Privacy Impact Assessment
for the

Global Enrollment System

DHS/CBP/PIA-002(b)

January 10, 2013

Contact Point
Cheryl C. Peters
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1438

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Global Enrollment System (GES) allows U.S. Customs and Border Protection (CBP), a component within the Department of Homeland Security (DHS), to handle the enrollment and vetting processes for trusted traveler and registered traveler programs in a centralized environment. Individuals who wish to participate in these programs voluntarily provide personally identifiable information (PII) to CBP in return for expedited transit at designated U.S. border ports of entry (POE). This Privacy Impact Assessment (PIA) is being conducted to describe CBP's trusted traveler programs, including specific improvements to the Global Entry (GE) trusted traveler program and to the Global Online Enrollment System (GOES), which is the standard application process for almost all trusted traveler programs. This PIA also describes CBP's registered traveler programs, which include the Small Vessel Reporting System (SVRS) and the Decal and Transponder Online Procurement System (DTOPS). The GES PIAs of April 20, 2006, and November 1, 2006, will be retired upon publication of this PIA.

Overview

The Global Enrollment System (GES) allows U.S. Customs and Border Protection (CBP), a component within the Department of Homeland Security (DHS), to handle the enrollment and vetting processes for trusted traveler and registered traveler programs[1] in a centralized environment. Individuals who wish to participate in these programs voluntarily provide personally identifiable information (PII) to CBP in return for expedited processing at designated U.S. border ports of entry (POE). CBP is therefore able to expedite the inspection and security process for these lower risk travelers and allow more scrutiny for those travelers who present an unknown risk.

This PIA describes CBP's trusted traveler programs, which include: Global Entry (GE), NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Free and Secure Trade (FAST). In addition, substantial improvements are being made to GE and the enrollment and vetting processes through the Global Online Enrollment System (GOES). GE, previously a pilot program, is now a permanent trusted traveler program.[2] Under GE, expedited processing into the U.S. and certain foreign countries will be expanded through a growing number of participating U.S. and foreign international airports and foreign partnerships. Through such partnerships, U.S. citizens and citizens of certain foreign countries will be able to apply for expedited clearance and admission at their respective airports. GOES, previously an optional online application process, is now the standard application process for almost all trusted traveler programs. SENTRI is the only program for which both electronic and paper applications (SENTRI Application, CBP Form 823S) are accepted.

This PIA also describes CBP's registered traveler programs, which include the Small Vessel Reporting System (SVRS) and the Decal and Transponder Online Procurement System (DTOPS). SVRS

[1] Trusted traveler and registered traveler programs typically require the same or similar types of personally identifiable information to be submitted by an individual; the difference between these programs is the level of vetting and screening conducted on individuals who apply to participate, for example trusted traveler programs require ongoing vetting of individuals while the individual maintains the benefit; while registered travelers do not.
[2] *See* Establishment of Global Entry Program; Final Rule, 77 Fed. Reg. 5681 (February 6, 2012).

is a registered traveler pilot program that, as an enhancement to the Local Boater Option (LBO), allows individuals with advance CBP approval of float plans to utilize a designated telephone line to notify a CBP officer of their arrival to the United States. DTOPS is a permanent registered traveler program that allows individuals to purchase, renew, or transfer user fees related to the transponders/Radio Frequency Identification (RFID) tags for their commercial vehicles or to the decals for their private aircraft or vessels in advance of crossing a U.S. border.

Background

Trusted traveler programs pre-dated the creation of DHS/CBP and were designed and implemented by predecessor agencies Immigration and Naturalization Service (INS) and the U.S. Customs Service. Subsequently, the biographical and biometric data collected from applicants and participants in these programs were stored through the use of localized application and enrollment processes and several stand-alone POE level databases.[3] As each of these programs conducted application, enrollment, and background checks in similar fashions, CBP developed a consolidated and more efficient national approach to support them,[4] and then adopted the GES name. GES is now the backbone IT system that supports all trusted traveler and certain registered traveler programs. For these programs, GES is the sole repository for enrollment, application, and background investigation data. Furthermore, CBP's ability to standardize the risk assessment process through GES reduces the administrative burden on CBP to re-vet applicants and the need for individuals to provide redundant data for applications to different programs.

GES currently supports over one million enrollees in trusted traveler and registered traveler programs. An individual's participation in any of the trusted traveler and registered traveler programs is completely voluntary. Under these programs, an individual agrees to provide personal biographical data and, in the case of trusted traveler programs, biometric data, so that CBP may determine his or her eligibility for the program. Upon being granted such eligibility, the individual may be provided expedited processing through designated U.S. border POEs, including the U.S. border at participating U.S. international airports and at the airports of CBP's respective international partners.

As domestic and international interest and participation in these programs continue to grow and GES has the capability to incorporate any future changes and improvements from these programs, CBP will provide additional updates through this PIA and other applicable DHS privacy documentation.

Trusted Traveler Programs

Trusted traveler programs provide expedited travel for pre-approved, low-risk international travelers through dedicated lanes and kiosks and include GE, NEXUS, SENTRI, and FAST. The data collection and vetting criteria and standards for these programs are similar. CBP ensures the individual's

[3] The System of Records Notice (SORN) for this precursor system was published by the former INS. *See* Global Enrollment System (GES) System of Records, Justice/INS-01762 Fed. Reg. 11919 (Mar. 13, 1997). This system was also referred to as the Global Enrollment System. Under DHS/CBP-002, the local GES SORN was updated to reflect the expansion and enhancement of the now national GES. *See* Global Enrollment System (GES) System of Records, DHS/CBP-002, 71 Fed. Reg. 20708 (Apr. 21, 2006).

[4] DHS/CBP published the April 20, 2006 PIA after DHS's reorganization, pursuant to the Homeland Security Act of 2002 (6 U.S.C. § 101 et seq.).

continued eligibility by performing daily checks of the individual's biographic information against a list of law enforcement wants or warrants. Each trusted traveler program is generally described below.[5]

Global Entry

GE, initially operating as a trusted traveler pilot program, is now a permanent trusted traveler program that allows for the expedited clearance of pre-approved, low-risk international air travelers through participating U.S. international airports.

All individuals who apply for GE membership[6] must undergo a rigorous background check and interview, conducted by a CBP officer, at a U.S. designated enrollment center. GES maintains vetting results with corresponding law enforcement database record numbers used to support the membership decision. As part of the interview process, biometric data is captured from GE applicants, which includes fingerprints stored by US-VISIT's Enumeration Services of the Automated Biometric Identification System (IDENT)[7] and facial photographs. Individuals who seek enrollment in a foreign country's trusted traveler program may also undergo an interview conducted by representatives from border agencies of the respective participating international partner country.

