<NOTICE>

<PREAMB>

<AGENCY TYPE='S'>DEPARTMENT OF HOMELAND SECURITY

<DEPDOC>[Docket No. USCBP-2019-0043]

<SUBJECT>Privacy Act of 1974; System of Records

AGENCY: U.S. Customs and Border Protection, Department of Homeland Security.

ACTION: Notice of Modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue the current DHS system of records titled "Department of Homeland Security/U.S. Customs and Border Protection-002 Global Enrollment System," and rename it as "Department of Homeland Security/U.S. Customs and Border Protection-002 Trusted and Registered Traveler Programs." This system of records allows the Department of Homeland Security/U.S. Customs and Border Protection (CBP) to collect and maintain records on individuals who voluntarily provide personally identifiable information to CBP in return for enrollment in a program that will make them eligible for dedicated CBP processing at designated U.S. border ports of entry, including all trusted traveler and registered traveler programs.

DATES: Submit comments on or before **April 10, 2020**. This modified system will be effective April 10, 2020.

ADDRESSES: You may submit comments, identified by docket number USCBP-2019-0043 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. 20528-0655.

Instructions: All submissions received must include the agency name and docket number USCBP-2019-0043. 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: Debra L. Danisek, (202) 344-1610, privacy.cbp@cbp.dhs.gov, CBP Privacy Officer, U.S. Customs and Border Protection, Ronald Reagan Building, 1300 Pennsylvania Avenue, NW, Washington, D.C. 20229. For privacy issues, please contact: Jonathan R. Cantor (202) 343-1717, Privacy@hq.dhs.gov, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, DHS/CBP proposes to update, rename, and reissue a current DHS system of records newly titled, "DHS/CBP-002 Trusted and Registered Traveler Programs (TRTP)." Formerly titled the "Global Enrollment System," this system of records allows CBP to collect and maintain records on individuals who voluntarily provide personally identifiable information to CBP in

return for enrollment in a program that will make them eligible for dedicated CBP processing at designated U.S. border ports of entry. This system of records includes information on individuals who participate in trusted traveler and registered traveler programs. This system of records notice is being re-published under the new name, with a more comprehensive description of these programs, and the removal of references to the CBP Trusted Worker Programs, which are covered under the DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities System of Records Notice (December 19, 2008, 73 FR 77753).

Trusted traveler programs facilitate processing for pre-approved members, permitting more efficient inspections, and helping move participants through the lines at the port of entry or other designated locations more expeditiously. CBP's trusted traveler programs include:

- Global Entry,[1] which enables CBP to provide U.S. citizens, lawful permanent residents (LPRs), and citizens of certain foreign countries dedicated processing when arriving at airports with designated Global Entry kiosks.

- NEXUS, which allows pre-screened travelers dedicated processing when entering the United States and Canada. Program members use specific processing lanes at designated U.S.-Canada border ports of entry, NEXUS kiosks when entering Canada by air, and Global Entry kiosks when entering the United States via Canadian Preclearance airports. NEXUS members

[1] Final Rule, Establishment of Global Entry Program (77 FR 5681, Feb. 6, 2012).

also receive dedicated processing at marine reporting locations.

- Secure Electronic Network for Travelers Rapid Inspection (SENTRI), which provides dedicated processing clearance for pre-approved travelers using designated primary lanes entering the United States at land border ports of entry along the U.S.-Mexico border.
- The Free and Secure Trade (FAST) program, which provides dedicated processing for pre-approved commercial truck drivers from the United States, Canada, and Mexico. Members may use dedicated FAST lanes at both northern and southern border ports.
- The U.S.-Asia Economic Cooperation (APEC) Business Travel Card (ABTC) Program, which allows for U.S. business travelers or government officials engaged in business in the APEC region dedicated screening at participating airports.

Individuals who apply for enrollment in a trusted traveler program must provide biographic and certain biometric information to CBP, as described below. CBP screens this information against databases to verify eligibility for trusted traveler program participation. Once an applicant is approved and enrolls in the trusted traveler program, his or her information is vetted by CBP on a recurrent basis to ensure continued eligibility.

CBP also sponsors registered traveler programs that, like trusted traveler programs, allow individuals to provide their information to CBP voluntarily prior to

travel in order to qualify for dedicated processing. Unlike trusted travelers, registered travelers are not subject to vetting, but rather maintain information on file with CBP to better facilitate their arrival at ports of entry.

