U.S. Customs and Border Protection

CBP Privacy Evaluation (CPE)

of the

Traveler Verification Service (TVS)

in support of the CBP Biometric Entry-Exit Program

August 15, 2022

Contact Point
Matthew S. Davies
Executive Director
Admissibility and Passenger Programs
Office of Field Operations

Reviewing Official
(b) (6), (b) (7)(C)
Privacy Officer
Privacy and Diversity Office
Office of the Commissioner

I. Background

U.S. Customs and Border Protection (CBP) is steadfast in its mission to safeguard United States borders while protecting the privacy of all individuals. As part of ongoing efforts to maintain the utmost standards of transparency and accountability for the CBP Biometric Entry-Exit (BE-E) Program, the CBP Privacy Office conducted a CBP Privacy Evaluation (CPE) of the BE-E Program's use of the facial comparison technology Traveler Verification Service (TVS). The CBP Privacy Office conducted this CPE in accordance with the conditions outlined in the 2018 TVS Privacy Impact Assessment (PIA),[1] to determine whether the BE-E Program collects, maintains, uses, and shares information using the TVS in compliance with the privacy mitigations described in its PIA, the DHS Privacy Policy Guidance Memorandum on the Fair Information Practice Principles (FIPPs),[2] and the CBP Directive for Privacy Policy, Compliance, and Implementation.[3] This report outlines the CBP Privacy Office's findings and recommendations.

CBP Facial Comparison Technology Overview

In 2013, CBP began developing and testing new processes and capabilities for conducting its biometric entry and exit mission. There are numerous challenges to deploying a nationwide biometric entry-exit program, including the myriad differences in logistics and types of locations where travelers seek admission to and depart the United States.[4] In addressing these challenges, CBP spent several years testing different technologies in various locations (such as air, land, and sea ports of entry) to determine which biometric tool could be deployed large-scale without disrupting legitimate travel and trade, while still meeting the biometric entry-exit mandate.[5]

---

[1] DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[2] The Fair Information Practice Principles (FIPP): Framework for Privacy Policy at the Department of Homeland Security (December 29, 2008), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

[3] CBP Directive 2120-010 Privacy Policy, Compliance, and Implementation (January 2, 2015), *available at* (b) (7)(E)

[4] For full description of the history of the CBP biometric entry-exit program and various pilots, please see DHS/CBP/PIA-030 Departure Information Systems Test (June 13, 2016) and DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), *available at* https://www.dhs.gov/privacy.

[5] Statutes that require DHS to take action to create an integrated entry-exit system include: Sec. 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), P.L. 106-215, 114 Stat. 337; Sec. 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, P.L. 104-208, 110 Stat. 3009-546; Sec. 205 of the Visa Waiver Permanent Program Act of 2000, P.L. 106-396, 114 Stat. 1637, 1641; Sec. 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), P.L. 107-56, 115 Stat. 272, 353; Sec. 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), P.L. 107-173, 116 Stat. 543, 552; Sec.

TVS represents successful operationalization of CBP's biometric facial comparison technology to verify the identity of travelers arriving and departing the United States in the land, air, and sea environments. TVS serves as CBP's backend matching service for the collection and processing of facial images in support of biometric entry and exit operations. The program is supported by a network of secure cameras with encrypted data and connections owned by CBP, its commercial partners (port authorities, commercial air carriers, and cruise lines), and the Transportation Security Administration (TSA),[6] designed to facilitate traveler identity verification. TVS operates by matching live images captured by cameras at Ports of Entry (POEs) and other travel touch points against photographs that CBP already maintains, including images captured from previous entry inspections, U.S. passports, U.S.-issued visas, and other DHS encounters.[7] CBP also uses TVS to match live photos against photos on travel documents presented by travelers, to include, for example, those with no previous encounters. CBP uses TVS to change photographs into biometric templates, which are then compared in TVS to determine if the templates match.