Approved individuals are provided expedited processing through the U.S. border at participating U.S. international airports. Upon entering such airport, an approved traveler may walk up to a dedicated GE lane, present his or her machine-readable passport or U.S. permanent resident card at a GE kiosk, and submit his or her fingerprints for scanning so that his or her identity can be matched to the fingerprints on file. Also at the kiosk, the traveler will make a customs declaration. Once these actions are completed, the kiosk will issue the traveler a transaction receipt, which will either direct him or her to the airport exit or to a CBP officer for further inspection. In addition, the expedited clearance processes may entail additional step(s) for travelers with a nonimmigrant visa or seeking admission under the Visa Waiver Program. These travelers will have additional screens to complete at the kiosk to determine the class of admission and period of stay for the traveler, and the kiosk will print the appropriate admission document at the end of the transaction.

GE enables CBP to expedite the inspection and security process for lower-risk travelers and focus its resources on other travelers. Additional improvements being made to GE include the expansion of participating U.S. and foreign international airports and foreign partnerships. The selection of participating U.S. international airports has typically been based on airports that experience the largest number of travelers arriving from outside of the United States. It is important to note that not every U.S. international airport offers GE kiosks for members to use; however, CBP plans to expand upon this roster in the future.[8]

---

[5] For additional information about trusted traveler programs, see http://www.cbp.gov/xp/cgov/travel/trusted_traveler/.

[6] For a list of conditions that could disqualify an individual for GE membership, see the Frequently Asked Questions page at http://www.globalentry.gov/faq html.

[7] For more information on IDENT's use of biometrics, see DHS/USVISIT-0012- IDENT System of Records, 72 Fed. Reg. 31080 (Jun. 5, 2007) (IDENT SORN), and DHS/NPPD/USVISIT/PIA-002 IDENT PIA, both of which are available at http://www.dhs.gov/privacy.

[8] For a current list of participating U.S. international airports, see http://www.globalentry.gov/terminalmaps html.

The addition of foreign partners will allow U.S. citizens (USC) and citizens of certain foreign countries to apply for expedited clearance and admission. Foreign partners may be added to GE through joint statements, some of which may be reciprocal, between the United States and a foreign country. The general purpose of the joint statement is to offer expedited entry to USCs and the citizens of the foreign country that is party to that joint statement, based on a mutually-determined set of vetting criteria and standards. CBP continues to work with government border authorities in various countries to create this growing international network in which, once individuals are screened and deemed trusted by the authorities in their own country, the other country in the alliance will accept them in their respective national trusted traveler programs (see Appendix A, *CBP Global Entry Expansion: Joint Statements,* for the specific conditions of each joint statement).

GES will experience substantial growth through increased GE membership and the addition of foreign partners. As part of the procedures for implementing a joint statement and adding foreign partners to GE, CBP and each foreign partner are executing parallel protocols that incorporate privacy protections. 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.

NEXUS

NEXUS, under which NEXUS Air, NEXUS Highway, and NEXUS Marine have been consolidated into a single inspection program, allows members to have crossing privileges at POEs between the United States and Canada. This affords pre-screened travelers expedited processing by U.S. and Canadian officials in dedicated processing lanes at Canadian pre-clearance airports, designated northern border POEs, and marine reporting locations.

NEXUS is a reciprocal program that requires USCs, Lawful Permanent Residents (LPR), Canadian citizens, and Landed Immigrants of Canada (LIC) to enroll with both CBP and the Canada Border Services Agency (CBSA) at joint enrollment centers. CBP permits authorized CBSA agents at these joint enrollment centers to have read-only access to GES to facilitate the vetting of those U.S. citizens and LPRs who apply for NEXUS membership. During the NEXUS enrollment process, CBP collects fingerprints from applicants and CBSA collects iris scans in accordance with its border authority. Iris scans collected at the kiosks are not used or collected by CBP; they are strictly used by CBSA, which matches kiosk iris scans to those it collects at enrollment for identity verification purposes and determining expedited entry into Canada. All individuals accepted into NEXUS are issued photo identification and a proximity RFID card. Participants traveling by air would use their NEXUS card at a NEXUS kiosk, where they would provide either an iris or fingerprint for biometric verification. The expedited clearance processes may entail additional steps at the kiosk for travelers with a nonimmigrant visa or arriving under the Visa Waiver Program. These travelers will have additional screens to complete at the kiosk to determine the class of admission and period of stay for the traveler, as well as printing the appropriate admission document.

NEXUS travelers crossing by land will need to have their RFID-enabled NEXUS card in their possession to utilize the designated lanes for expedited processing. NEXUS travelers arriving by vessel

in the marine environment can utilize their NEXUS card in lieu of a passport and may receive clearance without the requirement of an in-person interview.

Secure Electronic Network for Travelers Rapid Inspection

SENTRI members have the benefit of access to dedicated primary lanes that allow expedited entry at designated U.S. southern border POEs from Mexico. As with other trusted traveler programs, SENTRI applicants must voluntarily undergo a thorough biographical background check against criminal, law enforcement, customs, immigration, and terrorist indices; a 10-fingerprint law enforcement check; and a personal interview with a CBP officer. Individuals accepted into SENTRI are issued a RFID card, which must be carried every time that individual passes through a dedicated primary lane. SENTRI members are also issued a sticker decal, which must be applied to the individual's vehicle or motorcycle that will be driven through a dedicated vehicle primary lane.

SENTRI members have the benefit of shorter wait times when passing through a dedicated primary lane. Information required in the inspection process is provided to the CBP officer upon the individual's arrival at the POE and the information is screened prior to his or her arrival at the primary inspection booth, thus the inspection time is reduced from an average of 30-40 seconds to an average of 10 seconds because the officer only needs to verify SENTRI membership of the travelers and that their vehicle has been registered.

Free and Secure Trade

FAST allows members to enter the United States by land or sea; it also affords expedited release to approved commercial truck drivers who make fully qualified FAST trips between the United States and Canada, FAST trips to the United States from Mexico, or FAST trips from Mexico through the United States to Canada. The data collection for FAST differs slightly due to the commercial nature of the program. In addition to the requirement for the commercial truck driver to be vetted, the company and cargo is also vetted. Expedited clearance through FAST can only be granted if every person in the vehicle is in possession of a valid FAST commercial driver card and is transporting eligible goods for a FAST-approved carrier and importer.

Global Online Enrollment System

GOES, previously an optional online application process, is now the standard application process for almost all trusted traveler programs and certain registered traveler programs. SENTRI is the only program for which both electronic and paper applications (SENTRI Application, CBP Form 823S) are accepted. GOES enables existing and prospective members of all trusted traveler programs to apply for and check the status of their enrollment online via a secure web site. GOES has also been streamlined to make the application process for trusted traveler programs easier and more efficient for applicants and to improve administrative oversight.

