Privacy Impact Assessment Update
for the

Global Enrollment System (GES):

Trusted Traveler Program (TTP) System

DHS/CBP/PIA-002(d)

August 15, 2017

Contact Point
Cheryl C. Peters
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1707

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the Global Enrollment System (GES), an information technology (IT) system that facilitates enrollment and security vetting for CBP's voluntary Trusted Traveler, Registered Traveler, and Trusted Worker Programs. Program participants volunteer to provide personally identifiable information (PII) and consent to CBP security vetting in return for expedited processing at designated U.S. Ports of Entry (POE) or for access to sensitive CBP-controlled areas or positions. CBP is updating this Privacy Impact Assessment (PIA) to document changes related to GES, including: (1) the introduction of the cloud-based Trusted Traveler Program (TTP) System for online application to CBP programs; and (2) the use of the General Services Administration (GSA) Login.gov portal for identity authentication.

Overview

The GES allows CBP to facilitate the enrollment and vetting processes for Trusted Traveler, Registered Traveler, and Trusted Worker Programs[1] in a centralized environment. Enrollment in these programs enables CBP to expedite the inspection and security vetting process for low-risk travelers and workers, allowing CBP to focus vetting resources toward providing additional scrutiny to individuals who present an unknown risk. Low-risk travelers are directed to dedicated lanes and kiosks at airports for expedited processing resulting from CBP's pre-approval activities. This expedited processing of low-risk travelers and workers concurrently allows CBP officers additional time to focus on higher risk and unknown individuals.

The previously published GES PIA and subsequent updates[2] describe the GES and CBP's Trusted Traveler Programs, which include: Global Entry (GE), NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), Free and Secure Trade for commercial vehicles (FAST),[3] and the U.S. Asia-Pacific Economic Cooperation (APEC)[4] Business Travel Card Program (ABTC).[5] The PIAs also detail the now fully operational Small Vessel Reporting System (SVRS) Registered Traveler Pilot Program and the Decal and Transponder Online

[1] Trusted Traveler/Worker and Registered Traveler Programs typically require the same or similar types of PII to be submitted by an individual; the difference between these programs is the level and frequency of vetting and screening conducted on individuals who apply to participate. For example, Trusted Traveler/Worker Programs require recurrent vetting of individuals for the full duration of the benefit, while Registered Traveler Programs do not.

[2] *See* DHS/CBP/PIA-002 Global Enrollment System (GES), *available at* www.dhs.gov/privacy.

[3] The FAST program is divided between the northern border, FAST North, and the southern border, FAST South. Because FAST North is a joint program between the United States and Canada, applicants must be approved by both the United States and Canada to participate. FAST South applicants must only be approved by CBP because the FAST South program is not shared with Mexico.

[4] 79 FR 27161, *available at* https://www.gpo.gov/fdsys/pkg/FR-2df/2014-10767.pdf.

[5] *See* ABTC Program, *available at* http://www.apec.org/about-us/about-apec/business-resources/apec-business-travel-card.aspx.

Procurement System (DTOPS) Registered Traveler Programs. In addition, the PIAs describe the Trusted Worker Programs including the Bonded Worker program, the CBP Licensed Broker program, and the eBadge program, which processes airport badges and credentials in cooperation with the Transportation Security Administration (TSA) and commercial service providers. Finally, the most recent GES PIA update[6] explains the expansion of recurrent vetting of trusted traveler and trusted worker populations through the U.S. Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Criminal Justice Information Service's (CJIS) National Crime Information Center (NCIC)[7] via an interface with the National Law Enforcement Telecommunications System (Nlets)[8] within the TECS Platform[9] (now known as the NCIC/Nlets Recurrent Vetting Service, or NNVS).

Reason for the PIA Update

CBP is issuing this PIA update for the Global Enrollment System to assess the following changes to the GES application process. By replacing the Global Online Enrollment System (GOES) with the TTP System, CBP is providing notice and privacy assessment of the following changes: (1) system name change to TTP System; (2) location of the data (cloud provider); and (3) authentication mechanism (Login.gov[10]).