II. Scope and Methodology

The CBP Privacy Office conducted this CPE to determine whether the collection, maintenance, use, and sharing of information utilizing TVS in support of the CBP BE-E Program is compliant with established privacy principles, policies, and legal requirements. CBP Privacy Office personnel reviewed existing privacy compliance documentation, policies, and legal requirements associated with TVS. The CBP Privacy Office also developed a comprehensive questionnaire designed to aid Privacy Office personnel in understanding the functions of TVS and clarify questions that arose during CBP Privacy Office's review of program-related compliance documents. The questionnaire was submitted to the Office of Field Operations (OFO) for responses, which were coordinated with Office of Information and Technology (OIT), and then reviewed by Privacy Office personnel.

In conducting this CPE, the CBP Privacy Office:

7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108-458, 118 Stat. 3638, 3817; Sec.711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, 121 Stat. 266, 338; and Sec. 802 of the Trade Facilitation and Trade Enforcement Act of 2015, P.L. 114-125, 130 Stat. 122, 199. In addition, through the Consolidated Appropriations Act of 2016 and the Bipartisan Budget Act of 2018, Congress authorized up to $1 billion in visa fee surcharges through 2027 to develop and implement the biometric entry-exit system. P.L. 114-113 129 Stat. 2242 (December 17, 2015); P.L. 115-123 132 Stat. 64 (February 9, 2018).

[6] TVS's support of TSA's identity verification of Trusted Traveler program participants engaged in domestic travel is outlined in DHS/TSA/PIA-046, *available at* https://www.dhs.gov/publication/dhstsapia-046-travel-document-checker-automation-using-facial-recognition.

[7] See: DHS/CBP/PIA-056 Traveler Verification Service: Appendix A (January 2020) for a list of CBP Owned and Operated Camera Collection Sites, available at, https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

- Reviewed DHS/CBP/PIA-056 Traveler Verification Service, as well as relevant System of Record Notices (SORNs) and Privacy Threshold Analyses (PTAs);
- Reviewed program and effort-specific PIAs that were developed before the overarching PIA was published, including:
    - DHS/CBP/PIA-030 Departure Information Systems Test-June 2016;
    - DHS/CBP/PIA-030(a) Departure Verification System-December 2016;
    - DHS/CBP/PIA-030(b) Traveler Verification Service (TVS);
    - DHS/CBP/PIA-030(c) Traveler Verification Service (TVS): Partner Process - June 2017 - Appendix Updated July 2018;
    - DHS/CBP/PIA-030(d) Traveler Verification Service (TVS): CBP-TSA Technical Demonstration - September 2017; and
    - DHS/CBP/PIA-030(e) Traveler Verification Service (TVS): CBP-TSA Technical Demonstration Phase II - August 2018.
- Developed and distributed a CPE questionnaire to OFO;
- Reviewed initial program responses and supporting documentation, including:
    - The Biometric Facial Debarkation Business Requirements;
    - Biometric Air Exit Business Requirements;
    - TVS Technical Reference Guides;
    - POE signage related to the program;
    - Public Awareness Campaign documents and signage;
    - CBP Security Assessment for one of CBP's commercial partners;
    - National Institute of Standards and Technology (NIST) NEC Facial Recognition Algorithm Performance Testing Summary;
    - OFO Biometric Exit Evaluating Bias and Performance Metrics presentation; and
    - Memorandum on "U.S. Citizen Opt Outs of Facial Comparison" issued on December 27, 2019, to the Ports outlining opt out provisions and requirements and the proper display of related signage.
- Coordinated with OIT to review system information related to data retention;

- Developed follow-up questions and reviewed responses provided by the OFO BE-E Program Office;
- Members of the CBP Privacy Office conducted site visits to POEs where TVS is deployed, including Atlanta Hartsfield International Airport, Dulles International Airport, John F. Kennedy International Airport, Las Vegas Harry Reid International Airport, Orlando International Airport, and Seattle-Tacoma International Airport;
- Reviewed complaints related to the collection and use of facial images submitted by members of the public to the CBP INFO Center;[8]
- Drafted an initial CPE report;
- Provided initial report to the OFO BE-E Program for review and comment;
- Provided report to the Office of Chief Counsel for review; and
- Finalized the report and provided it to OFO BE-E Program Office as well as the DHS Privacy Office.