Easier Application Process for Certain Trusted Traveler Programs

New NEXUS members and new USC and LPR SENTRI members automatically receive the benefit of using the GE kiosks for expedited clearance upon arrival, provided that all required documents

for GE are on file in GES. Current NEXUS members and U.S. citizen and LPR SENTRI members who have their fingerprints and the required travel documents registered in GES have also been extended these GE benefits. NEXUS or SENTRI members whose information in GES is incomplete may obtain GE benefits by providing ten fingerprints and/or travel document information, as appropriate, at an enrollment center. Non-LPR SENTRI members who are Mexican nationals can apply for GE benefits at no additional fee, but they will need to submit a GE application and pass a thorough risk assessment conducted by CBP and the Mexican government before receiving full GE benefits.

Standard Application Process for Trusted Traveler Programs

An individual that wishes to apply for any of the trusted traveler programs, including applicants from GE-participating countries, must do so through GOES. Individuals may access GOES by visiting the CBP website[9] and reviewing their particular program of interest (GE, NEXUS, SENTRI, FAST). To initiate the application process, the individual must provide an email address so that he or she may set up a GOES user ID and password. In addition, the individual will be asked to provide answers to a set of security questions, which may be used later to verify the individual's identity prior to accessing GOES in the event he or she has forgotten or misplaced his or her user ID, password, or both. GOES registration also allows for notification to the individual via email when new information regarding the individual's application or enrollment status is available.

Once an individual is registered in GOES, he or she may choose a particular program—GE, NEXUS, SENTRI, or FAST—and enter all data required. Upon completion of the application, GOES directs all applicants to a Pay.gov webpage to pay the application fee. GOES forwards the applicant name and a tracking number to the DHS/CBP-003 Credit/Debit Card Data System (CDCDS) System of Records for payment reconciliation. Pay.gov sends a nightly activity file, including the last four digits of the credit card, authorization number, billing name, billing address, tracking number, and Pay.gov tracking numbers, to CDCDS. Pay.gov also sends a daily batch file with the necessary payment information to a commercial bank for settlement processing. After processing, the commercial bank sends a settlement file, including the full credit card number, authorization number, card type, transaction date, amount, and tracking number to CDCDS. Pay.gov provides CBP the tracking number and the amount paid.[10] Once GOES receives confirmation from Pay.gov that the payment has been processed successfully, GOES will retain the Pay.gov tracking number for payment reconciliation purposes. No credit card information will be collected or maintained by GOES.

Trusted traveler programs offer a renewable five-year membership. If a current member of any of the GES programs wishes to renew his or her application or apply for a different program, the option to renew becomes available up to a year in advance of the membership expiration date. The member

[9] GOES may be accessed at https://goes-app.cbp.dhs.gov/main/goes.
[10] For more information about the collection of application fees, see DHS/CBP-003 Credit/Debit Card Data System (CDCDS) System of Records, 76 Fed. Reg. 67755 (Nov. 2, 2011). For more information about authorized electronic mechanisms for payments to the Federal government, including Pay.gov, see "TREASURY/FMS .017, Collections Records--Treasury/FMS," in Treasury Dept., Funds Management Div., Financial Management Service, Notice of Systems of Records, 77 Fed. Reg. 62602, 62616 -62618 (Oct. 15, 2012).

provides his or her membership identification number to retrieve application data from GES to initiate the renewal process. Renewal applications follow the same process as initial applications in GOES and GES.

Throughout the application process, GOES will provide the applicant with status and further instructions to finalize his or her enrollment. At the end of the online application process, GOES displays an application summary page that displays the application information recorded in the system. The applicant can click "Back to Application Wizard" link to correct information. Some screens automatically populate personal information fields with application information already recorded in the system; if the information is incorrect, the applicant may use the "Update Registration Data" hyperlink to change the information. The applicant will receive instructions on setting up interviews, as well as approval and denial letters, through GOES.

Through a review of biographic application data in GES, biometric information in IDENT, and the comparison of this information with other law enforcement databases, CBP officers determine the relative risk of the applicant and record whether or not the applicant should be approved into the trusted traveler program.

Members of trusted traveler programs may submit updates to their names, addresses, or employment either online in GOES, or by visiting their nearest Global Entry, NEXUS, or SENTRI enrollment center to notify them of the change.

Registered Traveler Programs

CBP offers expedited border crossing for travelers into the United States through its registered traveler programs, which include SVRS and DTOPS. Like the trusted traveler programs, registered traveler programs allow individuals to provide their information to CBP ahead of time to allow CBP to stage the information for processing in advance of the border crossing. Whereas trusted traveler programs grant approved members expedited processing based upon their having cleared a vetting process, registered traveler programs merely keep individuals' information on file so that they may receive faster clearance upon arrival at a POE.

Small Vessel Reporting System and Related Options for Small Vessel Operators

In general, pursuant to 8 C.F.R. § 235.1(a), operators of small pleasure vessels who arrive in the United States from a foreign port or place must apply in person, to a CBP officer, at a POE during its operating hours to enter the country lawfully. CBP offers a few options for pleasure vessel operators that provide an exception to the requirement to report in person; however, the small vessel operators must still report their arrival to CBP. *See* 19 U.S.C. § 1433.

SVRS helps CBP increase compliance with small vessel reporting regulations and to concentrate enforcement resources on high-interest vessels by enabling the operators of pleasure vessels to report their arrival from foreign waters quickly and easily to CBP. Travelers who utilize SVRS may fall into the following categories: (1) Current members of CBP trusted traveler programs, including NEXUS Marine; (2) Travelers who currently hold an I-68 Canadian Border boat landing permit; or (3) Participants of the Local Boater Option (LBO), a pilot program that CBP operates in Miami, FL; Tampa, FL; and San Juan,

Puerto Rico. All SVRS applicants must be interviewed to complete their enrollment. If this has already been accomplished during a trusted traveler program, I-68, or LBO enrollment, it will not need to be repeated for SVRS enrollment.

Small vessel operators that have not enrolled in a trusted traveler program, do not hold an I-68 Canadian Border permit, or do not participate in the LBO program may still enroll in SVRS, but will be required to attend an in-person interview with a CBP officer. Once the application process is complete and the boater is approved, an SVRS number will be issued along with instructions to set up a password for the SVRS website. The password will allow the enrollee to use the SVRS website to add, update, or activate a float plan as required for expedited entry under the program. The application for SVRS is available online at the SVRS website: https://svrs.cbp.dhs.gov/.

Prior to travel, enrollees can submit float plans consisting of biographical information of all persons intending on traveling, vessel registration information, and itinerary information. Once a float plan is entered and activated, SVRS will issue a float plan number, which authorizes the boater to utilize a designated telephone line manned by a CBP officer or an automated attendant upon return to the United States. The CBP officer or automated attendant will ask a series of questions reflecting those on a Customs Declaration (CBP Form 6059B) and provide the participant with an arrival number or refer the participant to a predetermined inspection site for a CBP inspection. In most cases, SVRS participants will not have to report for an in-person inspection upon arrival to the United States.

