This document is scheduled to be published in the Federal Register on 03/11/2020 and available online at **federalregister.gov/d/2020-04984**, and on **govinfo.gov**

9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. USCBP-2019-0044]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection-002 Trusted and Registered Traveler Programs (TRTP) System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a modified and reissued system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/U.S. Customs and Border Protection-002 Trusted and Registered Traveler Programs," previously titled "Global Enrollment System (GES) System of Records," and this proposed rulemaking. In this proposed rulemaking, the Department and the U.S. Customs and Border Protection (CBP) proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number USCBP-2019-0044, 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 notice. 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 Danisek, (202) 344-1610, CBP Privacy Officer, U.S. Customs and Border Protection, 1300 Pennsylvania Ave, NW, Washington, D.C. 20229. For privacy issues, please contact: Jonathan R. Cantor, Privacy@hq.dhs.gov, (202) 343-1717, 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 (SORN) 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). A fuller description of this revised SORN can be found herein the Federal Register.

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 also receive dedicated

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

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 in the system of records notice. 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.

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 the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Similarly, 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. The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed and provide an opportunity for public comment.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/CBP-002 TRTP System of Records. Some information in DHS/CBP-002 TRTP System of Records relates to official DHS national security, law enforcement, and immigration activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes or to avoid disclosure of activity techniques. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

A notice of system of records for DHS/ DHS/CBP-002 TRTP System of Records is also published in this issue of the Federal Register.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The general authority citation for Part 5 continues to read as follows:

Authority: 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301.

* * * * *

2. Add, at the end of Appendix C to Part 5, paragraph “82” to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

82. The DHS/U.S. Customs and Border Protection (CBP)-002 Trusted and Registered Traveler Program (TRTP) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP-002 TRTP System of Records collects and maintains records on individuals who voluntarily provide personally identifiable information to U.S. Customs and Border Protection in return for enrollment in a program that will make them eligible for dedicated CBP processing at designated U.S. border ports of entry and foreign preclearance facilities. The DHS/CBP-002 TRTP system of records contains personally identifiable information in biographic application data, biometric information, conveyance information, pointer information to other law enforcement databases that support the DHS/CBP membership decision, Law Enforcement risk assessment worksheets, payment tracking numbers, and U.S. or foreign trusted traveler membership decisions in the form of a "pass/fail."

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted 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 to an external law enforcement and/or intelligence agency may affect ongoing law enforcement, intelligence, or national security activity. As such, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2) and (k)(2) has exempted these records 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 received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

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 or registered traveler programs.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and

to avoid detection or apprehension, which would undermine the entire investigative process. When an investigation has been completed, information on disclosures made may continue to be exempted if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2020-04984 Filed: 3/10/2020 8:45 am; Publication Date: 3/11/2020]