III. Findings

The CBP Privacy Office finds that OFO and OIT are operating TVS for the BE-E Program in a manner consistent with requirements in current privacy compliance documentation, DHS/CBP policy, and U.S. law. Furthermore, a FIPPs-based analysis demonstrated that the CBP BE-E Program is operating in a privacy-protective manner. Based on our findings, the CBP Privacy Office makes the following recommendations:

Recommendation: As a best practice, OFO should continue to conduct periodic signage audits and continue to require that all POEs engaged in the collection of biometric information confirm the proper placement of privacy signage, as well as the provision of gate announcements as applicable depending on agreements with our commercial partners, annually; submitting audit results to the CBP Privacy Office for review.

Recommendation: Continue to provide regular messaging, through either the issuance of memorandums, training presentations, or muster notices, that U.S. citizens and otherwise exempt non-citizens are allowed to opt out of the collection of facial images under the BE-E Program and request alternative identity verification procedures.

[8] Only those complaints specifically indicating an issue or concern with the use of TVS, CBP's requirement that biometrics be provided by travelers, or a concern that U.S. Citizens were not afforded the opportunity to opt out of the collection were included as part of this review.

A. Transparency

Requirement: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

Review: The CBP Privacy Office reviewed available Privacy Compliance documentation associated with the BE-E Program and TVS, including the current and previous iterations of the PIA, various SORNs, and PTAs; public messaging regarding the BE-E Program; and available Privacy Notices, signage, informational tear sheets, and airline gate announcements provided at the point of collection. The CBP Privacy Office also reviewed the program's responses to the CPE Questionnaire and supporting information and documentation, such as a memorandum to the Ports related to the proper display of signage, and a public facing website[9] that describes the collection and use of facial images; as well as information from several formal and informal discussions with program staff.

Finding: Pursuant to DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information,"[10] CBP must be transparent in how it handles PII through various mechanisms, including PIAs, SORNs, public notices, and other means. The CBP Privacy Office found that the BE-E Program has been aggressively transparent in its publication of privacy compliance documentation and conducted PTAs and PIAs for all programmatic changes. CBP has completed thirteen PTAs and published six PIAs outlining various operational aspects of the BE-E Program through its development, as well as Technology Demonstration phases.[11] In an effort to consolidate the program under a single PIA, the CBP Privacy Office published DHS/CBP/PIA-056 Traveler Verification Service in November of 2018 and updated the appendices February 2021.[12] This PIA and its appendices provide a holistic overview of the entire BE-E Program and the new biometric facial comparison matching solution, TVS. This overarching PIA includes an assessment of its privacy risks and the agency's mitigation strategies.

The BE-E Program has prioritized transparency in its operations. Along with frequent privacy compliance publications, the program manages a robust public facing website[13] for travelers to learn more about the program. To satisfy the legal and policy requirements for notice

---

[9] To provide the public with a better understanding of what facial comparison technology is, why CBP uses it, and what the collection process generally looks like for individuals transiting a POE, OFO has launched a public-facing website (https://www.biometrics.cbp.gov/).

[10] See: DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information", at 3 (April 27, 2017), available at: https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[11] Previous iterations of TVS PIAs are available at https://www.dhs.gov/publication/departure-information-systems-test.

[12] See: DHS/CBP/PIA-056 Traveler Verification Service (November 2018), available at, https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

[13] https://www.biometrics.cbp.gov/.

and transparency, the BE-E Program has published a variety of privacy compliance documents, including multiple PIAs with frequent programmatic updates. This public facing documentation provides a detailed description how CBP collects, uses, maintains, and shares biometrics using TVS. CBP publishes frequent updates to the public-facing privacy documentation to account for new or updated biometric collections across the spectrum of transportation modes, including pilot efforts for new collections, technologies, and capabilities.

The CBP Privacy Office found that the BE-E Program provides notice at the time of collection through signage, message boards, tear sheets, and gate announcements. While the wording of the notice may differ slightly depending on the environment (air, land, sea), whether the data is being collected by CBP or one of its commercial partners, and when the collection was initiated, the messaging includes language related to the ability of U.S. citizens and otherwise exempt non-citizens to opt-out of the collection, how the collected image will be used, and how long the data will be retained.

