Privacy Impact Assessment Update
for the

Global Enrollment System (GES): Global Entry Facial Recognition

DHS/CBP/PIA-002(e)

December 13, 2019

Contact Point

Stephan Mongin
Office of Field Operations
U.S. Customs and Border Protection
(202) 325-3167

Reviewing Official

Jonathan R. Cantor
Acting 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 Global Entry, a program that provides dedicated processing for pre-approved travelers arriving in the United States. 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 provide notice to the public regarding the upgrade of Global Entry kiosks with facial recognition technology to facilitate traveler identification and entry processing.

Overview

CBP offers a number of trusted traveler programs, including Global Entry, that enable CBP to expedite the inspection and security process for low-risk travelers, allowing CBP to focus resources toward providing additional scrutiny to individuals who present an unknown risk. Low-risk travelers are directed to dedicated lanes and kiosks at designated ports of entry for expedited processing resulting from CBP's pre-approval activities. This expedited processing of low-risk travelers and workers allows CBP Officers (CBPOs) additional time to focus on higher risk and unknown individuals.

The previously published Global Enrollment System (GES) PIA and subsequent updates[1] describe GES and CBP's Trusted Traveler/Trader Programs, which include the following: Global Entry, NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), Free and Secure Trade for commercial vehicles (FAST),[2] and the U.S. Asia-Pacific Economic Cooperation (APEC)[3] Business Travel Card Program (ABTC).[4] In addition, the PIAs describe the Trusted Worker Programs such as the Bonded Worker program, the CBP Licensed Broker program, and the eBadge program, in partnership with the Transportation Security Administration (TSA) and commercial service providers. In 2016, the U.S. Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Criminal Justice Information Service's (CJIS) National Crime Information Center (NCIC)[5] expanded upon the recurrent vetting of trusted traveler and trusted worker

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

[2] 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.

[3] 79 FR 27161, *available at* https://www.gpo.gov/fdsys/pkg/FR-2df/2014-10767.pdf.

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

[5] 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

populations via an interface with the National Law Enforcement Telecommunications System (Nlets)[6] within the TECS Platform[7] (now known as the NCIC/Nlets Recurrent Vetting Service, or NNVS). Finally, the most recent PIA Update[8] described the name change of the previous Global Online Enrollment System (GOES) to the new Trusted Traveler Program (TTP) System, along with the new location of the GES data within a cloud environment, and the addition of Login.gov as a mechanism for the identity verification of TTP System users.

Reason for the PIA Update

CBP is issuing this PIA update to assess the privacy impacts of the following programmatic changes: (1) updates to the existing Global Entry kiosks to use cameras and facial recognition technology provided by CBP's Traveler Verification Service (TVS);[9] and (2) the use of photographs collected at the Global Entry kiosk, rather than the collection of travel documents and fingerprints, to verify traveler identity.

Global Entry Facial Recognition Process

CBP uses Global Entry kiosks to process eligible travelers entering the United States through designated air ports of entry. To continue to offer Global Entry members expedited service through the CBP inspection process, CBP has equipped Global Entry kiosks at select airports[10] with facial recognition technology. As part of the current enrollment interview process, CBP captures fingerprints and facial images for identity verification of Global Entry applicants. These biometric records are stored in the DHS Office of Biometric Identity Management's Automated Biometric Identification System (IDENT).[11] Historically, Global Entry members provided a swipe of their passports and submitted their fingerprints at the kiosk to verify their identity by matching them against the fingerprints stored in IDENT. While not used to verify the individual's identity, the individual also provided a facial image at the kiosk which was stored as part of the traveler's entry record. Under the new process, CBP will no longer collect the member's fingerprints through

information on NCIC is available at https://www.fbi.gov/services/cjis/ncic.

[6] 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/.

[7] *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.

[8] *See* DHS/CBP/PIA-002(d) Global Enrollment System (GES); Trusted Traveler Program (TTP) System, *available at* www.dhs.gov/privacy.

[9] *See* DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2019), *available at* www.dhs.gov/privacy.

[10] This change will also impact NEXUS members who have access to GE kiosks in U.S. airports and NEXUS kiosks in Preclearance locations.

[11] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.

the Global Entry kiosk upon entry, but will use the facial image to retrieve the traveler's record and verify his or her identity. This image will then be enrolled in IDENT as a biometric encounter.

CBP creates photographic galleries (organized by airport and terminal) using the Advance Passenger Information System (APIS)[12] manifest for incoming flights during a brief, defined period of time, which is generally only a certain portion of the day. To populate the localized galleries with photographs, the TVS[13] compiles pre-existing photographs already maintained in the Automated Targeting System (ATS)[14] Unified Passenger Module (UPAX) system. CBP may have captured these images from U.S. passports or visas, previous entry inspections, and/or other DHS encounters, including Global Entry enrollment photos.[15] The TVS then generates a biometric template[16] for each gallery photograph and stores the template, but not the actual photograph, in the TVS cloud for matching when the traveler arrives at the Global Entry kiosk.

