) upon arrival in or departure from the United States. The biometric data is stored in the Automated Biometric Identification System (IDENT) information technology platform. IDENT stores and processes biometric data (e.g., digital fingerprints, palm prints, photographs, and iris scans) and links biometrics with biographic information to establish and verify identities. The IDENT information technology platform serves as the biometric repository for the Department, and also stores related biographic information.

Previously DHS established the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program to manage an automated entry and exit system. On March 16, 2013, US-VISIT's entry and exit operations (including deployment of a biometric exit system) were transferred to CBP through the Consolidated and Further Continuing Appropriations Act of 2013 (Pub. L. 113-6, H.R. 933). The Act also transferred US-VISIT's overstay analysis function to U.S. Immigration and Customs Enforcement (ICE) and US-VISIT's biometric identity management services to the Office of Biometric Management (OBIM), which is a newly-created office within the National Protection and Programs Directorate (NPPD). CBP assumed biometric entry and exit operations on April 1, 2013.

CBP continues to develop mechanisms to collect biometric information from departing aliens since assuming responsibility for US-VISIT's entry and exit operations. During these operations, CBP officers may employ technology (e.g. wireless handheld devices or standalone kiosk) to collect biographic and biometric information from certain aliens determined to be in-scope pursuant to 8 CFR § 215.8 "Requirements for biometric identifiers from aliens on departure from the United States" prior to exiting the United States. Biometrics are checked against the IDENT system's watchlist of known or suspected terrorists (KST), criminals, and immigration violators to help determine if a person is using an alias or attempting to use fraudulent identification. Biographic and biometric data is encrypted when it is collected and the data is transmitted in an encrypted format to the IDENT system. The data is automatically deleted from the mobile device after the transmission is complete. The handheld mobile devices incorporate strict physical and procedural controls, such as Federal Information Processing Standard (FIPS)-compliant data encryption; residual information removal; and required authorization for users to sign-in using approved user account names and passwords.

Collection of additional biometric information from individuals crossing the border (such as information regarding scars, marks, tattoos, and palm prints) aids biometric sharing between the Department of Justice (DOJ) Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) and the IDENT system. The end result is enhanced access to (and in some cases acquisition of) IAFIS/NGI information by the IDENT system and its users. DHS, DOJ/FBI, and the

Department of State (DOS)/Bureau of Consular Services entered into a Memorandum of Understanding (MOU) for Improved Information Sharing Services in 2008. The MOUs established the framework for sharing information in accordance with an agreed-upon technical solution for expanded IDENT/IAFIS/NGI interoperability, which provides access to additional data for a greater number of authorized users.

CBP collects border crossing information stored in this system of records through a number of sources, for example: (1) travel documents (e.g., a foreign passport) presented by an individual at a CBP port of entry when he or she provided no advance notice of the border crossing to CBP; (2) carriers that submit information in advance of travel through the Advance Passenger Information System (APIS); (3) information stored in the Global Enrollment System (GES) (see DHS/CBP-002 Global Enrollment System (GES) SORN, 78 FR 3441, (January 16, 2013)) as part of a trusted or registered traveler program; (4) non-federal governmental authorities that issued valid travel documents approved by the Secretary of DHS (e.g., an Enhanced Driver's License (EDL)); (5) another federal agency that issued a valid travel document (e.g., data from a DOS visa, passport including passport card, or Border Crossing Card); or (6) the Canada Border Services Agency (CBSA) pursuant to the Beyond the Border Entry/Exit Program. When a traveler enters, is admitted to, paroled into, or departs from the United States, his or her biographical information, photograph (when available), and crossing details (time and location) is maintained in accordance with the DHS/CBP-007 Border Crossing Information SORN.

DHS/CBP is updating the categories of records to provide notice that CBP is

collecting biometrics such as digital fingerprints, photographs, and iris scans from certain non-U.S. citizens at the time of the border crossing or in support of their use of Global Entry or another trusted traveler program. In addition, CBP is updating the categories of records in the SORN to provide notice that CBP plans to collect information regarding scars, marks, tattoos, and palm prints from individuals at the border to aid biometric interoperability between the IAFIS/NGI and the IDENT system. Finally, CBP is updating the categories of records associated with APIS transmissions to better reflect the information collected and maintained in the DHS/CBP-007 BCI SORN.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-007 BCI SORN 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 functions.