Registered traveler programs include:

- Decal and Transponder Online Procurement System (DTOPS), which allows individuals registered to eligible commercial vehicles to pay their annual user fees in advance online and cross the border using decals or transponders that facilitate CBP inspection.

- Pleasure boat reporting options, which allow operators of small vessels arriving in the United States from a foreign location to report their arrival to CBP remotely instead of in person as required under 19 U.S.C. 1433. Travelers who are members of another CBP trusted traveler program, who hold an I-68 Canadian Border boat landing permit, or who participate in the Local Border Option (LBO) may be eligible for remote arrival reporting.

CBP has signed a number of joint statements with foreign partners to permit citizens of certain foreign countries to apply for Global Entry. Some of these joint statements also permit Global Entry members to apply for trusted traveler programs operated by foreign partners. CBP continues to work with government border authorities in various countries to create this growing international network. As part of the procedure for implementing a joint statement, and adding foreign partners to Global Entry, CBP and each foreign partner execute parallel procedures that incorporate privacy protections. A more in-depth discussion of the arrangements by country is made available in

DHS/CBP/PIA-002(b) GES Privacy Impact Assessment and Appendix A "CBP Global Entry Expansion: Joint Statements."

The authority for TRTP derives from CBP's mandate to secure the borders of the United States, and to facilitate legitimate trade and travel. The statutes that permit and define these programs include:

- Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, 8 U.S.C. 1365b(k);
- Section 215 of the Immigration and Nationality Act, as amended, 8 U.S.C. 1185;
- Section 402 of the Homeland Security Act of 2002, as amended, 6 U.S.C. 202;
- Section 404 of the Enhanced Border Security and Visa Reform Act of 2002, 8 U.S.C. 1753; and
- Section 433 of the Tariff Act of 1930, as amended, 19 U.S.C. 1433.

The Regulations that permit and define TRTP include Parts 103 and 235 of Title 8 of the Code of Federal Regulations. See, especially, 8 CFR §§ 103.2, 103.7, 103.16, 235.1, 235.2, 235.7, and 235.12. Pursuant to the Independent Offices Appropriations Act of 1952, 31 U.S.C. 9701, individuals seeking to enroll in trusted traveler or registered traveler programs must pay a fee when they apply or renew their membership. *See* 8 CFR § 103.7(b)(1)(ii)(M).

Participation in these programs is entirely voluntary. Joint Statements with

foreign partners establish that each country's use of GES information for vetting will be consistent with applicable domestic laws and policies. Participants should be aware that when they submit their information to a foreign country or agree to share their information with a foreign partner, the foreign country uses, maintains, retains, or disseminates their information in accordance with that foreign country's laws and privacy protections.

Consistent with DHS's information sharing mission, GES information may be shared with other DHS components whose personnel have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. 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.

DHS/CBP is simultaneously issuing a notice of proposed rulemaking to exempt portions of the DHS/CBP-002 TRTP SORN from the Privacy Act requirements. Pursuant to 5 U.S.C. 552a(j)(2) of the Privacy Act, law enforcement related records, including the information from other law enforcement databases that support the DHS/CBP membership decision, and the law enforcement risk assessment worksheet that have been created during the background check and vetting process, are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); (f); and (g)(1). Pursuant to 5 U.S.C. 552a(k)(2), records created during the background check and vetting process are exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). In

addition, when a record contains information from other exempt systems of records, DHS/CBP will claim the same exemptions for that record as are claimed for the original systems of records and will claim any additional exemptions that this notice delineates.

CBP will not assert any exemptions with regard to accessing or amending an individual's application data in a trusted or registered traveler program and/or final membership determination in the trusted traveler programs. However, this data may be shared with law enforcement and/or intelligence agencies pursuant to the routine uses identified in the TRTP SORN. The Privacy Act requires that DHS maintain an accounting of such disclosures made pursuant to all routine uses. Disclosing the fact that a law enforcement and/or intelligence agency has sought particular records may affect ongoing law enforcement activity. As such, pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), DHS will claim an exemption from (c)(3), (e)(8), and (g)(1) of the Privacy Act, as is necessary and appropriate to protect this information. This updated system will be included in DHS's inventory of record systems.

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. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial

Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/CBP-002 TRTP System of Records.

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

<PRIACT><HD2>SYSTEM NAME AND NUMBER:

Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-002 Trusted and Registered Traveler Programs (TRTP).

<HD2>SECURITY CLASSIFICATION:

Unclassified.