BE-E Program personnel regularly visit POEs to ensure that privacy signage is in place, informational tear sheets are available, and that suggested notification language is used during boarding gate announcements. When onsite visits are not possible, the BE-E Program request photographs of the signage to ensure that proper notice is provided. The CBP Privacy Office also independently verified the display of signage, availability of tear sheets, and the conduct of TVS-related gate announcements during site visits at Atlanta Hartsfield International Airport (Georgia), Dulles International Airport (Virginia), John F. Kennedy International Airport (New York), Las Vegas Harry Reid International Airport (Nevada), Orlando International Airport (Florida), and Seattle-Tacoma International Airport (Washington).

Where airlines or airports are partnering with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP. CBP provides notice to departing travelers at airport departure gates and travelers arriving at ports of entry through message boards or electronic signs, as well as verbal announcements in some cases, to inform the public that CBP or a stakeholder will be taking photos for identity verification purposes. CBP also provides notice to the public that eligible travelers may opt out of the biometric process and request alternative identity verification procedures. CBP works with airlines, cruise lines, airports, and other port facilities to incorporate appropriate notices and processes into their current business models.

Upon request, CBP officers provide individuals with a tear sheet with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on CBP's biometric matching process, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information. Additionally, signage posted at CBP's Federal

Inspection Services (FIS) area provides information to travelers on search procedures and the purpose for those searches.[14]

In addition, to ensure transparency and increase public awareness of the BE-E Program, CBP has conducted outreach and provided briefings to members of the privacy, civil rights, and civil liberties advocacy communities to provide insight into agency operations, as well as specific information about how biometric data is collected and used in support of the BE-E Program. Program staff have supported advocacy engagement events, including through the provision of informational presentations. OFO, in coordination with the CBP and DHS Privacy offices, facilitated a tour of Orlando International Airport for the DHS Data Privacy and Integrity Advisory Committee (DPIAC), an independent board that provides advice to the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII. The tour focused specifically on the application and use of TVS. A similar demonstration was provided at Las Vegas Harry Reid International Airport to members of the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the Executive Branch tasked with ensuring that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.

In addition, to provide the public with a better understanding of what facial comparison technology is, why CBP uses it, and what the collection process generally looks like for individuals transiting a POE, OFO has launched a public-facing website.[15] CBP has launched a public awareness campaign to increase traveler knowledge of the BE-E program occurring when travelers arrive and depart airports and seaports. This campaign has appeared in national publications including The Economist and The Hill. Signs to promote public awareness have also been prominently displayed at dozens of airports and seaports.

Recommendation: As a best practice, the OFO BE-E Program should continue to conduct periodic signage audits and continue to require that all POEs engaged in the collection of biometric information confirm the proper placement of privacy signage, as well as the provision of gate announcements as applicable depending on agreements with our commercial partners, annually and submit audit results to the CBP Privacy Office for review.

This recommendation ensures continued collaboration between the operational BE-E Program and the CBP Privacy Office. While the BE-E Program can conduct site visits and request photographs to confirm sign placement, there is not currently an established or recurring assessment involving regular reporting to the CBP Privacy Office. Regardless of the auditing method, establishing a routine review of privacy messaging and reporting to the CBP Privacy

[14] Current text for signs and tear sheets are also available at: https://biometrics.cbp.gov/resources.
[15] https://www.biometrics.cbp.gov/.

Office will help guarantee that adequate notice is provided to travelers whose facial images are collected as part of the BE-E Program.

B. Individual Participation

Requirement: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Review: The CBP Privacy Office reviewed the CBP biometrics website and Privacy Notices/signage associated with the BE-E Program. The CBP Privacy Office also reviewed the program's responses to the CPE Questionnaire.

Finding: DHS Privacy Policy Guidance Memorandum 2017-01[16] requires that CBP involve the individual in the use of his/her PII, and where possible seek the person's consent for its collection, use, dissemination, or maintenance. The CBP Privacy Office found that the program provides substantial information about how data subject to this collection is used; and that the opportunity to consent is provided through their voluntary participation in the program.