The exemptions for the existing system of records notice published May 28, 2013 (78 FR 31958) continue to apply for this updated system of records for those categories of records listed in the previous System of Records Notice. However, several new categories of records may contain law enforcement sensitive information. Due to the nature of this information, CBP will issue an updated notice and final rule for proposed exemptions for these new categories of records pursuant to 5 U.S.C. 552a(j)(2) and 5 U.S.C. 552 a(k)(2). Furthermore, to the extent certain categories of records are ingested from other systems, the exemptions applicable to the source systems will remain in effect.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the Federal Government collects, maintains, uses, and disseminates 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. In the Privacy Act, an individual is defined 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 (FOUO), and Law Enforcement-

Sensitive (LES).

System location:

CBP maintains records at CBP Headquarters in Washington, D.C. and at field offices. This computer database is located at CBP National Data Center (NDC) in Washington, D.C. Computer terminals are located at customhouses, border ports of entry, airport inspection facilities under the jurisdiction of DHS, 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.

Categories of individuals covered by the system:

Individuals with records stored in BCI includes U.S. citizens, lawful permanent residents (LPR), and immigrant and non-immigrant aliens who lawfully cross the U.S. border by air, land, or sea, regardless of method of transportation or conveyance.

Categories of records in the system:

CBP collects and stores the following records in the BCI system as border crossing information:

- Full name (last, first, and, if available, middle);
- Date of birth;
- Gender;
- Travel document type and number (e.g., passport information, permanent resident card, Trusted Traveler Program card);
- Issuing country or entity and expiration date;

- Photograph (when available);
- Country of citizenship;
- Tattoos;
- Scars;
- Marks;
- Palm prints;
- Digital fingerprints;
- Photographs;
- Digital iris scans;
- Radio Frequency Identification (RFID) tag number(s) (if land or sea border crossing);
- Date and time of crossing;
- Lane for clearance processing;
- Location of crossing;
- Secondary Examination Status; and
- For land border crossings only, License Plate number or Vehicle Identification Number (VIN) (if no plate exists).

CBP maintains in BCI information derived from an associated APIS transmission (when applicable), including:

- Full name (last, first, and, if available, middle);
- Date of birth;
- Gender;

- Country of citizenship;
- Passport/alien registration number and country of issuance;
- Passport expiration date;
- Country of residence;
- Status on board the aircraft;
- Travel document type;
- United States destination address (for all private aircraft passengers and crew, and commercial air, rail, bus, and vessel passengers except for U.S. Citizens, LPRs, crew, and those in transit);
- Place of birth and address of permanent residence (commercial flight crew only);
- Pilot certificate number and country of issuance (flight crew only, if applicable);
- Passenger Name Record (PNR) locator number;
- Primary inspection lane;
- ID inspector;
- Records containing the results of comparisons of individuals to information maintained in CBP's law enforcement databases as well as information from the Terrorist Screening Database (TSDB);
- Information on individuals with outstanding wants or warrants; and
- Information from other government agencies regarding high risk parties.

CBP collects records under the Entry/Exit Program with Canada, such as border crossing data from the CBSA, including:

- Full name (last, first, and if available, middle);

- 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.

In addition, air and sea carriers or operators covered by the APIS rules and rail and bus carriers (to the extent voluntarily applicable) also transmit or provide the following information to CBP for retention in BCI:

- 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 passengers 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).
- For passengers and crew departing the United States:
    - Final foreign airport/port of arrival.

Other information also stored in this system of records includes:

- Aircraft registration number provided by pilots of private aircraft;
- Type of aircraft;
- Call sign (if available);
- CBP issued decal number (if available);
- Place of last departure (e.g., ICAO airport code, when available);
- Date and time of aircraft arrival;
- Estimated time and location of crossing U.S. border or coastline;
- Name of intended airport of first landing, if applicable;
- Owner or lessee name (first, last, and middle, if available, or business entity name);