<HD2>SYSTEM LOCATION:

Records are maintained at the CBP Headquarters in Washington, D.C. and field offices. CBP maintains records in the Trusted Traveler Programs (TTP) information technology system, as well as other applications that support trusted traveler and registered traveler application and program management. CBP may also maintain these records in various CBP law enforcement systems for participant screening.

<HD2>SYSTEM MANAGER(S):

Trusted Traveler Program Manager, Office of Field Operations, and Executive Director, Passenger Systems Program Directorate, Office of Information and Technology, U.S. Customs and Border Protection, 1300 Pennsylvania Ave., NW, Washington, D.C. 20229.

<HD2>AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, 8 U.S.C. 1365b(k); Section 215 of the Immigration and Nationality Act, as amended, 8 U.S.C. 1185; Section 402 of the Homeland Security Act of 2002, as amended, 6 U.S.C. 202; Section 404 of the Enhanced Border Security and Visa Reform Act of 2002, 8 U.S.C. 1753; Section 433 of the Tariff Act of 1930, as amended, 19 U.S.C. 1433; 31 U.S.C. 9701; and Parts 103 and 235 of Title 8 of the Code of Federal Regulations (See, especially, 8 C.F.R. §§ 103.2, 103.7, 103.16, 235.1, 235.2, 235.7, and 235.12).

<HD2>PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to assess on an ongoing basis applicants' eligibility for enrollment in trusted traveler and registered traveler programs.

<HD2>CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who apply to use any form of automated or other expedited inspection for verifying eligibility to cross the border into the United States.

<HD2>CATEGORIES OF RECORDS IN THE SYSTEM:

TRTP collects the following information on trusted travelers:

Biographic application data, including:

- Full name;
- Alias(es);
- Date of birth;
- Place of birth;
- Language preference;
- Gender;

- Current and former addresses;
- Telephone numbers;
- IP address;
- Country of citizenship;
- Alien registration number (if applicable);
- Employment history (if available);
- PASS ID or Trusted Traveler membership number;
- Countries visited in the last five years;
- Criminal history (provided by applicant);
- Parental or Legal Guardian permission (if 18 years or younger);
- Driver's license number;
- Issuing state or province of the applicant's Driver's License;
- Trusted Traveler Program System (TTP) user name and password (password is maintained in an encrypted format); and
- Answers to security questions to reset password.

Vehicle or Vessel information, as appropriate, including:

- Flag and home port (where the vessel is foreign flagged);
- Name, registration number, and registration issuing state or province of the applicant's vessel;
- Make and model, year, color, Vehicle Identification Number (VIN), and license plate number of the vehicle; and
- Owner name, gender, and date of birth.

Biometric data, including:

- Fingerprints (collected and stored through the DHS Automated Biometric Identification System (IDENT) for future identity verification);
- Fingerprint Identification Number (FIN);
- Height;
- Eye color; and
- Facial photographs.

Information added by DHS/CBP:

- Criminal history information, as well as responsive information from other law enforcement databases that support the DHS/CBP membership decision;
- Law enforcement risk assessment worksheet;
- Pay.gov tracking number;
- Program membership decision in the form of a "pass/fail;" and
- Foreign government membership decisions in the form of a "pass/fail."

The following information is collected on registered pleasure boat travelers:

- Full name;
- Gender;
- Date of birth;
- Place of birth;
- Country of citizenship;
- Address;
- Contact telephone number;

- Alternate telephone number;
- Contact email address;
- Password;
- Document type and number (e.g., U.S. Passport, Permanent Resident Card, Birth Certificate), place of issue, and expiration date of document; and
- Vessel information including registration number, hull ID number, decal number, registered name, location where vessel is registered, and vessel description (e.g., length, type, manufacturer, model, year, hull colors).

The following information is collected about Decal and Transponder Online Procurement System (DTOPS) registered travelers:

- Account name;
- Physical address;
- Shipping address;
- Pay.gov tracking number;
- Free and Secure Trade (FAST) ID, if the conveyance's owner is Customs Trade Partnership Against Terrorism (C-TPAT)/FAST approved;
- Conveyance model year;
- Conveyance manufacturer name;
- Conveyance identification numbers and information, which are specific to the type of conveyance (e.g., local registration number, an aircraft's tail number, Coast Guard ID number, vessel name);
- Contact name;
- Contact telephone number; and

- Contact email address.