Trusted Traveler Program (TTP) System

CBP has developed the TTP System to replace GOES as the primary public-facing, online interface for applicants to submit program application, background investigation, and enrollment data. CBP has used GOES to support more than six million enrollees in CBP's Trusted Traveler Programs, and to enable existing and prospective Trusted Traveler Program members to apply for and check the status of their enrollment online via a secure website. CBP is replacing GOES with the TTP System, which will become the main system for online enrollment into the Trusted Traveler Programs. To maintain continuity, GOES will not be retired until the TTP System becomes fully operational. Once launched to the public, individuals will no longer be able to access GOES. The user will need to create an account in Login.gov to view membership information,

[6] *See* DHS/CBP/PIA-002(c) Global Enrollment System (GES) (November 1, 2016), *available at* www.dhs.gov/privacy.

[7] The National Crime Information Center (NCIC) is an FBI-owned system that assists law enforcement in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists. Additional information on NCIC is available at https://www.fbi.gov/services/cjis/ncic.

[8] The National Law Enforcement Telecommunications System (Nlets) is a non-profit organization owned by the states that allows state and federal law enforcement agencies, as well as select international agencies, to securely share law enforcement, criminal justice, and public safety related information. Additional information on Nlets is available at http://www.nlets.org/.

[9] *See* DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative (August 5, 2011), *available at* www.dhs.gov/privacy.

[10] *See* General Services Administration Privacy Impact Assessment for Login.gov (March 29, 2017), *available at* www.gsa.gov/pia.

update information, or renew an application in TTP. Membership benefits for existing members are not contingent on the creation of a TTP account. Similar to GOES, TTP only temporarily stores information. The information collected from TTP will be transferred to GES once the individual submits an application.

Transition to the Cloud

As part of a broader CBP effort to transition major IT applications from physical servers to a cloud-based environment, CBP is launching the cloud-based TTP System[11] to replace GOES. The TTP System is the first of many CBP applications that are migrating to the new cloud environment. This cloud environment will offer a more flexible and scalable platform to operate CBP's IT capabilities and solutions. In addition to migration to the cloud, the TTP System will also be optimized for use on tablets and mobile devices to improve user experience and permit applicants to enroll in any of the CBP's Trusted Traveler Programs. Last, the transition to the TTP System will allow travelers to apply to all TTP programs online through one interface. Although they may apply to NEXUS, FAST North, and SENTRI via a paper-based process, they will be required to create a TTP System account in order to schedule an appointment and activate their card to complete the enrollment process.

Login.gov

As part of the TTP System enhancements, CBP is partnering with GSA to pilot the use of the newly-released federal identity authentication mechanism, Login.gov, to authenticate GES applicants who register in the TTP System. Login.gov verifies the authenticity of users looking to access public services offered by CBP and other federal agencies using the same User ID or email address for all services. Login.gov collects biographic and contact information and uses two-factor authentication, sending a temporary, single-use security code to a phone via voice or text to allow a user to log-in. Login.gov subsequently shares the user's phone number and email address with the TTP System.

Individuals who seek to apply to a Trusted Traveler Program are directed to Login.gov, where they must create an account by first entering their email address, which will become the individual's UserID. Login.gov automatically sends a link to that applicant's email account, who then must follow the link to verify that the email address is correct. The applicant is then prompted to create a password and enter a phone number; once entered, Login.gov sends a security code via text or voice call to the applicant's phone. The applicant then inputs the security code to Login.gov to verify his or her identity. After the applicant's identity is verified, Login.gov sends an email with a 16-character personal key which will allow the applicant to verify his or her account in

[11] The TTP System is hosted in a Federal Risk and Authorization Management Program (FedRAMP)-certified public cloud environment. FedRAMP standardizes security assessment, authorization, and continuous monitoring for cloud products and services. CBP is working to transition many of its systems to the cloud by 2020.

future instances, most commonly occurring in the case of a lost phone or forgotten password.

After successfully logging into Login.gov, the user may proceed into the TTP System. Then the applicant selects his or her desired program (*e.g.*, Global Entry, NEXUS, SENTRI, or FAST) and provides the required information to apply. Login.gov sends to the TTP System the applicant's email address, phone number, and a universal unique identifier (UUID). The applicant then enters his or her name, residence and mailing addresses, phone number, date of birth, and city, state/province, and country of birth into the TTP System.

Applicants may also make limited updates to their data through the TTP System (although once the user has submitted his or her application, he or she may not make additional changes until after CBP has approved the application). Users may also monitor their application and enrollment status online. Upon completion of the application, the TTP System directs applicants to the U.S. Department of Treasury's Pay.gov[12] webpage to pay the application processing fee. The TTP System then sends all completed and paid applications to CBP's GES to initiate the electronic vetting and risk assessment and complete the enrollment process. Once approved, program members must activate their Trusted Traveler cards online.