- Owner or lessee contact information (address, city, state, zip code, country, telephone number, fax number, and email address, pilot, or private aircraft pilot name);
- Pilot information (license number, street address (number and street, city state, zip code, country, telephone number, fax number, and email address));
- Pilot license country of issuance;
- Operator name (for individuals: last, first, and middle, if available; or name of business entity, if available);
- Operator street address (number and street, city, state, zip code, country, telephone number, fax number, and email address);
- Aircraft color(s);
- Complete itinerary (foreign airport landings within 24 hours prior to landing in the United States);
- 24-hour emergency point of contact information (e.g., broker, dispatcher, repair shop, or other third party who is knowledgeable about this particular flight)
    - Full name (last, first, and middle (if available)) and telephone number;
- Incident to the transmission of required information via eAPIS (for general aviation itineraries, pilot, and passenger manifests), records will also incorporate the pilot's email address.

To the extent private aircraft operators and carriers operating in the land border environment may transmit APIS, similar information may also be recorded in BCI by CBP with regard to such travel. CBP also collects the license plate number of the

conveyance (or VIN number when no plate exists) in the land border environment for both arrival and departure (when departure information is available).

Authority for maintenance of the system:

Authority for BCI is provided by 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); 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 (8 U.S.C. 1185 and 1354); and the Tariff Act of 1930, as amended (19 U.S.C. §§ 1322-1683g, including 19 U.S.C. §§ 66, 1433, 1454, 1485, 1624 and 2071).

Purpose(s):

CBP collects and maintains this information to vet and inspect persons arriving in or departing from the United States; to determine identity, citizenship, and admissibility; and to identify persons who: (1) may be (or are suspected of being) a terrorist or having affiliations to terrorist organizations; (2) have active warrants for criminal activity; (3) are currently inadmissible or have been previously removed from the United States; or (4) 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 to ensure information related to a particular border crossing is available for providing any applicable benefits related to immigration or other enforcement purposes. Lastly, CBP maintains information in BCI to retain a historical

record of persons crossing the border to facilitate 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 Offices of the United States Attorneys, 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 United States 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's 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 CBSA 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 (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 the 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.

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:

CBP stores records in this system electronically in the operational system 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:

CBP retrieves records by name or other personal identifiers listed in the categories of records, above.

Safeguards:

DHS/CBP safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the

information that is being stored. CBP limits access to BCI to those individuals who have a need to know the information for the performance of their official duties and who also 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 and LPRs, information in BCI that is related to a particular border crossing is maintained for 15 years from the date when the traveler entered, was admitted to or paroled into, or departed the United States, at which time it is deleted from BCI. For non-immigrant aliens, the information will be maintained for 75 years from the date of admission or 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.

Information related to border crossings prior to a change in status will follow the 75 year retention period for non-immigrant aliens who become U.S. citizens or LPRs following a border crossing that leads to the creation of a record in BCI. All information regarding border crossing by such persons following their change in status will follow the 15 year retention period applicable to U.S. citizens and LPRs. For all travelers, however, BCI records linked to active law enforcement lookout records, DHS/CBP matches to enforcement activities, or investigations or cases 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, D.C. 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 DHS exempted portions of this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. Nonetheless, DHS/CBP 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 DHS Chief Freedom of Information Act (FOIA) Officer 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 that concern him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA 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 C.F.R. 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. Although 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

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, CBP 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:

BCI receives information from individuals who arrive in, depart from, or transit through the United States. This system also collects information from carriers that operate vessels, vehicles, aircraft, or trains that enter or exit the United States, including private aircraft operators. Lastly, BCI receives border crossing information received from CBSA.

Exemptions claimed for the system:

No exemption shall be asserted with respect to information maintained in the system that is ***collected from a person*** at the time of crossing and submitted by that person's air, sea, bus, or rail carriers if that person, or his or her agent, seeks access or amendment of such information.

The Privacy Act, however, 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.

Additionally, this system contains records or information recompiled from or created from information contained in other systems of records that are exempt from

certain provision of the Privacy Act. This system also contains accountings of disclosures made with respect to information maintained in the system. For these records or information only, in accordance with 5 U.S.C. 552a(j)(2) and (k)(2), DHS will also claim the original exemptions for these records or information from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f); and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information.

Dated: May 1, 2015

Karen L. Neuman
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2015-11288 Filed: 5/8/2015 08:45 am; Publication Date: 5/11/2015]