As a biometric-based initiative, the involvement of individuals in the collection of information is paramount to the success of the BE-E Program. To increase awareness of, and participation in, biometric identity verification programs, CBP's biometrics.cbp.gov website provides members of the public with the ability to view detailed information related to how the collection of biometric identifiers occurs. The site also includes examples of the CBP biometric notification documents available for each of the different entry/exit environments (air, land, sea), in addition to privacy notices in other languages (Arabic, French, Japanese, Korean, Simplified Chinese, and Spanish). The website's privacy tab amplifies the transparent nature of CBP's traveler identity verification process, and includes a link to the agency's PIA, which provides an overview of TVS, the program's privacy risks, CBP's mitigation strategies for those risks, and the redress opportunities that are available for individuals that participate in the program. CBP has launched a public awareness campaign to increase traveler knowledge of the BE-E program occurring when travelers arrive and depart airports and seaports. This campaign has appeared in national publications including The Economist and The Hill. Signs to promote public awareness have also been prominently displayed at dozens of airports and seaports.

[16] See: DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information", at 3 (April 27, 2017), available at: https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

Though CBP has taken steps to provide more information to the public regarding its use of facial comparison tools, there is an inherent risk associated with it use, specifically the capture of images from individuals that may not be interested in participating in the program.

As is the case with many traveler-related programs within the Department, DHS Traveler Redress Inquiry Program (TRIP) serves as the single point of contact for persons who have inquiries or are seeking resolution regarding difficulties they experienced during travel at U.S. ports of entry. To date, CBP has received two redress requests related to the BE-E Program through TRIP. In both instances, the complaints were related to the traveler's referral for traditional processing because the TVS system was unable to accurately match them with previously collected images.

Additionally, the CBP Information Center has processed 15 cases/requests involving facial comparison technology or CBP's collection of facial images since the start of the 2020 fiscal year. The CBP Information Center functions as the primary point of contact for the public to ask questions; seek clarification on CBP-related regulations, requirements, programs, processes, and practices; and to make service-related comments, compliments or complaints. Members of the public can visit the CBP Information Center website (https://help.cbp.gov) for access to information related to imports and exports, as well as travel topics related to programs administered by CBP. Internally, the CBP Information Center serves as the coordination point for the entire agency in addressing concerns related to its interaction with the traveling public, industry, Congress, and other government entities.

Of the 15 cases/requests that the CBP Information Center processed in Fiscal Years 2020 and 2021 related to TVS and/or the collection of facial images, most submissions involved concerns about why the collection of facial images was necessary, that officers were not properly informed that U.S. citizens and otherwise exempt non-citizens may opt out of certain facial image collections, and improper conclusions that this program constituted a surveillance effort. While there were some claims that confirmed messaging related to the collection was present at the POE, there were others that outlined a lack of notice that the process is voluntary for U.S. citizens and otherwise exempt non-citizens and that there was not a sufficient explanation of how the data would be used. Had the cases involved more than just a request for information about the program or a complaint about the fact that the program existed, the request would have been forwarded to the appropriate DHS component for review and resolution. For example, all concerns involving potential civil liberties would be forwarded to the CBP Custody Support and Compliance Division (CSCD) and the DHS Office of Civil Rights and Civil Liberties (CRCL).

While the CBP Information Center is typically a venue for travelers to lodge complaints related to their experience with CBP, it is also a mechanism for members of the public to provide compliments following positive experiences with the agency. In reviewing CBP Information

Center related cases associated with the collection of facial images, one traveler's submission praised CBP its informative displays outlining the use of facial comparison technology.

> *Recommendation*: Continue to provide regular messaging, through either the issuance of memorandums, training presentations, or muster notices, that U.S. citizens and otherwise exempt non-citizens are allowed to opt out of the collection of facial images under the BE-E Program in lieu of more traditional processing.

Despite finding that the BE-E Program provides substantial notice to individuals about the collection of facial images through the posting of signage, gate announcements, and informational literature (tear sheets), CBP Privacy Office did find a number of concerns about the collection of this information submitted to the CBP Information Center. In some cases, U.S. citizens were concerned that they had not been adequately afforded the opportunity to opt for more traditional processing, as outlined on the signage available at the POE. The reissuance of previously issued memorandum on this, or the provision of new, regular, messaging will ensure that officers at the POEs understand the opt out provision and are able to more readily facilitate the alternative processing of those U.S. citizens that choose to opt out of the facial comparison technology for biometric entry-exit.

C. Purpose Specification

Requirement: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Review: The CBP Privacy Office reviewed the TVS PIA, BE-E Program PTAs, and the legal authorities associated with CBP's collection of biometric information.