Decal and Transponder Online Procurement System

DTOPS is a registered traveler program that allows individuals who are registered to a C-TPAT/FAST ID commercial vehicle to cross the U.S. border more easily. Decals or transponders attached to the vehicle identify the individual and allow for faster screening. Through DTOPS, individuals can purchase, renew, or transfer user fees related to the transponders/RFID tags for their commercial vehicles or to the decals for their private aircraft or vessels in advance of crossing a U.S. border. If a transponder/RFID tag or decal has not been purchased in advance, a fee is collected each time a conveyance crosses the border. In addition, an aircraft or vessel user fee application must be completed upon entry. With DTOPS, owners of commercial vehicles, private aircraft, and private vessels over 30 feet in length must pay a yearly fee for such assets to cross the U.S. border. To conveniently satisfy this fee in advance, owners can use the DTOPS website[11] to purchase transponders/RFID tags for commercial vehicles, as well as decals without radio frequency capability for private aircraft or vessels over 30 feet in length.

To purchase a transponder/RFID tag or decal, an applicant must provide an account name and email address, physical address, shipping address, contact name, contact phone number, and contact email address. Conveyance identification information must also be provided, which includes the registered owner name, address, and the C-TPAT/FAST ID of either a company or an individual. To complete the purchase online, electronic bank information or credit card information is collected on the Pay.gov

[11]The DTOPS website is https://dtops.cbp.dhs.gov/.

website. DTOPS forwards the applicant name and a tracking number to the DHS/CBP-003 CDCDS System of Records for payment reconciliation. Pay.gov sends a nightly activity file, including the last four digits of the credit card, authorization number, billing name, billing address, tracking number, and Pay.gov tracking numbers, to CDCDS. Pay.gov also sends a daily batch file with the necessary payment information to a commercial bank for settlement processing. After processing, the commercial bank sends a settlement file, including the full credit card number, authorization number, card type, transaction date, amount, and tracking number to CDCDS. Once DTOPS receives confirmation from Pay.gov that the payment has been processed successfully, DTOPS will retain the Pay.gov tracking number for payment reconciliation purposes. Once registered, owners can use the DTOPS website to order a free replacement transponder, transfer the paid fee to a different vehicle, or pay to renew their registration.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The authority for GES 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 GES 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 GES include 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.

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 C.F.R. 103.7(b)(1)(ii)(M).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The DHS/CBP-002 – GES SORN is being updated and published concurrently with the posting of this PIA. The DHS/USVISIT-004 - DHS Automated Biometric Identification System (IDENT) SORN (72 Fed. Reg. 31080 (Jun. 5, 2007)) also applies to the information collected.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The Authority to Operate for GES was granted on May 28, 2009.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. CBP is proposing to NARA the following retention: All GES 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, abandonment, or as a result of CBP termination. Fingerprints provided to IDENT will be retained in accordance with the IDENT SORN.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected from GES applicants is covered by the Paperwork Reduction Act, and the OMB control number for this collection is 1651-0121. SVRS and DTOPS OMB collection numbers are pending.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Categories of individuals covered by GES include individuals who apply to use any form of automated or other expedited inspection for verifying eligibility to cross the borders into the United States. Persons eligible for the GES-supported trusted traveler programs include USCs, LPRs of the United States, Mexican nationals, and citizens of Canada and other nations participating through joint statements as mentioned in Appendix A. Non-U.S. citizens must have valid entry documents, be admissible to the United States, and demonstrate they are low risk travelers by providing certain documents called for by regulation (e.g., 8 C.F.R. § 235.7) in conjunction with a completed applicable trusted traveler application form for the desired program. Information collected through each of the trusted traveler programs is added into GES and IDENT. GES collects and maintains all enrollment data for trusted traveler program applicants as follows:

Biographic application data may include:

- Full name;

- Alias(es);
- Date of birth;
- Place of birth;
- Language preference;
- Gender;
- Current and former addresses;
- Telephone numbers;
- Country of citizenship;
- Alien registration number (if applicable);
- Employment history (if available);
- PASS ID or Trusted Traveler membership number, GOES user ID,
- Password and answers to security questions (for lost passwords);
- Countries visited in the last five years;
- Criminal history;
- Parental or Legal Guardian permission (if 18 years or younger);
- Driver's license number; and
- Issuing state or province of the applicant's Driver's License.

Vehicle or Vessel information may include, as appropriate:

- 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, VIN number, and license plate number of the vehicle;
- Owner name, gender, and date of birth; and
- Pay.gov tracking number.

Biometric data may include:

- Fingerprints (stored in IDENT);
- Fingerprint Identification Number (FIN);
- Eye color;
- Height; and

- Facial photographs.

While trusted traveler applicants provide digital photographs and fingerprints, GES maintains only the applicants' facial photographs. The fingerprint data is maintained in IDENT.[12] Fingerprint information will be designated as GES data in the IDENT database in order to be easily distinguishable from non-GES data stored in IDENT. This designation will allow CBP to limit access in accordance with mission responsibilities.

GES also maintains vetting results with corresponding law enforcement database record numbers used to support the membership decision. The review of biographic application data in GES and biometric information in IDENT, and the comparison of this information with other law enforcement databases, permit a CBP officer to determine the relative risk level of the applicant and record whether or not the applicant is admitted into the trusted traveler program.

All trusted traveler programs require fingerprints for initial vetting at enrollment, but they do not all require fingerprints to validate identity at each entry. SENTRI, FAST, and NEXUS Highway employ RFID cards that provide the CBP officer with identity information, including a digital photograph collected during the enrollment process, which expedites clearance. Only the air environment utilizes biometrics through the kiosks to validate identity.

Registered traveler programs do not conduct the same type of vetting as the trusted traveler programs. SVRS collects the following information:

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

[12] IDENT maintains fingerprints used for initial vetting of applicants and for corroborating fingerprints from each border crossing (referred to as an "encounter") once a trusted traveler is enrolled. IDENT will also maintain limited biographic information (name and birth date), which will be used to identify those fingerprints. As part of the GES application process, the fingerprints are sent to the FBI for vetting purposes to check against law enforcement databases, but are not maintained by the FBI. A traveler who crosses the border at a POE provides fingerprints, typically at an automated machine, to verify that he/she is the same individual who was initially approved as a trusted traveler and enrolled in the program. IDENT maintains a record of every encounter during which an individual's fingerprints are submitted and compared with enrollment fingerprints already stored in the system. The record includes limited biographic data; the fingerprints; and the date, time, and location of where the fingerprints were collected. Fingerprints provided to IDENT will be retained in accordance with the IDENT SORN. See DHS/USVISIT-0012- IDENT System of Records, 72 Fed. Reg. 31080 (Jun. 5, 2007)

- Contact email address;
- Password;
- Document type & number (*e.g.,* U.S. Passport, Permanent Resident Card, Birth Certificate etc.), 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, etc.).