Privacy Impact Analysis

Authorities and Other Requirements

The changes described above do not impact the Trusted Worker Program. Additionally, CBP's authorities related to the Global Enrollment System, specifically the Trusted Traveler Programs, have not changed since the last PIA update.

The information collected from applicants in the TTP System continues to receive coverage in a similar manner to GOES, under DHS/CBP-002 Global Enrollment System,[13] DHS/ALL-037 E-Authentication Records System of Records,[14] and Paperwork Reduction Act (PRA) Office of Management and Budget (OMB) control numbers 1651-0008 and 1651-0034. SORN coverage is now additionally provided under GSA/TTS-1 Login.gov.[15]

Characterization of the Information

The TTP System collects the same information that was previously collected by GOES.

[12] *See* Treasury Financial Management Service Pay.gov PIA, *available at* https://www.fms.treas.gov/pia/paygov_pia%20.pdf.

[13] *See* DHS/CBP-002 Global Enrollment System (GES) System of Records, 78 FR 3441 (November 1, 2016).

[14] *See* DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (August 11, 2014).

[15] *See* GSA/TTS-1 Login.gov, 82 FR 6552 (January 19, 2017).

Login.gov enhances the security of login information by using multi-factor authentication to verify the identity of individuals seeking benefits or services from federal agencies. Login.gov will collect the following information from applicants in order to create a user profile:

- Email address (also serves as User ID);
- Password; and
- Phone number (for two-factor authentication).

All Login.gov records are stored electronically in a database in GSA's virtual cloud environment.[16] As a security measure, Login.gov requires each user to provide a phone number at account creation to enable two-factor authentication. Login.gov also generates and assigns each user a universal unique identifier (UUID) during the account creation process and then an additional UUID for each partner agency that user accesses via Login.gov. The UUID is stored during each of the user's sessions so that CBP and other partner agencies may use it to locate a user's profile within its own system. For example, if an individual accesses two different agencies' information or services through Login.gov, that user is assigned two different UUIDs. However, each agency will only be provided the user's UUID related to that particular visit to the respective agency's website.

Following account creation, Login.gov assigns each user a 16-character recovery code or personal key, which may be used as a security challenge question if the user does not have access to his or her phone. Finally, each user must consent to the sharing of his or her User ID or email address with CBP (or the appropriate partner agency) to access that agency's services and information, and to enable that agency to recognize that user on subsequent visits. All user account information is encrypted using Transport Layer Security over Hypertext Transfer Protocol Secure (TLS over HTTPS) (*i.e.*, when phone numbers, email addresses, and UUIDs are shared with CBP and other partner agencies).

Login.gov shares the following data elements with the TTP System to verify that the user has been authenticated:

- UUID;
- User ID or email address (pre-populated in the TTP System); and
- Phone number.

Once registered via Login.gov, applicants select their desired program and enter the required application information as described in previous GES PIAs and subsequent updates. Aside from the above-described changes, the PII collection, process, and procedural requirements discussed previously in the 2013 and 2016 GES PIAs remain in effect.

[16] *See* GSA/TTS-1 Login.gov, 82 FR 6552 (January 19, 2017).

Privacy Risk: There is a risk that an individual may input inaccurate information into Login.gov, resulting in a failure to authenticate and access the TTP System.

Mitigation: Login.gov requires the user to verify both his or her email address and phone number by sending verification links and security codes to the system user's email account and registered phone. These authentication methods ensure that individuals cannot register with Login.gov unless the information they provide is accurate and complete.

Uses of the Information

CBP collects information from applicants on a voluntary basis, in order to assess their eligibility for enrollment in its Trusted Traveler, Registered Traveler, and Trusted Worker Programs supported by the GES/TTP System. CBP conducts recurrent vetting on Trusted Traveler and Trusted Worker applicants and enrollees to safeguard against threats to law enforcement or national security, and to determine their eligibility to receive expedited processing at the border or access to sensitive CBP-controlled areas or positions. CBP also vets these individuals to ensure that they either meet or remain eligible for program participation. Unlike Trusted Travelers and Trusted Workers, CBP will not use the information to conduct recurrent vetting or assess further eligibility of Registered Travelers.