<HD2>RECORD SOURCE CATEGORIES:

TRTP records are obtained from the individual and from external law enforcement systems. DHS/CBP may use a number of DHS/CBP databases during the vetting process before individuals will be enrolled and accepted in any trusted traveler program. These databases include the Automated Targeting System (ATS), which contains historical and enforcement data on travelers, and provides a gateway to other sources of data. These other external sources include the Terrorist Screening Database, FBI criminal history, and National Crime and Information Center outstanding wants/warrants, vehicle and driver's license-related data contained in the International Justice and Public Safety Network's National Law Enforcement Telecommunications System (Nlets) system, and Department of State alien records, lookouts, and status indicators. Vetting results are also based on checks of the FBI's Integrated Automated Fingerprint Identification System for criminal history and IDENT for immigration related records. Trusted traveler applicants from partnering foreign countries will have membership determinations recorded in TRTP that are received by DHS/CBP from their home country's government.

<HD2>ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. sec. 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. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agencies 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, only 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. secs. 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 there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

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 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.

I. To foreign governments, at the request of the individual, for the purpose of applying to that country's trusted traveler program.

J. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency for the purpose of determining an individual's eligibility for membership in a trusted traveler or registered traveler program.

K. To federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or to assist in anti-terrorism efforts.

L. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate in the proper performance of the official duties of the officer making the disclosure.

M. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, which relate to the purpose(s) stated in this SORN, for purposes of testing new technology.

N. 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, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

<HD2>POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

DHS/CBP stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

<HD2>POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by any of the personal identifiers listed in the categories of records above.

<HD2>POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

CBP is proposing to NARA the following retention schedules: Trusted traveler data is retained for the duration of an individual's active membership plus three years after an individual's membership is no longer active, either as a result of expiration without renewal at the end of a five-year term, as a result of abandonment, or as a result of CBP termination. DTOPS master file data is retained for twelve years after the account, decal, transponder, or VIN is inactive or deactivated.

<HD2>ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/CBP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. CBP has imposed strict controls to minimize the risk of compromising the information that is being 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.

<HD2>RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/CBP will consider individual requests to determine whether information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and CBP's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." 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, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about the individual may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual 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, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes 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 the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

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

<HD2>CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to CBP. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

Regardless of whether the Privacy Act or JRA applies, travelers who believe that records in this system maintain incorrect or inaccurate information may direct inquiries to the CBP Info Center, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. Travelers may also contact the DHS Traveler Redress Inquiry Program (DHS TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/dhs-trip if they have experienced a travel-related screening difficulty, including those they believe may be related to incorrect or inaccurate information retained in their record(s).

<HD2>NOTIFICATION PROCEDURES:

See "Record Access Procedures" above.

<HD2>EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2) seeks to exempt the law enforcement related records, including information from other law enforcement databases that support the DHS/CBP membership decision, and the law enforcement risk assessment worksheet that have been created during the background check and vetting process, from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), seeks to exempt records created during the background check and vetting process from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H),(e)(4)(I); and (f).

Also, the Privacy Act requires DHS maintain an accounting of such disclosures made pursuant to all routine uses. However, disclosing the fact that CBP has disclosed records covered by this SORN to an external law enforcement and/or intelligence agency

may negatively affect and interfere with ongoing law enforcement, intelligence, or national security activity. As such, pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), DHS will claim an exemption from (c)(3), (e)(8), and (g)(1) of the Privacy Act, as is necessary and appropriate to protect this information.

In addition, when a record contains information from other exempt systems of records, DHS/CBP will claim the same exemptions for that record as are claimed for the original systems of records and will claim any additional exemptions that this notice delineates.

Finally, in its discretion, CBP may not assert any exemptions with regard to accessing or amending an individual's application data in a trusted or registered traveler program or accessing their final membership determination in the trusted traveler programs.

<HD2>HISTORY:

DHS/CBP-002 Global Enrollment System, 78 FR 3441 (January 18, 2013); DHS/CBP-002 Global Enrollment System of Records, 71 FR 20708 (April 21, 2006).</PRIACT>

<SIG><NAME>Jonathan R. Cantor,

<TITLE>Acting Chief Privacy Officer,

Department of Homeland Security.</SIG>

<FRDOC> [FR Doc. 2020–04980 Filed 3–10–20; 8:45 am]

<BILCOD> BILLING CODE 9111–14–P

[FR Doc. 2020-04980 Filed: 3/10/2020 8:45 am; Publication Date: 3/11/2020]