DTOPS collects the following information:

- Account name;
- Physical address;
- Shipping address;
- Pay.gov tracking number;
- Contact name;
- Contact telephone number; and
- Contact email address.

In addition, the specific information collected and retained when ordering decals, transponders, or both, includes conveyance information and payment information. Payment information is supplied by the user, but not retained within DTOPS. DTOPS receives a code from Pay.gov indicating either success or failure of the payment, at which time the shipment of the decal or transponder will be initiated. For registering vehicles, if the commercial carrier is C-TPAT/FAST approved, then the FAST ID is collected. If the owner is C-TPAT/FAST approved, then the owner's FAST ID is also collected. If the owner is not C-TPAT/FAST approved, then the owner must supply their name, address, city, state/province code, zip/postal code, and country code. Information about the conveyance itself includes model year, manufacturer name, and conveyance ID information specific to the type of conveyance. For aircraft, the tail number is collected. For vessels, the vessel name, and at least one of the US Coast Guard ID number, local registration number, or hull ID number is collected. For commercial vehicles, the Vehicle Identification Number (VIN), transponder ID, vehicle color, primary license plate number, country code, and state/province code are supplied.

2.2 What are the sources of the information and how is the information collected for the project?

All application information in GES is collected from the individual, sometimes via an electronic device. Biographic information in GES is collected from the GOES application fields completed by the individual. At the enrollment center, photographic facial images will be collected by digital cameras and fingerprints will be captured with scanning devices. For GE enrollees entering the United States, information will be collected at kiosks to verify identity. The kiosk prompts travelers to slide their

passport into a reader, look into a camera for a facial photo, and press their fingertips to the scanner for fingerprint capture.

Vetting results stored in GES are based on checks of external law enforcement systems. The main database checked during the vetting process, before individuals will be enrolled in any trusted traveler program, is TECS, which contains historical and enforcement data on travelers, and provides a gateway to other sources of data. These other 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 National Law Enforcement Telecommunication System, and Department of State (DOS) 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.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No commercial data is used as a source of information for GES.

2.4 Discuss how accuracy of the data is ensured.

The initial application data is submitted by the applicant online through GOES and is checked during the vetting process by CBP Officers who check multiple law enforcement databases. The data is verified again during the enrollment phase when the CBP Officer interviews the applicant to verify the submitted application data and travel documents.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that inaccurate application data may result in an erroneous decision to offer or deny enrollment in a trusted traveler program.

Mitigation: This risk is mitigated by the personal interview that is required for all trusted traveler program applicants. If there are doubts as to whether an individual applying for the trusted traveler program is the same individual of record in a law enforcement database, or if that law enforcement database record's accuracy is questionable, CBP will use the personal interview, the complete application data, or offer the applicant an opportunity to reapply and clarify the potential inaccuracy to determine the validity and relevancy of the data.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

Information is being collected from voluntary applicants in order to assess their eligibility for enrollment in a GES-supported trusted traveler program. Trusted traveler biographic information is checked daily for wants or warrants to ensure the individual is eligible for expedited processing at the border. Registered traveler programs do not use the data to accept or deny individuals into the program, but merely to provide advanced submission to CBP for expedited processing at the border. Data collected in the application process is data that CBP Officers often already routinely encounter and use for official law enforcement and admissibility purposes as provided for by their unique border security and search authority. By collecting and processing this passenger data in advance of travel, CBP seeks to offer expedited service for those travelers who elect to volunteer and are otherwise eligible to participate.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. GES does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

US-VISIT, as steward of IDENT, has an assigned role in the application process for GES. Of the biometric data collected at enrollment, the applicant's ten fingerprints are submitted to IDENT for the purpose of checking for any immigration related records on the applicant. However, the results of the background check, as well as any matching information and the final determination on membership (Accepted or Denied) is stored in GES, exclusively.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that applicants and enrollees may not know how their information will be used by GES, particularly for international partnerships.

Mitigation: This risk is mitigated by the publication of this PIA and the corresponding SORN, which provide transparency as to the uses of GES. For GE, the Global Entry Information Guide is available for download on the Global Entry website at http://www.globalentry.gov/downloads.html. Also, the Frequently Asked Questions page at http://www.globalentry.gov/faq.html explains that CBP uses the information collected during enrollment to make sure each individual meets program eligibility

requirements. With the exception of CBSA for NEXUS, foreign partnering agencies do not have system access to GES. CBP has only granted authorized CBSA officers with read-only access to GES at joint enrollment centers to facilitate NEXUS enrollment, which does not allow for manipulation of the data or electronic dissemination.

Privacy Risk: There is a risk that information used to enroll individuals in a registered or trusted traveler program will be used for a purpose inconsistent with the original collection.

Mitigation: This risk is mitigated by the manner in which information is collected and stored for trusted and registered traveler programs. All system users are trained to use information strictly for determining program eligibility. For both GES and IDENT, access is granted to users by a limited number of system administrators and access level varies based on need-to-know and function of the user.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Notice is provided in the form of this PIA and the corresponding SORN for GES. Additionally, individuals are asked to certify a Privacy Act statement on the GOES website notifying applicants of the information collection required for program consideration. For GE, an Information Guide describing the collection can be found on the GE Downloads page at http://www.globalentry.gov/downloads.html. Frequently Asked Questions are also available at http://www.globalentry.gov/faq.html.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Participation in a trusted or registered traveler program is voluntary, so consent is implied when an applicant applies to the program. As part of the GOES application, applicants must certify that they understand any information they provide, including any supporting documentation, biometric data, and statements made during interviews, may be shared among law enforcement and other government agencies as necessary to conduct a background investigation. As explained in this PIA, the collected data in GES is used only for the purposes defined, including border and immigration management, national security, and law enforcement. Once enrolled, individuals have no opportunity to "opt out" of the use of their data for any of these stated purposes.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals participating in or applying for a GES program may not feel they received adequate notice as to the use of their collected information.

Mitigation: This risk is mitigated by the Privacy Act notice required to be certified by the applicant in GOES and the paper SENTRI form. This notice explains that GES application information, including supporting documentation, background information, finger and biometric data will be subject to a check of criminal information databases, immigration and customs databases, and other enforcement databases, as well as shared among law enforcement and other government agencies as permitted under the Privacy Act and other applicable laws. This notice further reminds applicants of the opportunity to decline to provide information for the application and that the programs are all voluntary.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

All GES data is retained for three years after an individual's membership is no longer active, whether due to expiration without renewal at the end of five years, abandonment, or CBP termination. Data is not deleted immediately after membership becomes inactive so that CBP can more easily vet an individual who chooses to reapply, as well as to provide a record for redress purposes. Fingerprints are retained in IDENT pursuant to the IDENT SORN, DHS/USVIST-0012 – IDENT SORN (72 Fed. Reg. 31080 (Jun. 5, 2007)).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that data might be retained unnecessarily for individuals who apply for membership to a GES program but never actually become members.