Finding: The CBP Privacy Office found that the BE-E Program is operating within its authorities to collect facial images and other data in support biometric entry and exit operations. CBP has general statutory authority to collect and consider biometric data, including facial biometrics, as well as the authority to confirm the identity of travelers in carrying out its responsibilities. This authority includes 8 U.S.C. § 1365b, which directs the Secretary of Homeland Security to develop and fully implement an automated biometric entry and exit data system. The BE-E Program provides a mechanism for the efficient screening of travelers, as well as a system that provides adequate real-time information to CBP personnel in support of passenger processing activities. In accordance with the INA, as well as published Privacy Compliance documentation, information collected via TVS is only used to verify traveler identities and create entry and exit records. In addition to what is explicitly noted under 8 U.S.C. § 1365b, CBP further communicates its authority to collect biometrics and how they will be used in the TVS PIA.

The CBP Privacy Office also found that the BE-E Program office works regularly and collaboratively with the CBP Office of Chief Counsel (OCC) on the BE-E Program and its relevant authorities.

D. Data Minimization

Requirement: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Review: The CBP Privacy Office reviewed the TVS PIAs, PTAs, and SORN, screen shots of the TVS User Interface, the program's responses to the CPE Questionnaire, and held discussions with personnel from CBP's OIT.

Finding: The CBP Privacy Office found that the BE-E Program uses TVS to collect facial images from travelers to compare them against existing photographs collected during previous interactions with CBP, other U.S. government agencies including passport photos collected by the Department of State, and those provided in foreign government travel documents. CBP uses this pre-existing data, in combination with a vendor-provided algorithm to create templatized versions of the images. When CBP is aware that a traveler is entering or exiting the country, based on available Advanced Passenger Information System (APIS) information,[17] the templates are staged in a biometric gallery that facilitates faster matching and confirmation of the traveler's biographic information.[18] Images captured during the entry and exit processing are templatized and then compared against those maintained in the gallery.

OIT confirmed the templates are not stored outside the processing of a traveler's entry or exit. While images collected in support of TVS are generally purged immediately following confirmation that the traveler is a U.S. citizen, there are specific circumstances where an image may be retained for up to 12 hours as a result of network issues. CBP ensures that images of U.S. citizens are deleted within 12 hours of capture through the use of a cache time configuration on the cloud service where the images are maintained. Images of otherwise exempt non-citizens are deleted within 14 days. The BE-E Program verified there were no instances in which images of U.S. citizens had been retained for longer than 12 hours. TVS stores facial images of non-U.S. citizens for 14 days.

---

[17] The Advance Passenger Information System (APIS) is a widely used electronic data interchange system that allows carriers to transmit traveler data to CBP. APIS data includes passenger information that would be found on the face of a passport, such as full name, gender, and country of passport issuance. CBP requires the transmission of APIS data for commercial carriers arriving in or departing from the United States

[18] See DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018) for more information on biometric galleries, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

The CBP Privacy Office coordinated with OIT to review screenshots from the TVS User Interface (UI) to verify the retention limits. The Privacy Office chose a random date (April 22, 2020) and verified that collections associated with older encounters were not retained and confirmed all deletions occurred in accordance with the established retention schedule. Separate UI screenshots from April 21, 2021, showed that images and templates associated with encounters that occurred 14 days before the review was conducted were also deleted, confirming that the program is complying with established retention requirements.

Facial images for in-scope travelers[19] are also transmitted to the Department's Automated Biometric Identification System (IDENT)[20] and Homeland Advanced Recognition Technology System (HART).[21] All biometrics of in-scope travelers are transmitted to IDENT/HART as encounters and are retained for 75 years in support of immigration, border management, and law enforcement activities. Information retrieved from CBP systems to build traveler galleries are retained in accordance with the System of Record Notices and records retention schedules for the systems where the data is maintained.