Global Entry members who provide a facial photograph at the kiosk are not required to provide fingerprints (though they are still required for initial enrollment and vetting), a customs declaration,[17] or a machine-readable passport or permanent resident card at the kiosk. Upon entering CBP's Federal Inspection Service (FIS) at a participating airport, an approved traveler may approach one of the new or updated Global Entry kiosks and present himself or herself for a photo in front of the kiosk camera. Once the Global Entry kiosk captures a new photo of the traveler, the kiosk submits the photo through the GES to the TVS, which conducts the backend biometric matching with previous photos on file and provides the matching results.[18] Based on

[12] *See* DHS/CBP/PIA-001 Advance Passenger Information System (June 5, 2013), *available at* https://www.dhs.gov/privacy and DHS/CBP-005 Advance Passenger Information System, 80 FR 13407 (March 13, 2015).

[13] CBP's TVS is an accredited information technology system consisting of a group of similar systems and subsystems that support the core functioning and transmission of data between CBP applications and partner interfaces. Since early 2017, CBP has used the TVS as its backend matching service for all biometric entry and exit operations that use facial recognition, regardless of air, land, or sea.

[14] *See* DHS/CBP/PIA-006 Automated Targeting System (January 13, 2017), *available at* https://www.dhs.gov/privacy.

[15] U.S. passport and visa photos are available via the Department of State's Consular Consolidated System. *See* Privacy Impact Assessment: Consular Consolidated Database, *available at* https://2001-2009.state.gov/documents/organization/93772.pdf. Other photos may include those from DHS apprehensions or enforcement actions, previous border crossings, and immigration records.

[16] A biometric template is a digital representation of a biometric trait of an individual generated from a biometric image and processed by an algorithm. The template is usually represented as a sequence of characters and numbers. For the TVS, templates cannot be reverse-engineered to recreate a biometric image. The templates generated for the TVS are proprietary to a specific vendor's algorithm and cannot be used with other vendor's algorithms.

[17] Note that the photograph does not replace the customs declaration; passengers will no longer provide an electronic declaration through the Global Entry kiosks, but will provide an oral declaration to a CBPO upon exit of the FIS.

[18] This process is the same as described in the TVS PIA for Simplified Arrival: "Once the traveler is matched, the TVS transmits the match results, along with a TECS system-generated unique traveler identifier and an ATS-UPAX-generated unique photo identifier, to TECS. In turn, the TECS primary arrival subsystem uses the TECS-generated identifier to retrieve the traveler's biographic information from the APIS manifest. Additionally, the TECS subsystem uses the ATS-UPAX-generated identifier to retrieve the historical image (which had matched with

these positive or negative matching results, the Global Entry kiosk issues a transaction receipt to the traveler, directing him or her to the baggage claim and exit, or to a CBPO for a brief interview or further inspection, if necessary. The transaction then generates a record of entry in TECS and the new facial image is enrolled in IDENT. CBP uses these encounter photos for future traveler verification. When comparing photos for a facial recognition match, TVS uses travel document photos as well as recently taken photos to improve accuracy because up to date photos may match better than document photos. The Global Entry process may include additional steps for nonimmigrant visa-holders or those seeking admission under the Visa Waiver Program.

In the event that the photo capture fails, or the photo fails to produce a match, the system reverts back to the original process requiring a passport swipe and fingerprint scan. If the passenger opts to cancel the transaction up to the point when he or she submits the photo, the passenger will receive a receipt referring him or her to an officer on primary to complete the process.

To initially operate this new program, CBP will upgrade, and in some cases, replace the existing Global Entry kiosks at select airports. Eventually, CBP plans to retire the older machines and replace them with new kiosks for this program.

Privacy Impact Analysis

Authorities and Other Requirements

CBP maintains biographic and biometric information from Global Entry members in accordance with the DHS/CBP-002 Global Enrollment System[19] System of Records. CBP's collection of this information is covered under the Paperwork Reduction Act (PRA) by the Office of Management and Budget (OMB) information collection control numbers 1651-0008, 1651-0034, and 1651-0138. The facial images used to create the gallery for identity verification are governed by the System of Records Notice (SORN) associated with that collection; these may include the Global Enrollment System SORN as well as DHS/CBP-007 Border Crossing Information (BCI),[20] ATS,[21] and TECS[22] SORNs.

the new image) stored in UPAX. The CBPO has the ability to view and evaluate the traveler's biographic data, along with any derogatory information, in the TECS primary arrival application, along with associated biometric match results from the TVS."