Mitigation: Once payment is processed by GOES, all applicant data will reside in GES, but this risk is mitigated by deleting all GES data on all denied applicants after three years. Applicant information is only retained if payment is processed. Fingerprints provided to IDENT will be retained in accordance with the IDENT SORN.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Fingerprints obtained during the enrollment process are maintained in IDENT. During the background check process these biometric records are checked against the FBI's criminal database, the Integrated Automated Fingerprint Identification System (IAFIS). These fingerprints are not stored by the FBI.

The only GES information shared with partnering international countries is trusted traveler application information (excluding vehicle-related information) submitted directly by the applicant, listed in Section 2.1 above, that is required for vetting. No derogatory information or records are exchanged; CBP only provides a "pass/fail" decision to the partnering international country and receives only a pass/fail for reciprocal programs.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Routine use B of the SORN for GES allows CBP to share fingerprints with the FBI to conduct a background check against its criminal database. Determining whether or not a GES applicant has a criminal history on record with the FBI is a necessary part of CBP's evaluation of that individual's risk level.

Sharing GES information with partnering international countries is compatible with Routine use A of the SORN, which allows for disclosure to foreign government agencies to elicit information necessary to make decisions on applications. In CBP's reciprocal joint statements, sharing biographic GE application data and vetting results in the form of a "pass/fail" transmission of U.S. citizens with these foreign governments is conditioned upon receiving the same type of data from those governments on their citizens who are applying for expedited entry into the U.S. Because of these international information sharing relationships, CBP is able to make well-informed decisions on GE applications of citizens from a growing number of countries.

6.3 Does the project place limitations on re-dissemination?

Re-dissemination of GES information by external agencies is prohibited.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

External sharing of GES data in response to a one-time request is documented on the DHS Form-191 (Accounting for Disclosure), a paper form, which notes the name of the individual whose records are requested, the system that the records are taken from, the nature of the disclosure, and the name of the requestor. System to system disclosures are documented electronically, including record number, date/time stamp and receiving system.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that GES information may be inappropriately shared with individuals or foreign countries and that these countries would have limited accountability for how they can use and further share this data.

Mitigation: CBP only shares GES application data as authorized by the GES SORN and as defined in a MOU. For information about the joint statements, see Appendix A. Access controls such as administrative passwords and restrictive rules regarding database access ensure that only authorized users can access GES and use the information in the system in accordance with information sharing agreements.

The CBSA, which has read-only access to GES for the purpose of vetting NEXUS applicants, has agreed to uphold the privacy and confidentiality terms of an MOU with CBP specifying that each participant agrees to not disclose any information obtained to third parties without first obtaining written permission from the other. Furthermore, CBP GES supervisors can only provide CBSA officers with read-only access to GES once they have passed CBP's TECS Privacy Awareness training. For CBSA's Privacy Statement related to NEXUS information sharing, see http://www.cbsa-asfc.gc.ca/prog/nexus/privacy-privee-eng.html. For information on privacy risk mitigation for CBP's other international partners receiving GES data, see Appendix A.

As part of the procedures for implementing a joint statement and adding foreign partners to GE, CBP and each foreign partner are executing parallel protocols that incorporate privacy protections. 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.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

To gain access to GES information, an enrollee may request information about his records contained in GES and IDENT through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)) by writing to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
799 9th Street NW
Washington, DC 20229

When seeking records from GES or any other CBP system of records, the request must conform to Part 5, Title 6 of the Code of Federal Regulations. *See* 6 C.F.R. Part 5. An individual must provide his or her full name, current address, and date and place of birth. He or she must also provide:

- An explanation of why the individual believes DHS would have information on him or her;
- Details outlining when he or she believes the records would have been created; and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this information, CBP may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

During the registration and application process, the registered traveler programs, and GOES provide a summary of the information in the system, so that the submitter can edit incorrect information prior to sending the registration or application information. Members of trusted traveler programs may submit updates to their names, addresses, or employment either online in GOES, or by visiting their nearest Global Entry, NEXUS, or SENTRI enrollment center to notify them of the change.

Individuals who think the decision to deny membership in GE was based on inaccurate information may contact a GE enrollment center to discuss the denial. A list of enrollment center locations can be found at http://www.globalentry.gov. Individuals may also write to the CBP Trusted

Traveler Ombudsman by email at Cbp.cbpvc@dhs.gov or by mail at the following address: U.S. Customs and Border Protection, P.O. Box 946, Williston, VT 05495, Attention: CBP Ombudsman. CBP will respond in writing to each inquiry, providing one of the following specific reasons for denial when possible: (1) applicant is inadmissible into the United States under applicable immigration laws; (2) applicant is in violation of customs or immigration laws, regulations, or other related laws; (3) applicant has been convicted or arrested for a criminal offense; (4) information provided in application has been found to be false, inaccurate, or incomplete; (5) applicant is not a citizen or permanent resident of the United States; or (6) applicant does not meet the program eligibility requirements for other reasons (e.g., applicant is under investigation or has been denied based on interview).

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are advised of the procedures for correcting their information on the respective website for each trusted traveler and registered traveler program. On the GE website, notice is provided under the "Denial Inquiries" link on the "Contact Us" page: http://www.globalentry.gov/denialinquiries.html/. Also, GE denial letters instruct applicants to contact their local enrollment center with questions regarding their denial. The GOES website, used for all trusted traveler applications, provides notice for information correction procedures under "Application Status Questions" on its Frequently Asked Questions page at https://goes-app.cbp.dhs.gov/common/FAQ.html#faq_status_3.

GE members who are denied NEXUS benefits by the CBSA can find information on redress options and request a review at the CBSA website, http://www.cbsa-asfc.gc.ca/recourse-recours/menu-eng.html. For information on redress procedures made available by CBP's other international partners receiving GES data, see Appendix A.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know that their denial was based upon erroneous information.

Mitigation: This risk is mitigated by the denial letter that lists the name and address of the applicant and a clear and concise statement of why the application was denied. For example, if the denial is due to criminal conviction or arrest, the type of offense, year, and state in which the incident occurred will be revealed. Individuals denied membership to a foreign trusted traveler program may seek redress through that program. See Appendix A.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

GES is protected through a multi-layer security approach. The protective strategies are physical, technical, administrative, and environmental in nature and provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

All GES access and activities are monitored by security and application logs, and regular audits are conducted according to the CBP audit and accountability policy and procedures as stated in the CBP Information Systems Security Policy and Procedures Handbook to ensure compliance. CBP employees found to have engaged in unauthorized access to CBP systems are subject to disciplinary action that could result in criminal penalties or dismissal.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All CBP personnel with user access to GES must complete the DHS Security Awareness Training Course which includes privacy training. Additionally, all CBP users must keep their TECS access up to date, which requires completion of the TECS Privacy Awareness (TPA) course every two years.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The user base for GES is CBP officers trained in the input of biographic information from travelers, the correct capture and storage of their biometric information, and in traveler vetting processes. They will access the system through CBP-standard workstations, with appropriate peripheral equipment, and the operation of the system will take place solely within CBP controlled space at designated Ports of Entry and the CBP Risk Assessment Center.