E. Use Limitation

Requirement: DHS should use PII solely for the purpose(s) specified in the notice. According to the notices provided at the point of collection, facial images collected as part of the BE-E Program are used for identity verification purposes, to verify each person presenting a travel document for entry in the United States is the true bearer of that document, or to confirm an individual's departure from the United States. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

[19] There is the requirement to biometrically confirm the arrival and departure of "in-scope" travelers. An "in-scope" traveler is any person who is required by law to provide biometrics upon entry to and exit from the United States pursuant to 8 CFR 235.1(f)(1)(ii) and 8 CFR 215.8(a)(2). "In-scope" travelers include any alien other than those specifically exempt as outlined in the CFR. Exempt aliens include: Canadian citizens under section 101(a)(15)(B) of the Act who are not otherwise required to present a visa or be issued a form I-94 or Form I-95; aliens younger than 14 or older than 79 on the data of admission; aliens admitted A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply.

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

[21] See DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART) Increment 1 (February 24, 2020), available at https://www.dhs.gov/privacy-impact-assessments.

Review: The CBP Privacy Office reviewed the BE-E Program's responses to the CPE Questionnaire, public notices (including signage and verbal announcements made by commercial partners), a security assessment conducted by CBP, and SORNs associated with the systems where data used by the BE-E Program are maintained.

Finding: The CBP Privacy Office found that the BE-E Program is operating in accordance with DHS and CBP policy by limiting the use of collected biometrics to facilitate legitimate travel and enforce immigration laws, which include activities related to counterterrorism and immigration enforcement. While CBP does not submit images of U.S. citizens, biometric information collected from in-scope travelers are submitted to the DHS Office of Biometric Identity Management (OBIM) to create encounters in IDENT.

As noted in the TVS PIA, commercial partners are not permitted to retain or share photos that are captured in support of CBP's identity verification operations. At the time of this report, CBP has conducted six security assessments of commercial partners' biometric exit solution. Each review has confirmed the commercial partner is not storing photos after matching with TVS occurs. Though the TVS-partners initiative indicates that commercial partners may collect separate photographs consistent with their contractual relationships with the travelers for commercial purposes, there are no current commercial partners that have communicated an intent to collect images for their own uses.

F. Data Quality and Integrity

Requirement: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

Review: The CBP Privacy Office reviewed the TVS PIA, other available BE-E Program compliance documentation, the NIST's Performance Testing Summary of the NEC Facial Recognition Algorithm, and the program's responses to the CPE Questionnaire.

Finding: The CBP Privacy Office determined that the BE-E Program has implemented several review and assessment mechanisms designed to ensure that quality and integrity of collected facial images used by CBP in the processing of travelers.

To mitigate risks associated with biases against race,[22] ethnicity, age, and gender present in various biometric facial comparison algorithms, NIST conducted an evaluation of the algorithms used. The analysis found that there are currently no detectable biases within the algorithm that CBP employs. The assessment also found that match rates have continued to improve over time, with images collected from individuals from all regions of the globe performing relatively equally,

[22] As CBP does not collect race/ethnicity nor is this information included in the APIS manifest, citizenship is used as a proxy to conduct its analysis.

between 98.1% and 99.6% match rates. Similar improvements were found with regard to age, though middle-aged people (between 26 and 65 years of age) tend to have slightly higher match rates. Despite the minimally lower match rate for young (age 14-25) and old (age 66-79) individuals, age bias for CBP's algorithm is considered negligible, with matches less likely to occur 0.3% and 0.1% of the time for those travelers respectively. The assessment also indicated that algorithm bias related to gender was negligible, with women only 0.04% more likely to match than men.

The BE-E Program also conducts daily tests to determine whether the True Accept Rate (TAR)[23] and False Accept Rate (FAR)[24] meets key performance parameters. If tests show that the FAR or TAR is falling below acceptable rates, adjustments to the threshold are made. Consistent with the NIST guidelines, if the FAR exceeds 0.1%, CBP data scientists adjust the matching threshold.

To ensure continued high performance of its biometric facial comparison algorithm, CBP partnered with NIST to conduct an independent and comprehensive scientific analysis of CBP's operational face matching performance.[25] The analysis included a review of the impacts of traveler demographics and image quality on CBP's facial comparison technology and allows NIST to provide objective observations regarding CBP's matching algorithms, optimal thresholds, and gallery creations.

G. Security

Requirement: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Review: The CBP Privacy Office reviewed the TVS PIA, other available BE-E Program privacy compliance documentation, the TVS System Security Plan, the TVS System Privacy Plan, and the program's responses to the CPE Questionnaire.