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

[20] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).

[21] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

[22] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

Characterization of the Information

In deploying facial recognition capabilities at Global Entry kiosks, CBP is not collecting any new information from Global Entry travelers; rather, CBP is reducing the amount of information the traveler must provide to verify the traveler's identity by no longer requiring the traveler to submit fingerprints and a passport scan. During the existing CBP Global Entry inspection process, CBP already collects and stores facial images, along with fingerprints and a passport scan. Under this new process, the facial image will continue to be collected, and will be used to retrieve the traveler's record instead of the passport scan. The use of facial recognition for identity verification will replace the collection of fingerprints. The use of facial image for identity verification reduces the information collection from the traveler, who no longer has to provide his or her fingerprints again and swipe a passport upon entry.

Privacy Risk: There is a risk that the new process will not be able to verify traveler identities based on previously collected facial photos, which may be old or not of high enough quality to produce a reliable match.

Mitigation: This risk is mitigated. CBP is continually testing and evaluating the accuracy of the camera technology and the algorithms to ensure a high degree of confidence across all demographics, even with older photos.[23] Additionally, the use of previously taken encounter photos stored in IDENT increases the accuracy of TVS. The encounter photos provide more up-to-date images of travelers than those taken when the traveler submitted his or her Global Entry application. If the traveler identity is not successfully verified through facial recognition, the kiosk reverts to the legacy process requiring the travel document and fingerprint scans, and then refers the passenger to a CBPO to verify the passenger's identity.

Uses of the Information

CBP collects facial images captured at the Global Entry kiosks in order to verify the identity of the traveler by comparing the facial photo captured at the kiosk with photos previously captured by CBP. In addition, the facial image replaces fingerprints as the primary mechanism for retrieving the traveler's records and for associating the new crossing record with the previous travel history. CBP uses this information to ensure accurate identification of travelers, in order to determine whether to refer travelers for additional customs and immigration inspection, as needed, and to ensure accurate records of travel into the United States.

[23] For additional information on CBP's efforts to ensure the accuracy of its facial recognition algorithm, please see DHS/CBP/PIA-056 Traveler Verification Service, available at www.dhs.gov/privacy.

As before, CBP collects biographic information from trusted travelers, on a voluntary basis, in order to assess their eligibility for enrollment in the respective programs. CBP conducts recurrent vetting on trusted traveler applicants and members to safeguard against threats to law enforcement or national security, and to determine their eligibility and subsequently, their continued eligibility to receive expedited processing at the border or access to sensitive CBP-controlled areas or positions.

Privacy Risk: There is a risk that biometrics CBP uses to verify the identities of individuals and to determine whether to refer travelers for additional customs and immigration inspection in the Global Entry Program will be used for a purpose inconsistent with the purpose of the original collection.

Mitigation: This risk is mitigated. CBP collects facial images of Global Entry travelers in order to verify their identities and thus status in the program, prior to entering the United States. Additionally, CBP creates entry records primarily in support of its mission to facilitate legitimate travel and enforce immigration laws, which include activities related to counterterrorism and immigration enforcement. Consistent with the existing Global Entry process, border crossing records and the associated photos of Global Entry travelers are stored in IDENT and may be available to authorized IDENT users for a variety of purposes, which DHS reviews and approves prior to granting access to the system. CBP owns and operates all of the Global Entry kiosks; no outside parties or vendors own any of the equipment or have access to the data residing on the kiosk.

Notice

CBP provided notice for Trusted Traveler Program members by publishing the GES PIA and subsequent updates and the corresponding SORN.[24] Similarly, this PIA provides notice of another expansion of CBP's facial recognition program to include identity verification of trusted travelers in the Global Enrollment System.

When an individual applies for a membership in a CBP trusted traveler program through the GES/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. CBP will also provide a general notice on the TTP System website to applicants in order to inform them of the how CBP uses the biographic and biometric information it collects. Global Entry participants are notified of the use of facial recognition through visible signage in front of the Global Entry

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

kiosks, the Global Entry website,[25] a Privacy Notice on various screens on the kiosks, and tear sheets with Frequently Asked Questions for those who request additional information.

CBP does not require anyone to participate in any Trusted Traveler 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 program requirements and as described in the applicable PIAs and SORN. The data collected through the Global Entry kiosks is used for the purposes articulated, including border and immigration management, national security, and law enforcement. Due to the voluntary nature of this program, the only opportunity for Global Entry members to opt out of the use of their biometric or biographic data is to cancel their membership.

Privacy Risk: There is a risk that individuals may not know how CBP will use the photos they submit to the Global Entry Facial Recognition Process upon entry into the United States, or will not know that CBP uses facial recognition to identify them based on their photo.