All users are assigned a role within GES. There are basic user roles (e.g., CBP Officer, CBP Risk Assessor, and CBSA Officer), supervisory user roles (e.g., supervisor and risk assessor supervisor) and support roles for OFO HQ, such as for running reports. The privileged user roles are the supervisory roles. These roles have the ability to create the basic user roles for CBP Officers at the POE.

Internal GES users are generally required to be US citizens who have successfully completed a

background investigation or equivalent, except for Canadian officers from the CBSA who have special GES user roles at the joint Enrollment Centers supporting the NEXUS Trusted Traveler Program. These CBSA users must have DHS Exception to Citizenship Request Forms approved before they can be granted GES access. CBSA officers only have read-only access. They do not have access to view hit records or attachments in GES. No other international partner has access to GES.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

CBP negotiates international arrangements with foreign government border authorities that are informal and non-binding. These arrangements are reviewed by CBP counsel and the proper channels.

Responsible Officials

Laurence Castelli, CBP Privacy Officer
U. S. Customs and Border Protection

Cheryl Peters, Program Manager
Office of Field Operations
U.S. Customs and Border Protection

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

APPENDIX A

CBP Global Entry Expansion: Joint Statements

Statement

Foreign partners may be added to Global Entry (GE) through joint statements between the United States and a foreign country, and the procedures for implementing joint statements may be reciprocal. The overall goal of the joint statement and its implementing procedures is to offer U.S. citizens and citizens of certain foreign countries expedited clearance and admission at their respective airports. As part of the procedures for implementing a joint statement and adding foreign partners to GE, CBP and each foreign partner are executing parallel protocols that incorporate privacy protections. 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.

CBP will update this PIA and amend Appendix A when foreign partners join GE, or when a partnership with a foreign entity changes. CBP has signed general joint statements with Australia, Israel, New Zealand, Panama, and Qatar. In addition, CBP is in the process of implementing the Asia-Pacific Economic Cooperation (APEC) Business Travel Card (ABTC) as part of GE, pursuant to the Asia-Pacific Economic Cooperation Business Travel Cards Act of 2011. Asia-Pacific Economic Cooperation Business Travel Cards Act of 2011, 112. Pub. L. 54, 125 Stat. 550 (Nov. 12, 2011), 8 U.S.C. § 1185 note. CBP will update this PIA and amend Appendix A after CBP executes parallel protocols, which incorporate privacy protections, and an Interconnection Security Agreement with each foreign partner, as applicable.

Joint Statements

The Netherlands: Fast Low Risk Universal Crossing (FLUX)

Participating Countries:

United States, the Netherlands

Eligibility:

GE (United States trusted traveler program) members; Privium (the Netherlands trusted traveler programs) members

Overview:

Fast Low Risk Universal Crossing (FLUX) is a permanent program that operates under an international bilateral agreement between the United States and the Netherlands. In this reciprocal

arrangement, GE members may apply for Privium, the Netherlands trusted traveler programs, to facilitate their entry to the Netherlands. Likewise, citizens of the Netherlands enrolled in Privium may apply for GE to facilitate their entry to the United States.

Application Process and Data Collection:

GE members may apply for Privium through the Dutch web portal. GE members must provide their PII directly to, and have their Privium applications reviewed by, the Netherlands Royal Marechaussee and pay a separate Privium membership fee.

Citizens of the Netherlands enrolled in Privium may apply for GE by completing an application only through the Dutch web portal. Once a Dutch citizen indicates he/she is an active Privium member, GE will automatically categorize him/her under FLUX. All Privium applicants are subject to comprehensive government background checks by both countries' law enforcement authorities, including checks of immigration and customs databases, collection of fingerprints, and interviews by both CBP officers and Royal Marechaussee officers at designated enrollment centers.

Membership Fees and Requirements:

Applicants must maintain membership in good standing in their home country's trusted traveler program at all times. This requires that as soon as a membership is cancelled or revoked by one country, the other country will be notified immediately so that appropriate actions, including the revocation of FLUX Alliance benefits.

Information Sharing:

The only GES information CBP shares with the Netherlands Royal Marechaussee is the biographic data submitted by the applicant that is used to conduct its own vetting on GE members applying for FLUX benefits. No vetting records or law enforcement records are shared. In its vetting process, the Royal Marechaussee uses the biographic data it receives from the applicant through GES to consult with various law enforcement/immigration systems, including: the National Schengen Information System, the National Index of Wanted Persons, the Criminal Records System, the Basic Register/Aliens Register, the Register of persons not entitled to a passport, and the National Documents System.

The joint statement signed between the United States and the Netherlands does not alter existing privacy protections. The United States collects, uses, retains, and disseminates all data submitted to GES in accordance with the GES SORN and this PIA, and U.S. law. The Netherlands collects, uses, retains, and disseminates data, which it receives from an applicant via GES, in a manner that is consistent with applicable domestic laws and policies. Limited information on retention of application data by the Dutch can be found on the FLUX Frequently Asked Questions page, https://www.flux-alliance.eu/frequently_asked_questions/. This PIA will be updated to describe the parallel protocols that incorporate privacy protections.

Correction and Redress:

GE members who are denied FLUX Alliance benefits are notified electronically by their GOES account. This denial notification informs the applicant that any questions or complaints about the outcome should be submitted in writing to the Netherlands Royal Marechaussee at the address provided. The current Joint Statement signed by the U.S. and the Netherlands does not specify a process for correction and redress offered by the Netherlands, but it stipulates that each country will collect, use and maintain applicant data in a manner consistent with applicable domestic laws and policies.

Citizens of the Netherlands who are denied GE benefits are notified electronically by their GOES account. If they feel there was erroneous information or errors in the application process they can follow the procedures described in Section 7.0 of this PIA.

Access and Security:

In a Joint Statement signed with CBP, the Netherlands has agreed to collect, use, and maintain the data it receives from GES in a manner consistent with its applicable domestic laws and policies. This would include any applicable laws on data security. The Royal Marechaussee receives GES data through an encrypted web service connection. At this time, there is no Interconnection Security Agreement in place with the Netherlands covering this connection.