For Login.gov, a user must opt-in to share any information with each partner agency such as CBP. For example, when a user navigates to CBP's TTP System website and accesses it via Login.gov, that user is provided an opportunity to consent to CBP's use of the User ID or email address. The email address provided by the user becomes the account through which Login.gov may share the participant's information at his or her request with other federal agencies as needed for other programs. The user can then change the email address associated with his or her Login.gov account at any time, but changing that address will redirect all email correspondence from CBP and other partner agencies. Additionally, the user's phone number is required to enable two-factor authentication. The user's phone number is required to receive and respond with the one-time security code for user authentication. If no phone number is provided, the user will not be able to create a Login.gov, or TTP System, account.

Privacy Risk: There is a risk that information used to enroll individuals in a Trusted Traveler, Registered Traveler, or Trusted Worker Program will be used for a purpose inconsistent with the original collection.

Mitigation: This risk is mitigated in Login.gov because each user's UUID is specific to only one agency, thereby decreasing the risk that a third-party could re-identify the user across visits to different agencies. In addition, Login.gov does not retrieve a user's account information unless that user provides either his or her password or recovery code. One copy of each user's account information is encrypted using his or her password, and a second copy is encrypted using the recovery code.

This risk is also mitigated by the manner in which CBP collects and stores information for Trusted Traveler, Registered Traveler, and Trusted Worker Programs in the TTP System. CBP manages the various programs in separate environments, which can interface when an applicant applies for a separate GES-managed program. The data segregation also supports software management for the various programs.

All TTP System users are trained to use information only to determine program eligibility. All CBP system administrators are required to take annual privacy training to refresh and emphasize the importance of effective practices for managing PII. All GSA personnel are trained on how to identify and safeguard PII through annual privacy and security training. Finally, all GSA staff who need to access, use, or share PII as part of their regular responsibilities related to Login.gov must complete additional role-based training.

Notice

CBP provided notice for Trusted Traveler, Registered Traveler, and Trusted Worker Programs by publishing the GES PIA and subsequent updates and the corresponding SORN. Similarly, this PIA provides notice of CBP’s migration from GOES to the TTP System, and its use of Login.gov for authentication and identity verification. In addition, the TTP System website notifies the applicant that he or she must create a Login.gov account to access system services. Once registered, users are directed to continue to CBP’s TTP System website to sign in and continue or complete the application process. Each Login.gov user is provided with the Privacy Policy and Terms of Use before creating an account and submitting information. The Login.gov Privacy Policy describes, among other things, what information is collected and automatically stored, how submitted information may be shared, site security, and the purposes for collecting the requested information. Users may access the Login.gov Privacy Policy on any webpage of the site. The Login.gov PIA is available at www.gsa.gov/pia.

When an individual applies for a program through the TTP System website, he or she must certify that he or she has read the Privacy Notice that describes the information collection required for program consideration. Furthermore, CBP will provide a general notice on the TTP System website to applicants who use it for processing purposes.

CBP does not require anyone to participate in any Trusted Traveler, Registered Traveler, or Trusted Worker Programs. Applicants must certify that they understand that 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 consistent with the applicable program PIAs, SORNs, and program guidelines. The data collected in GES is used only for the purposes articulated, 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.

Privacy Risk: There is a risk that applicants and enrollees may not know how CBP will use their information submitted to the TTP System.

Mitigation: CBP mitigates this risk by providing Privacy Notices on the TTP System website that state the purpose for collecting the data. CBP also mitigates this risk by the publishing a series of GES PIAs and the applicable SORNs, which provide transparency into GES information usage.

Data Retention by the Project

There are no changes to the CBP's retention schedule, and thus, the same retention practices that applied to the previous system apply to the TTP System. The TTP System only retains information until the individual submits an application. The information is then transferred to GES. GES data is retained for three years after an individual's membership in a Trusted Traveler or Trusted Worker Program is no longer active, due to expiration without renewal at the end of five years, abandonment, or CBP termination.

For Login.gov, all records will be maintained for at least six years in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2 "System access records," which covers user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges to partner agencies for usage of Login.gov. However, GSA is authorized to maintain the information for longer if it is required for business use. Login.gov must be able to provide users access to information and services at partner agencies and, therefore, GSA is authorized to maintain the information longer than the six-year retention period if it has a business need.

Privacy Risk: There is a risk that GSA may retain Login.gov user information longer than necessary for business purposes, since there is no clear trigger for account deletion.

Mitigation: This risk is not mitigated. In general, GSA will retain the information for six years or consistent with its business need, which may be indefinite; however, GSA provides notice of its retention in the Login.gov Privacy Policy and PIA.