Mitigation: CBP mitigates this risk by providing Privacy Notices on the home screen of every updated kiosk that states the purpose for collecting the data, uses of the data, sharing, and disposal. In addition, visible signage, the Global Entry website, and tear sheets are available at the FIS for those who request additional information. CBP also mitigates this risk by publishing a series of GES and TVS PIAs as well as the applicable SORNs, which provide transparency into GES information usage.

Data Retention by the Project

There are no changes to the CBP's GES retention schedule, and thus, the same retention practices that applied to the previous GES PIAs also apply to the new processes described in this PIA. The kiosks retain information, including the photos, only until the individual is processed for admission into the United States. The information is then transferred to the GES. Photos in the GES are retained for three years after an individual's membership in a Trusted Traveler program is no longer active, whether the inactivity is due to expiration without renewal at the end of five years, abandonment, or CBP termination. For photos that are shared with the TVS for matching purposes, CBP will follow the TVS retention schedule.[26] CBP does not retain the facial images of U.S. citizens in ATS-UPAX once their identities are verified by the TVS. Only photos of non-U.S. citizens are retained for the full 14 days in ATS-UPAX. However, images of all members of Trusted Traveler Programs, including Global Entry, are enrolled in IDENT as a biometric

[25] https://www.cbp.gov/travel/trusted-traveler-programs/global-entry.
[26] *See* DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), *available at* https://www.dhs.gov/privacy.

confirmation of a traveler's arrival in the United States.[27] CBP is currently working to finalize the official records retention schedule to submit to the National Archives and Records and Archives Administration for approval. The travelers' historical photos, which are retrieved from ATS-UPAX for the purposes of matching with the new photos captured at the Global Entry kiosk, will be maintained in the TVS cloud matching service for up to 12 hours after identity verification, for continuity of operations purposes.

Privacy Risk: There is a risk that the TVS may retain Global Entry user information longer than necessary, since the TVS is a separate IT system.

Mitigation: The TVS does not retain the images of any travelers, including U.S. citizens, once their identities are verified by the TVS.[28] Only photos of non-U.S. citizens are retained for the full 14 days in ATS-UPAX. However, photos of all Global Entry members, including U.S. citizens, are stored for 75 years in IDENT, consistent with the border security purpose for which the information is collected as well as to improve the accuracy of future image captures.[29]

Information Sharing

The information sharing parameters described in the previous GES PIAs and associated SORNs remain in effect. There are no changes to information sharing associated with the use of facial recognition at Global Entry kiosks. The use of facial recognition does not constitute a new collection of any information by CBP; accordingly, no new information is shared pursuant to this process. No metadata pertaining to the use of facial recognition is available outside of CBP. As before, all information related to Global Entry members, including each of the photos taken upon entry, is available to authorized IDENT users outside of CBP as documented in previous PIAs. In addition, CBP continues to share relevant Global Entry records and associated border crossing information as documented in the previous PIAs and in accordance with the relevant SORNs.

[27] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.

[28] Photos of all travelers, including U.S. citizens, are held in the TVS cloud matching service for no more than 12 hours after identity verification, in case of an extended system outage.

[29] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.

Redress

Individuals may continue to request information about their records in the GES/TTP System by mailing their request in the format described in DHS/CBP-002 Global Enrollment System[30] to:

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

Privacy Risk: There is a risk that individuals are not aware of their ability to request access to their trusted traveler or border crossing records.

Mitigation: This risk is mitigated. This PIA, the TVS PIA,[31] and other relevant PIAs and SORNs describe how individuals can make access requests under FOIA or the Privacy Act. Redress is available for U.S. citizens and lawful permanent residents through requests made under the Privacy Act as described above. U.S. law does not extend Privacy Act protections to individuals unless they are U.S. citizens or 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 records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records collected and retained pursuant to the TVS process, 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 administrative burden on investigative agencies.

[30] *See* DHS/CBP-002 Global Enrollment System (GES) System of Records, 78 FR 3441 (November 1, 2016).
[31] *See* DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), *available at* https://www.dhs.gov/privacy.

Auditing and Accountability

The same auditing and accountability procedures are in place for both the GES and the new Global Entry Facial Recognition Process. The CBP Office of Information Technology granted GEP a three-year Authority to Operate on April 6, 2017.

Responsible Officials

Stephan Mongin
Office of Field Operations
U.S. Customs and Border Protection
202-325-3167

Debra L. Danisek
CBP Privacy Officer
Office of Privacy and Diversity
U.S. Customs and Border Protection
202-344-1610

Approval Signature

[Original signed and on file with the DHS Privacy Office]

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