The Republic of Korea: Smart Entry Service (SES)

Participating Countries:

United States, the Republic of Korea (ROK)

Eligibility:

GE (U.S. trusted traveler program) members; SES (the ROK trusted traveler program) members

Overview:

SES is a trusted traveler program operated by the government of the ROK. SES provides expedited processing for pre-approved, low-risk travelers at designated airports in the ROK via the use of e-gates. CBP has partnered with the ROK Immigration Service (ROKIS) to link SES with GE. U.S. citizens, who are already GE members, may apply to SES; ROK citizens, who are already SES members, may apply to GE.

Application Process and Data Collection:

U.S. citizens, who are GE members and choose to apply to SES, apply through their GOES accounts. The application is sent to the ROKIS for review. Once the U.S. citizen GE members are "conditionally approved" in SES, they must visit an enrollment center in ROK within six months to complete enrollment in SES.

ROK citizens, who are SES members, can apply for GE through the Korean portal. The application is submitted electronically to ROKIS. ROKIS will then send a copy of the applicant data to CBP for vetting. If the applicant passes CBP checks, the application is conditionally approved and the member is invited for an interview. Notifications are made via the GOES account.

Membership Fees and Requirements:

Applicants must maintain membership in good standing in their home country's trusted traveler program at all times. This requires that as soon as a membership is cancelled or revoked by one country, the other country will be notified immediately so that the country may take appropriate actions. SES applicants must pay U.S. $100 application fee at the time of their interview in the ROK.

Information Sharing:

The only GES information CBP shares with the ROKIS is the biographic data submitted by the applicant that CBP used to conduct its own vetting of GE members, who choose to apply for SES. CBP does not share vetting records or law enforcement records. In its vetting process, the ROKIS uses the biographic data it receives from the applicant through GES to consult with various ROK law enforcement and immigration systems.

The joint statement signed between the United States and the ROK does not alter existing privacy protections. The United States collects, uses, retains, and disseminates all data submitted to GES in accordance with the GES SORN and this PIA, and U.S. law. The ROK collects, uses, retains, and disseminates data, which it receives from an applicant via GES, in a manner that is consistent with applicable domestic laws and policies. This PIA will be updated to describe the parallel protocols that incorporate privacy protections.

Correction and Redress:

GE members who are denied SES benefits are notified electronically by their GOES account. This denial notification informs the applicant that any questions or complaints about the outcome should be submitted in writing to the ROKIS at the address provided. The current Joint Statement signed by the U.S. and the ROKIS does not specify a process for correction and redress offered by the ROKIS, but it stipulates that each country will collect, use and maintain applicant data in a manner consistent with applicable domestic laws and policies.

ROK citizens who are denied GE benefits are notified electronically via their GOES accounts. If they feel there was erroneous information or errors in the application process they can follow the procedures described in Section 7.0 of this PIA.

Access and Security:

In a Joint Statement signed with CBP, the ROK has agreed to collect, use, and maintain the data it receives from GES in a manner consistent with its applicable domestic laws and policies. This would include any applicable laws on data security. The ROKIS receives GES data through an encrypted web service connection. There is an Authority to Test interim agreement in place with the ROKIS covering this connection.

United Kingdom: International Expedited Travellers (IET) Initiative

Participating Countries:

United States, United Kingdom

Eligibility:

UK citizens by invitation only

Overview:

CBP has signed a Joint Statement with the United Kingdom Home Office and the United Kingdom Border Agency of Great Britain and Northern Ireland (UKBA) regarding the intention to offer GE expedited processing for British trusted travelers through the International Expedited Travellers (IET) Initiative. IET is currently underway as a pilot program and is not a fully reciprocal agreement allowing for expedited entry into the UK for U.S. citizens.

Application Process and Data Collection:

Approximately 1,000 British citizens who frequently travel to the United States have been selected by the airlines and the U.S. Embassy in London to receive letters inviting them to apply for participation in the IET pilot. CBP will provide promotional codes to the airlines to allow invited applicants to complete an online CBP GE application through GOES. This application will include all necessary information fields that the United States requires for enrollment and threat assessment of an applicant. CBP does not share any GES information with the UK. When GOES conditionally approves a British IET applicant, the applicant will be instructed to obtain a certificate from the British government stating that they have vetted the applicant and the applicant passed. A CBP officer at the Enrollment Center will ask the IET applicant to present this certificate at his or her interview. The certificate will then be scanned into GES and used as part of CBP's own vetting of the applicant.

Throughout the application process, GOES will provide the IET GE applicant with status and further instructions to finalize their enrollment. Applicants using GOES will receive instructions, such as setting up interviews, and approval and denial letters through GOES.

Membership Fees and Requirements:

All UK applicants will pay the $100 (U.S.) non-refundable fee to CBP online prior to submitting their application.

Information Sharing:

CBP does not share any GES data with the UK.

Correction and Redress:

IET applicants who are denied GE benefits are notified electronically by their GOES account, and if they feel there was erroneous information or errors in the application process, they can follow the procedures described in Section 7.0 of this PIA. The UK does not offer separate redress for IET denials

apart from that offered by CBP as it does not collect GES data.

Access and Security:

At this time, CBP does not share GES information with the U.K. Data in GES on IET applicants and participants is subject to the auditing and accountability provisions in Section 8.0 of this PIA.

Germany: Global Entry/ABG

Participating Countries:

United States, Germany

Eligibility:

German citizens by invitation only

Overview:

CBP has signed a joint statement with the German border authority to allow select German citizens to apply for GE through the Global Entry/ABG program. Global Entry/ABG is currently underway as a pilot program and is not a fully reciprocal agreement allowing for expedited entry into Germany for U.S. citizens.

Application Process and Data Collection:

CBP will provide promotional codes to Lufthansa airlines to allow invited applicants to complete an online CBP GE application through GOES. This application will include all necessary information fields that the United States requires for enrollment and threat assessment of an applicant. CBP does not share any GES information with the German government. When GOES conditionally approves a German applicant, he will be instructed to obtain a certificate from the German government stating that they have vetted the applicant and the applicant passed. A CBP officer at the enrollment center will ask the German applicant to present this certificate at his or her interview. The certificate will then be scanned into GES and used as part of CBP's own vetting of the applicant.

Membership Fees and Requirements:

All German applicants will pay the $100 (U.S.) non-refundable fee to CBP online prior to submitting their application.

Information Sharing:

CBP does not share any GES data with Germany.

Correction and Redress:

German applicants who are denied GE benefits are notified electronically by their GOES account, and if they feel there was erroneous information or errors in the application process, they can follow the procedures described in Section 7.0 of this PIA. Germany does not offer separate redress for Global Entry/ABG denials apart from that offered by CBP as it does not collect GES data.

Access and Security:

At this time, CBP does not share GES information with Germany. Data in GES on German applicants and participants is subject to the auditing and accountability provisions in Section 8.0 of this PIA.