Information Sharing

The information sharing parameters described in the previous GES PIAs and associated SORNs remain in effect. CBP shares ABTC, NEXUS, and FAST North application information with the Canadian Border Services Agency (CBSA). The United States and Canada do not share PII with APEC or any ABTC international database because they are transitional members of the ABTC international program.

CBP may share GES application information with partnering international countries, excluding vehicle-related information, as applicable, once submitted directly by the applicant undergoing the vetting process. No derogatory information or records are exchanged through these arrangements, and CBP only receives a "pass/fail" decision from the partnering international country and conversely only provides a pass/fail for reciprocal programs. All information sharing agreements must be reviewed and approved through an internal CBP process that includes a review by CBP policy and privacy officials, and the CBP Office of Chief Counsel. Once CBP approves an information sharing arrangement, it is forwarded to DHS for final review and approval.

CBP may share GES information pertaining to airport workers with airport authorities through commercial service providers as part of the Security Threat Assessments (STA) and customs checks process associated with the eBadge Program.

Finally, for applicants who are approved by Login.gov for entry into CBP's TTP System, Login.gov shares relevant information with the TTP System, such as the Login.gov-generated UUID, phone number, and User ID or email address. The user must consent to the sharing of his or her User ID or email address by Login.gov with CBP in order to access the TTP System and to enable the TTP System to recognize that user on subsequent visits. The email address is the only data element that is currently pre-populated in the TTP System.

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 consistent with DHS/CBP-002 Global Enrollment System and DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities,[17] and only subject to the terms of any applicable information sharing arrangement. 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 authorized activities and only within the parameters of its information sharing agreements.

Redress

Individuals may continue to request information about their records in GES by mailing their request, in the format described in DHS/CBP-002 Global Enrollment System[18] and the DHS/ALL-037 E-Authentication Records System of Records[19] to:

[17] *See* DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 75 FR 77753 (December 19, 2008).

[18] *See* DHS/CBP-002 Global Enrollment System (GES) System of Records, 78 FR 3441 (November 1, 2016).

[19] *See* DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (August 11, 2014).

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002

For Login.gov, users can access their information directly at any time and may modify or amend any of their user account information (such as the email address or phone number) by accessing it on their account.[20]

Privacy Risk: There is a risk that an individual may be unable to successfully complete the Login.gov authentication process and access his or her TTP System account.

Mitigation: This risk is mitigated. The authentication process for Login.gov is very basic and does not require knowledge-based questions or a high level of identity proofing. If an individual fails to complete the login process, he or she can try again with a new email or phone number, or he or she may request a new verification code.

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for records in GES.

Mitigation: This risk is partially mitigated. This PIA, DHS/CBP-002 Global Enrollment System,[21] and DHS/ALL-037 E-Authentication Records System of Records[22] describe how individuals can make access requests under the Privacy Act or Freedom of Information Act (FOIA). Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access or correction of GES records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in GES, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation, or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible

[20] *See* GSA/TTS-1 Login.gov, 82 FR 6552 (January 19, 2017).
[21] *See* DHS/CBP-002 Global Enrollment System (GES) System of Records, 78 FR 3441 (November 1, 2016).
[22] *See* DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (August 11, 2014).

administrative burden on investigative agencies.

Auditing and Accountability

The same auditing and accountability procedures in place for GOES are in place for the TTP System, which has been granted an Interim Authority to Operate. The Department is processing a full ATO to ensure that the relevant security and accountability measures are in place.

Login.gov has been granted a full Authority to Operate by the General Services Administration. Login.gov resides in a FedRAMP authorized cloud environment that complies with Federal Information Processing Standards (FIPS) 199[23] for moderate systems. Administrative access to Login.gov is protected from misuse by two-factor authentication (strong passwords plus government-issued personal identity verification (PIV) card), and the system is audited and monitored regularly for inappropriate or unusual activity.[24]

Responsible Officials

Cheryl C. Peters
Office of Field Operations
U.S. Customs and Border Protection
202-344-1707

Debra L. Danisek
CBP Privacy Officer
Office of Privacy and Diversity
U.S. Customs and Border Protection
202-324-1610

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

[23] FIPS 199 is a Federal Government standard that establishes security categories of information systems used by the Federal Government, one component of risk assessment. For more information, please see http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[24] For more information about Login.gov security and access controls, please *see* the Privacy Impact Assessment for Login.gov LOA1 (March 29, 2017), *available at* https://www.gsa.gov/portal/content/102237.