Finding: The CBP Privacy Office finds that facial images collected in support of the BE-E Program are adequately protected from inappropriate access and use. TVS data is maintained in

[23] The True Accept Rate (TAR) is a statistic used to measure biometric performance when performing the verification task. It is the percentage of times a system (correctly) verifies a true claim of identity

[24] The False Accept Rate (FAR), is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. A conventional value for access control is for false positive rate of 1 in 10 000.

[25] NISTIR 8381: Face Recognition Vendor Test (FRVT), Part 7: Identification for Paperless Travel and Immigration (July 2021), available at, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8381.pdf.

a FedRAMP certified[26] cloud environment which meets the requirements of Office of Management and Budget (OMB) Circular A-130[27] and in some instances exceed the standards established in NIST 800-53.[28] TVS complies with all aspects of the Federal Information Security Modernization Act of 2015 (FISMA),[29] and has system security plans that have been approved as part of the Certification and Accreditation (C&A) process.

H. Accountability and Auditing

Requirement: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Review: The CBP Privacy Office reviewed the TVS PIA, other available BE-E Program privacy compliance documentation, and the program's responses to the CPE Questionnaire.

Finding: The CBP Privacy Office finds that the BE-E Program maintains effective oversight measures to ensure only authorized personnel have access to biometric data collected from travelers, and that data is only used in accordance with the DHS FIPPs.

As is required of all DHS employees, any CBP personnel, including contractors, with access to biometric data are required to complete annual privacy awareness training. The training is designed to raise employee's awareness of the importance of maintaining privacy in the workplace, and how to identify and safeguard PII. Additionally, access to TVS is limited and only possible after CBP personnel have completed a User Access Request (UAR) form, provided documentation of completed Privacy Awareness training, and have the approval of their supervisor. As a means of maintaining TVS, System Administrators review and update the list of approved users every month, ensuring that those that no longer require access are removed.

While these controls help to ensure only authorized users have access to data maintained in TVS, creating templatized versions of the biometric images collected in support of this program helps to ensure they cannot be used for unauthorized purposes. As noted in the TVS PIA, CBP creates biometric templates of each of the historical photos, as well as the newly-captured exit photos in order to secure the photos for matching and storage. In creating the template, the

[26] FedRAMP leverages NIST standards and guidelines to provide standardized security requirements for cloud services; a conformity assessment program; standardized authorization packages and contract language; and a repository for authorization packages
[27] See: OMB Circular A-130: Managing Information as a Strategic Resource, available at, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.
[28] See: NIST 800-53: Security and Privacy Controls for Information Systems and Organization, available at, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[29] See: Public Law 113-283, 128 Stat. 3073 (December 18, 2014), available at: https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.

biometric features or characteristics are extracted from an image by the TVS algorithm as numbers. In converting the image into a numeric template, the image is rendered useless outside of TVS. The process, and the way that the templates are represented, also makes it impossible to reverse-engineer an image from a template.

Templates are created for all images captured, as well as for the historical images that are used to populate the matching gallery. In both cases, the templates are deleted after the matching process concludes. For templates created from pre-existing photographs to support the matching gallery, deletion of the template occurs when the flight gallery is deleted, generally after the flight has departed. Templates created from the image collected at the time of arrival or departure are not stored, and the images they are based on are deleted within 12 hours for U.S. citizens and 14 days for non-U.S. citizens.

In the wake of the 2019 breach, CBP also implemented additional safeguards to ensure the security of biometrics systems and information, strengthening the agency's security posture where sensitive data is concerned. Specifically, CBP deployed cyber enhanced technology that facilitates audit tracking, logging, and enhanced encryption to further protect image data; restricted the use of removable media devices on systems collecting images; updated contractual, policy, and security requirements; and implemented enhanced usage of Data Loss Protection (DLP) and encryption practices across the enterprise. CBP also took steps to strengthen privacy protections in contracts and acquisitions language to ensure vendor compliance with security requirements; and provided recommendations for new language related to incidents involving contractors and contractor-operated systems to the DHS Privacy Office for inclusion in an update to the Department's Privacy Incident Handling Guidance (PIHG).[30]

[30] See: DHS 047-01-008: Privacy Incident Handling Guidance (December 4, 2017), available at, https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf.