Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies

Report to Congress

Homeland Security

U.S. Department of Homeland Security

Assistant Secretary for Legislative Affairs
U.S. Department of Homeland Security
Washington, DC 20528

August 30, 2019

Message from the Assistant Secretary for Legislative Affairs

I am pleased to present the following report, "Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies," which has been prepared by the Transportation Security Administration (TSA) and the U.S. Customs and Border Protection (CBP). This report is required by Section 1919 of the *FAA Reauthorization Act of 2018* (P.L. 115-254), signed into law on October 5, 2018.

The report describes CBP and TSA's development and implementation of biometric technology pilots. It includes assessments on the operational and security impact of biometric technology; potential effects on privacy with the expanded use of biometric technologies methods to mitigate privacy risks; methods to analyze and address matching performance errors; and special assessments on the biometric entry-exit program.

This report is being provided to the following Members of Congress:

The Honorable Roger Wicker
Chairman, Senate Committee on Commerce, Science, & Transportation

The Honorable Maria Cantwell
Ranking Member, Senate Committee on Commerce, Science, & Transportation

The Honorable Ron Johnson
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Gary C. Peters
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Bennie G. Thompson
Chairman, House Committee on Homeland Security

The Honorable Mike Rogers
Ranking Member, House Committee on Homeland Security

Please do not hesitate to contact us at (202) 447- 5890 if we may be of further assistance.

Respectfully,

CHRISTINE M. CICCONE
Assistant Secretary for Legislative Affairs

Executive Summary

TSA, CBP, travelers, and travel industry partners recognize that identity and vetting are critically important elements in the air environment. Travelers are repeatedly asked to prove their identity within the travel continuum. Governments and industry partners must repeatedly verify travelers' asserted identity at check-in, bag-check, security checkpoint, and at departure. Projected increases in air travel volume, combined with current infrastructure and operational constraints, underscore the need to automate current processes. Facial biometric technology has potential to modernize and streamline the process without sacrificing safety and security by reducing the reliance on manual identity verification processes.

At the direction of Congress, CBP developed a pilot biometric entry-exit program to aid in the identity verification of travelers upon entry into and exit from the United States. CBP and the Department of Homeland Security (DHS) invested in developing an identity as a service solution (IDaaS) that uses facial comparison to automate manual identity verification. This solution is called the Traveler Verification Service (TVS). The biometric entry-exit program is carried out through a privacy-by-design model and firmly situated within the DHS Fair Information Practice Principles.[1]

TVS offers a secure system that works quickly and reliably. It uses existing traveler data to build small galleries of faces associated with each departing flight and enables CBP and its partners such as TSA, select air carriers and airport authorities to simply take and submit a traveler's photo for identity verification. Live photos are compared against the correlating flight gallery[2] and TVS returns verification results in seconds. For travelers at the gate, this means the traveler's facial biometric can serve as a boarding pass. For industry partners, it can mean a convenient, efficient, and safe travel experience redefined by biometrics.

CBP established a rigorous process to review data associated with matching performance of biometric facial comparison. Although TVS true match rates can vary, CBP's analysis found a negligible effect in regards to biometric matching attributed to demographic variables. Further, because data privacy, protection, and mitigation of algorithmic or operational bias are prime concerns, CBP actively makes improvements while seeking to ensure there are no signs of bias,[3]

[1] See DHS Privacy Policy Directive 140-06, available at: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

[2] A pre-positioned "gallery" of traveler face templates is created using the biographic data from the airline manifest to retrieve the photos from government holdings, such as passports, visas, and previous entries.

[3] CBP measures and evaluates true match and non-match rates, as well as false match and non-match rates to provide a comprehensive understanding of system effectiveness in alignment with its mission. CBP analyzes for

and engages in a robust public dialogue on appropriate standards. CBP also engages in outreach with privacy advocates, the National Institute of Standards and Technology (NIST), and U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) to monitor performance and progress.

While TSA is not evaluating the use of facial comparison for law enforcement purposes, it is assessing its use for traveler identity verification as part of its mission to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA is using CBP's TVS for international travelers in this assessment process. In October 2018, TSA published the *TSA Biometrics Roadmap for Aviation Security and the Passenger Experience.*[4] The Biometrics Roadmap defines clear pathways to improve security, safeguard the Nation's transportation system, and accelerate the speed of action through smart investments and collaborative partnerships. In pursuing these goals, TSA seeks to use innovative collaboration concepts and solutions to enhance security effectiveness, improve operational efficiency, and yield a consistent, streamlined traveler experience. As it works to test the use of opt-in facial image collection and matching processes for additional populations, including TSA Pre✓® travelers and the general flying public, TSA is grounding its solutions in rigorous scientific study and analysis. TSA is committed to protecting traveler privacy as part of its biometrics effort, and as such, incorporates privacy considerations into each phase of biometric solution development.

Beginning in March 2017, CBP and TSA began evaluating the use of facial comparison at the security checkpoint through a series of multi-phased pilots. Early success on initial proof of concept testing in October 2018 encouraged TSA and CBP to explore the viability of expanded use of TVS at the checkpoint through data integration between TVS and TSA Secure Flight systems. Both agencies will continue to build on their efforts to evaluate the ways in which biometrics technology can improve the traveler experience. TSA and CBP are committed to enhancing security consistent with their homeland security missions and biometrics efforts, including facial comparison.

---

demographic biases in its biometric exit systems. No bias based on demographics has been statistically identified in its approach. However, operational and environmental conditions, such as lighting, show much greater correlation.

[4] https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf

U.S. Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies

Table of Contents

I. Legislative Language

This Report to Congress was compiled pursuant to Section 1919(c) of the *FAA Reauthorization Act of 2018* (P.L. 115-254), signed into law on October 5, 2018, which states in part:

> (c) REPORT REQUIRED.—Not later than 270 days after the date of enactment of this Act, the Secretary shall submit to the appropriate committees of Congress, and to any Member of Congress upon the request of that Member, a report that includes specific assessments from the Administrator and the Commissioner of U.S. Customs and Border Protection with respect to the following:
>
> (1) The operational and security impact of using biometric technology to identify travelers.
> (2) The potential effects on privacy of the expansion of the use of biometric technology under paragraph (1), including methods proposed or implemented to mitigate any risks to privacy identified by the Administrator or the Commissioner related to the active or passive collection of biometric data.
> (3) Methods to analyze and address any matching performance errors related to race, gender, or age identified by the Administrator with respect to the use of biometric technology, including the deployment of facial comparison technology;
> (4) With respect to the biometric entry-exit program, the following:
>
> (A) Assessments of— (i) the error rates, including the rates of false positives and false negatives, and accuracy of biometric technologies; (ii) the effects of biometric technologies, to ensure that such technologies do not unduly burden categories of travelers, such as a certain race, gender, or nationality; (iii) the extent to which and how biometric technologies could address instances of travelers to the United States overstaying their visas, including— (I) an estimate of how often biometric matches are contained in an existing database; (II) an estimate of the rate at which travelers using fraudulent credentials identifications are accurately rejected; and (III) an assessment of what percentage of the detection of fraudulent identifications could have been accomplished using conventional methods; (iv) the effects on privacy of the use of biometric technologies, including methods to mitigate any risks to privacy identified by the Administrator or the Commissioner of U.S. Customs and Border Protection related to the active or passive collection of biometric data; and (v) the number of individuals who stay in the United States after the expiration of their visas each year.
>
> (B) A description of— (i) all audits performed to assess— (I) error rates in the use of biometric technologies; or (II) whether the use of biometric technologies and error rates in the use of such technologies disproportionately affect a certain race, gender, or nationality; and (ii) the results of the audits described in clause (i).

(C) A description of the process by which domestic travelers are able to opt-out of scanning using biometric technologies.

(D) A description of— (i) what traveler data is collected through scanning using biometric technologies, what agencies have access to such data, and how long the agencies possess such data; (ii) specific actions that the Department and other relevant Federal departments and agencies take to safeguard such data; and (iii) a short-term goal for the prompt deletion of the data of individual United States citizens after such data is used to verify traveler identities.

II. Background

Biometrics are recognized as unique physical characteristics that can be used to identify a person. Physiological traits such as fingerprints, facial images, iris patterns, hand geometry, speech, and gait, are all examples of biometric indicators. Today, biometrics are commonly used to accurately identify a person or authenticate an individual's identity. The U.S. Department of Homeland Security (DHS) uses biometric information for a variety of mission purposes. For example, U.S. Customs and Border Protection (CBP) uses biometrics as part of its border security mission and under its mandate to establish and implement a biometric entry-exit system. As part of its mission to protect the Nation's transportation systems and to ensure freedom of movement for people and commerce, the Transportation Security Administration (TSA) is exploring the use of biometrics for identity verification for both traveler screening, and to enable access to airport sterile areas by airport workers.

Over the past decade, significant developments and improvements in biometrics technology have occurred. At the same time, the use of biometrics technology has also prompted concerns about accuracy, privacy, and security, among other issues. While CBP and TSA explore the use of biometrics consistent with their respective missions, they are mindful of those considerations as well as the need to build to and utilize enterprise biometric services offered through DHS's Office of Biometric Identity Management (OBIM).

A. CBP's Progress Toward a Biometric Exit System

CBP has used biometrics to verify the identities of foreign nationals entering the United States at air ports of entry since the mid-2000s. In recent years, it has also made significant progress towards achieving a biometric entry and exit solution mandated by federal statute and executive orders. Under existing laws[5] and Executive Order 13780,[6] CBP is required to implement measures to verify identities of travelers upon entry to and exit from the United States. After receiving the biometric entry-exit mission in 2013 and through the authorization of fee funds,[7] CBP accelerated the implementation of a capability to biometrically verify the identities of travelers arriving and departing the United States by air while facilitating travel processes.

In 2017, after several successful biometric pilots, CBP began vetting the Traveler Verification Service (TVS), a facial image matching service that uses biographic data to retrieve all associated traveler facial images from DHS holdings and segment them into smaller, more manageable data sets,[8] for use in the live environment. TVS uses the product of a fusion of

[5] *See, e.g.*, *Intelligence Reform and Terrorism Prevention Act of 2004* (Pub. L. No. 108-458, 118 Stat 3638 (2004)) and the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53, 121 Sat. 266 (2007)).

[6] https://www.federalregister.gov/documents/2017/03/09/2017-04837/protecting-the-nation-from-foreignterrorist-entry-into-the-united-states

[7] The *FY 2016 Consolidated Appropriations Act* (P.L. 114-113) funded the Biometric Entry-Exit Program through the authorization of up to $1B in fee collections on H-1B and L-1visa applications through FY 2025.

[8] For example, by flight, by cruise, or by frequent border crossers.

biometric and biographic information, enabling the biometric data to be the key to verify the traveler identity with the advance biographic data. The matching service compares the traveler's live photo to source images such as the travel document, enabling CBP to confirm the entry and departure of in-scope,[9] aliens. TVS was initially demonstrated at airports across the United States, as well as in the sea environment in 2017. CBP began piloting the capability at land ports of entry in the pedestrian environment in August 2018.

CBP's facial matching service is being leveraged to support biometric entry and exit processing for sea and land operations. Each travel mode offers unique challenges that require integrated solutions to mitigate any potential negative impacts to travel and trade. Biometric solutions must be thoroughly designed and tested to ensure that they are effective; compatible with expediting travel; can be integrated into existing infrastructure, systems, and processes; are not cost prohibitive, and do not put individuals' privacy at undue risk.

PROGRESS TO DATE

Processed more than 20 million travelers using facial comparison including:

- 10,749,134 arriving flights
- 3,422,909 departing flights
- 5,576,903 preclearance flights
- 600,728 flights through TSA checkpoints
- 250 cruise ships
- Biometrically confirmed over 17,840 foreign nationals who overstayed

Figure 1 Biometric Entry Exit Statistics (as of June 2019)

Air Entry and Exit

CBP envisions the facial matching service will significantly reduce the need to manually check paper travel documents by providing an automated process which can replace manual checks of travel document across the travel continuum. In 2017, CBP demonstrated TVS at eight international airports at boarding gates using CBP officers to process each traveler. CBP also partnered with JetBlue Airways, Delta Air Lines, British Airways, and Los Angeles International Airport (LAX) to evaluate biometric exit boarding integrated with stakeholder departure control systems. In Fiscal Year (FY) 2018, CBP's transformed entry process using facial comparison was reengineered and deployed in the air entry environment at 15 airports including four preclearance locations, with plans to expand further in 2019.

[9] An "in-scope" traveler is any person who may be required by law to provide biometrics upon entry into the United States pursuant to 8 CFR 235.1(f)(ii), or upon exit from the United States pursuant to 8 CFR 215.8. "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 Immigration and Nationality 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.

Prior to departure, the TVS creates a pre-positioned "gallery" of traveler face templates using the biographic data from the airline manifest to retrieve the photos from government holdings, such as passports, visas, and previous entries. During boarding, the stakeholder system takes a picture of the traveler. The TVS compares the picture against the gallery and provides a biometric match result.

Due to the success of CBP's stakeholder engagement strategy to date, CBP has received letters of commitment from 26 airports and airlines to begin implementation of biometric exit using CBP's matching service. CBP is actively working with each committed partner to implement biometric exit solutions. In FY2018, biometric air exit started at nine airports and ended at 16 airports. Total in-scope travelers exiting the country processed started at 40,000 monthly and ended FY2018 with 157,000 monthly. These numbers continued to grow steadily during FY2019, growing 54% since the beginning of the calendar year, with 548,000 being processed in the month of April 2019.

By 2022, CBP's goal is to deploy biometric exit to the top 20 airports, which account for more than 97 percent of departing commercial air travelers from the United States. CBP is actively working to expand stakeholder partnerships and adoption, prioritizing the highest volume of international airports and carriers to achieve the biometric air exit implementation goal. CBP continues efforts to consider innovative ways to utilize TVS with mobiles phones, tablets and watches. CBP will look to expand partnerships with international airports and governments and to further expand capabilities in preclearance locations to continually improve security and facilitation of traveler processes.

Sea Environment

Leveraging the investment in TVS for the air environment, CBP is partnering with the cruise industry to modernize traveler and crew inspections by implementing facial matching technology in the sea environment. Preparations are underway to apply the use of facial comparison technology in the debarkation (arrival) and embarkation (departure) points at seaports. These improvements will enable increased security and enforcement as well as facilitate traveler inspections.

Today, five major cruise lines are engaged with CBP to develop facial biometric processing supported by the TVS for closed-loop cruises.[10] Going forward, a focus on expanding integration with cruise partners will be implemented, focused initially on closed-loop cruises for debarkation. Through FY2020, CBP will seek to expand across closed-loop embarkation. Beyond FY2020, capabilities will be expanded to open-loop cruise routes.

Land Environment

[10] A closed-loop cruise is a term that refers to a cruise itinerary which begins and ends at the same U.S. location. An open-loop cruise is one that begins and ends in different ports, either departing from or arriving in the United States.

The Land Biometric Exit strategy focuses on implementing an interim exit capability while simultaneously investigating innovative technologies to reach the long-term goal of a comprehensive exit solution. CBP is actively piloting capabilities at the land border in both the pedestrian and vehicle environments to determine the best long-term approach for a comprehensive biometric entry-exit capability. Since September 2018, 139 impostors were identified on entry using the TVS capability in a land pedestrian environment. Details on the challenges of implementing biometrics in the land border are detailed in section VI, and CBP's strategy to mitigate those challenges are in section IV.

In late 2017, CBP began the initial implementation of an interim land exit approach to provide a capability for CBP to report the final departure from the United States of third-country nationals at land ports of entry.[11] The third country nationals' capability is a short-term solution that leverages the biometric exit mobile platform from the air environment and allows compliant in-scope travelers a means to biometrically report departure. Since January 2018, more than 180 mobile devices have been deployed to 74 land border ports of entry to support this initiative. CBP personnel have deployed to more than 50 locations to provide training courses for the mobile app to support these deployments.

CBP will continue to evaluate concepts of operation and technologies in the land environment to determine the final approach. Solutions being evaluated leverage the underlying TVS architecture in both the pedestrian and vehicle environments.

B. CBP and TSA Partnership to Evaluate Biometrics at the Checkpoint

In March 2017, CBP and TSA began evaluating the use of facial comparison at the TSA checkpoint for identity verification. In April 2018, the TSA Administrator and CBP Commissioner signed a policy memorandum promoting a collaborative approach to the continued development and use of biometric technology at airports.

The goal of the partnership is to enhance security and promote effective use of resources. CBP and TSA established multi-phased pilots involving volunteer international travelers. The first phase at John F. Kennedy International Airport (JFK) began in October 2017 to collect data and validate the technology. In the second phase at LAX in August 2018 and Hartsfield-Jackson Atlanta International Airport (ATL) in November 2018, TSA used CBP's TVS to test biometrics for identity verification in an operational environment. In the third phase, CBP and TSA will explore data-sharing and integration between biometric and traveler vetting systems. The goal will be to create a consolidated traveler identity verification that meets the operational needs of both agencies. In 2019, CBP and TSA plan to continue working on the necessary technical integration and pilot planning activities. The results of the pilot will help inform the rollout plans at TSA checkpoints.

[11] [11] DHS/CBP/PIA-026(a), *Biometric Exit Mobile Program* (June 29, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp026a-bemobile-june2018.pdf.

C. TSA's Exploration of Biometrics

TSA protects the Nation's transportation systems to ensure freedom of movement for people and commerce. The TSA Administrator's 2018-2026 Strategy[12] details the three strategic priorities that will guide the agency as it seeks to further enhance transportation security.

- **Improve security and safeguard the transportation system:** TSA will lead by example by strengthening operations through powerful and adaptable detection capabilities, intelligence-driven operations, and enhanced vetting.
- **Accelerate action:** TSA will build a culture of innovation that anticipates and rapidly counters the changing threats across the transportation system. TSA will develop its ability to make timely, data-driven decisions, and rapidly field innovative solutions.
- **Commit to our people:** TSA will foster a diverse, inclusive, and transparent work environment, establishing itself as a choice federal employer. TSA will use available tools and authorities to cultivate a skilled workforce equipped to meet the challenges of tomorrow.

Identity verification and traveler vetting are integral to TSA's multi-layered security processes and core security mission. The identity verification process ensures that the person seeking access to the airport sterile environment is the person who was vetted by TSA's Secure Flight against intelligence-driven watch lists, and receives the appropriate level of physical screening. Currently, TSA relies on a manual identity verification process through which Transportation Security Officers (TSOs) and, for checked baggage, airline employees, verify a traveler's identity by manually reviewing their boarding pass and a valid form of identification (ID). For photo ID documents, TSOs must visually confirm the photo on the document matches the traveler. Once a TSO confirms a traveler's identity, he/she direct the traveler to proceed to security screening based on their Secure Flight vetting status as it appears on the boarding pass. Automated facial recognition capabilities can play an important role, in increasing the effectiveness of this travel document checker (TDC) position at the checkpoint.

TSA is deploying Credential Authentication Technology (CAT) to increase security at checkpoints. CAT addresses ID fraud vulnerabilities by verifying the security features on a traveler's ID and boarding pass. CAT also provides automated access to real-time Secure Flight traveler vetting information at the checkpoint. In the future, biometrics will complement the capabilities CAT offers by enabling TSA to match the person's facial image against the facial image on file or on their ID.

In 2013, TSA established the TSA Pre✓® Application Program. Under this trusted traveler program, TSA conducts significant additional vetting of applicants; those individuals that TSA has determined are low risk are then eligible for expedited screening at participating U.S. airports. Members of the traveling public voluntarily pay a fee and provide their biographic and information and fingerprints to conduct the enrollment and vetting to check an applicant's criminal history, potential ties to terrorism, enrollment eligibility, and citizenship. As of September 2018, TSA has transitioned from single-factor biometric enrollment (fingerprints) to

[12] Available at: https://www.tsa.gov/sites/default/files/tsa_strategy.pdf.

multi-modal biometric enrollment (fingerprints and face), so that facial images can be used for identity verification.

In June 2017, TSA assessed, as a proof of concept, the use of biometric authentication technology to verify the identity of TSA Pre✓® travelers. As part of this proof of concept, TSA compared a fingerprint scanned using this technology with the fingerprint provided at the time of TSA Pre✓® enrollment. This proof of concept demonstrated the potential for biometrics to enhance security through increased assurance of traveler identity. It also underscored the need for additional work to explore other biometric technologies, such as facial images, and integrate those biometrics into airport checkpoint operations.

Additionally, in 2018, TSA conducted a three-week proof of concept at LAX using facial comparison to provide automated verification of identities at the TDC. This proof of concept was available to e-Passport[13] holders who volunteered to test the technology. Travelers scanned their e-Passports to verify the name on the e-Passport matched the name on the traveler's boarding pass. If it matched, the system extracted the traveler's digital photo from the e-Passport chip. The traveler was then prompted to complete a photo capture with a facial comparison camera. Facial comparison technology compared the e-Passport photo to the real-time photo and prompted the e-Gate to open if they matched. After the e-Gate opened, the travelers proceeded to the TDC; those who did not match were directed to the TDC officer. All passengers were required to complete the standard TDC process for manual identity and travel document verification, regardless of the e-Gate biometric matching results.

Recognizing the need for TSA to take a more comprehensive approach to biometrics, Administrator David Pekoske championed the development of the Biometrics Roadmap,[14] published in October 2018. The roadmap provides the following:

- Defines clear pathways to improve security, safeguard the Nation's transportation system, and accelerate the speed of action through smart investments and collaborative partnerships;
- Incorporates feedback gathered during more than 40 engagements with aviation security leaders from airlines, airports, and solution providers; and
- Includes feedback gathered from key government stakeholders, including TSA internal offices, DHS headquarters, and operational components.

[13] E-Passports contain an electronic chip that holds the same information that is printed on the passport's data page including a digital photograph of the holder. See https://www.dhs.gov/e-passports.
[14] Available at: https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

It also outlines four goals to achieve TSA's vision for biometrics.

Figure 2 TSA's Vision, Goals, Objectives, and Principles for Checkpoint Biometrics

Goal 1: In partnering with CBP on biometric technology pilots, TSA is exploring the feasibility of applying biometric solutions at the TSA checkpoint. While CBP and TSA mission requirements differ in some regards, CBP's biometric air exit program offers the opportunity to conduct joint operational pilot projects, collect data, refine solutions, and exchange data. TSA's partnership with CBP will also enable TSA to identify and examine technical, legal, and regulatory issues before broader deployment.

Goal 2: To further implement biometrics for TSA Pre✓®, TSA continues enhancing the trusted traveler experience for TSA Pre✓® travelers. As of September 2018, TSA is capturing photos for those who renew in person or who are enrolling for the first time in the TSA Pre✓® Application Program.

Goal 3: TSA will explore opt-in biometric solutions for additional travelers beyond international outbound and trusted travelers. An assessment of the appropriate authorities, privacy issues, and potential risks and benefits as it explores ways to improve the screening experience for standard (non-TSA Pre✓®) domestic travelers will be conducted. As TSA explores biometric solutions for additional travelers, it will conduct pilot projects and seek input from a diverse group of stakeholders. Additionally, TSA will continue to partner with DHS and interagency partners, including DHS Science and Technology (S&T) Directorate, and OBIM, as well as CBP, and the DHS Office of Privacy and DHS Office of Civil Rights and Civil Liberties, to evaluate biometric solutions for domestic travelers.

Goal 4: TSA will develop supporting infrastructure for biometric solutions that align with legal and policy authorities. TSA's biometrics efforts will also align with the DHS-wide transition to enterprise biometric services offered through OBIM's Homeland Advanced Recognition Technology (HART) system. Common standards will also allow TSA to establish assessment processes, making it possible to quickly evaluate security procedure changes, assess cybersecurity posture, develop qualified product and service lists, and implement audits and controls to ensure operations adhere to applicable laws, policies, and compliance authorities.

III. Operational and Security Impacts of Using Biometric Technology

Recognizing the important role that biometric technology can play in enhancing security and improving operations, CBP and TSA are methodically studying the impact of these technologies through a number of pilots and demonstrations. Though the operational and security factors that are driving the use of biometric technologies are distinct for both agencies, CBP and TSA's assessments are helping to refine biometric solutions and biometrics efforts throughout DHS.

On an average day, CBP processes more than one million travelers arriving at air, sea, and land ports of entry. Innovative technologies are being used to enhance a wide range of its operational capabilities. The use of biometrics, specifically facial comparison technology, assists CBP in confirming the departure of non-U.S. citizens and facilitates future processing at entry and exit. Through CBP's development of biometrics at entry-exit, it has found that biometrics are an effective tool in combatting the use of stolen and fraudulent travel and identity documents. The goal is to ultimately enhance identity verification while facilitating a more secure travel experience.

A. CBP Operational and Security Impacts

In addition to the responsibilities referenced in Section II B, CBP has the ongoing mission to inspect all incoming and departing travelers and conveyances to determine admissibility to the United States and enforce and administer U.S. immigration laws.

A key aspect of effective enforcement is the ability to discern individuals who are lawfully present in the United States from those who have violated their terms of admission. An effective immigration system requires an end-to-end process that collects exit data and matches that to entry data. Without exit data, there is no meaningful way to determine whether foreign nationals have overstayed their periods of admission.

Biometric data, when used with biographic data, allows CBP to confirm with greater assurance a traveler's true identity, ensuring the traveler matches the biographic identity that has been vetted through DHS databases. As biometric technology has evolved, the ability to use individual characteristics to confirm identity for all travelers, including U.S. citizens, is now a reality for all modes of transportation.

To implement a biometric entry-exit solution that is both operationally feasible and realistic, CBP established key parameters based on existing operational constraints and infrastructure limitations.

CBP's Key Strategic Parameters Table 1

Key Strategic Parameter	Description
Do not add another processing layer to known travel processes	Avoid a stove piped, independent approach by integrating biometrics into already existing travel processes.
Utilize existing infrastructure	The solution will work in existing port infrastructure for entry and exit processing.
Utilize existing business models	Leverage existing stakeholder (airline, cruise line) systems, processes, and business models.
Leverage current traveler behavior	Leverage traveler behaviors and expectations that require minimal new or unexpected steps for travelers.
Leverage existing data and IT infrastructure	Leverage existing traveler data, such as passport and visa information, and leverage existing government IT infrastructure as much as possible.
Utilize existing DHS enterprise biometric services, capabilities, and investments	Leverage and integrate with DHS Enterprise Services for shared biometric matching capabilities.

For the initial implementation of biometric exit solutions in the air environment, CBP is working in partnership with the air travel industry to lead the transformation of air travel using biometrics as the key to enhancing security and unlocking benefits, which will dramatically improve the entire traveler experience. The strategic benefits are described in the following table:

CBP Strategic Benefits Table 2

Strategic Benefit	Description
Improved business process	An enhanced entry-exit business process that integrates within existing government and stakeholder business models.
Stronger relationships	An environment that allows CBP and stakeholders to work together and that allows for further airline modernization.
A positive impact on inbound security and throughput	Enhanced inbound security and more efficient throughput.
Improved traveler experience	An overall enhanced traveler experience.
Improved data integrity	Utilize DHS enterprise biometric repositories provided to ensure accurate biometric identity records.
Enhanced visa overstay enforcement	Support the ID and tracking of visa overstays by closing information gaps associated with current exit reporting capabilities allowing for improved enforcement action.

CBP is transforming the way the agency identifies travelers by shifting the key to unlocking a traveler's record from biographic identifiers to biometric ones – primarily a traveler's face.

Pre-staging the existing traveler data upstream in the travel process enables all stakeholders to transform from manual and redundant processes to safer and automated traveler movement. CBP will continue to increase security by using a live facial biometric to match the traveler to advance traveler information, while also checking any existing fingerprints on file against the biometric watch list, which decreases dependency on less reliable paper travel documents, such as passports and visas. New facial comparison processes will enhance CBP's biometric capabilities alongside of the existing fingerprint processes.

CBP is partnering with the air travel industry and TSA to deploy a biometric air entry-exit solution that improves and streamlines the overall traveler experience. The four primary goals of this large-scale transformation is to make air travel more:

- **Secure** - Providing increased certainty as to the identity of travelers at multiple points in the travel continuum;
- **Simple** - Eliminating the need for physical document and boarding pass checks, as well as the collection of fingerprints;
- **Facilitative** - Establishing a clear and easily understood process that will reduce the potential for major "bottlenecks" within the air travel process; and
- **Compliant** - Employing a high integrity biometric entry and exit system that not only increases CBP's certainty as to the identity of travelers, but also more ably holds accountable those violating terms of admittance.

B. TSA Operational and Security Impacts

For TSA, biometrics can provide important benefits in air travel. TSA experienced a milestone year in 2018, screening a record setting 813.8 million travelers.[15] This amounts to more than 2 million travelers per day. TSA is already on track to exceed this in 2019. Like TSA, airlines, airports, and security regulators around the globe are faced with an ever-rising volume of air travelers to screen. In light of rising air travel volume and operational constraints, TSA must look to innovative technologies, like biometrics, to enhance security and efficiency while improving the traveler experience.

[15] https://www.tsa.gov/blog/2019/02/07/tsa-year-review-record-setting-2018

TSA evaluates potential changes to its aviation security programs and technology solutions through the lens of the Risk Mitigation Trade Space Framework.[16] The framework contains the following elements:

Figure 4 TSA's Risk Mitigation Trade Space Framework

- **Operational Efficiency** – What is the effect of a new security technology or procedure on operational footprint, wait times, and TSA's workforce staffing?
- **Security Effectiveness** – What is the effect of a new security technology or procedure on TSA's ability to detect, deter, or otherwise mitigate threats? How may adversaries shift their tactics in response to such changes?
- **Traveler Satisfaction** – What does the new technology or procedure do to improve the traveler experience?
- **Industry Vitality** – What, if any, is the economic impact of implementation? Is there an industrial base capable of supporting implementation or production of new systems?
- **Fiscal/Policy Issues** – What are the relevant issues at play and how will TSA address them?

Biometrics could potentially improve the traveler experience and open the door to innovative models of public-private cooperation between TSA and aviation industry stakeholders. That said, biometric solutions raise unique issues about privacy and accuracy that are addressed later in this report.

Operational Impacts – From an operational perspective, the introduction of biometrics to the TSA checkpoint will most directly affect the TDC position. This position is staffed by a TSO who gathers boarding passes and identity credentials from each traveler in the queue to quickly perform a series of screening steps (see *Figure 5*).

The planned use of CAT will help automate *steps 1, 3, and 5*. The automation of these tasks will increase TSA's confidence in the validity of credentials used to travel and the accuracy of the biographic data used to conduct Secure Flight vetting. CAT will also mitigate the threat of altered and counterfeit IDs, reduce the need for boarding passes at the checkpoint for many travelers (eliminate *step 4*), and automatically look up a traveler's vetting status in near-real time from Secure Flight's vetting engine.

The use of biometrics (for example, facial comparison) will also largely automate *step 2* by increasing assurance of identity beyond what is currently possible in a manual, human-based

[16] Strategic Five-Year Technology Investment Plan for Aviation Security: 2015 Report to Congress.

operation.[17] Specifically, biometrics will help mitigate threats posed by impostors using valid credentials for fraudulent purposes at the checkpoint (see subsection on *security impacts* for more detail).

For *step 6*, further integration of access control solutions with credential authentication and biometric technologies will help more fully automate the TDC process.

The development of this biometrically enabled solution will allow TSA to better secure access to the airport sterile environment and evaluate how to potentially reinvest valuable officer resources to other screening tasks. The automation of TDC functions will create a need for a 'TSO resolution' *step 7* in the event of system issues (for example, biometric match error, and alarm resolution).[18] In the future, TSOs will oversee biometric operations at the TDC to help travelers use the technology and address issues as they happen. TSOs will continue to provide important security safeguards, including directing travelers to the correct screening lane based on the travelers vetting status.

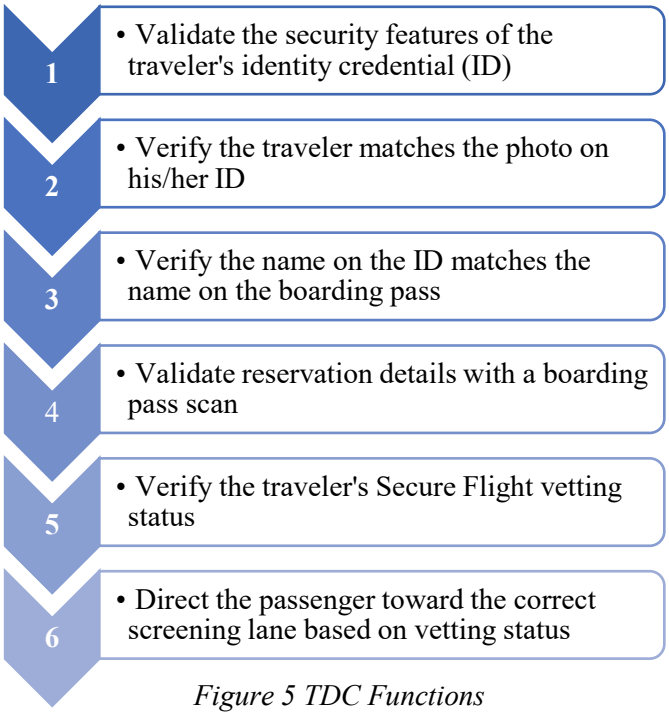

Figure 5 TDC Functions

Given the diversity of airports across the United States and their unique layouts, the operational placement and use of a fully integrated biometric solution will vary from facility to facility. For example, the use of an automated, biometric solution at a relatively small checkpoint may result in faster TDC processing times. However, the throughput of the checkpoint may be largely unaffected because a faster TDC process would merely shift traveler volume from the queue into the screening lane itself. A screening lane can only operate as fast as its slowest piece of transportation security equipment. This result underscores the need for continued investment across the entire checkpoint security enterprise.

On the other hand, at larger checkpoints with more lanes the operational efficiencies of an automated, biometric TDC may be greater. This would especially be true if the ratio of biometrically enabled TDCs to screening lanes was higher than the ratio of manual or CAT TDCs to screening lanes, thus freeing up TSO resources that could be used elsewhere. TSA will continue to explore this area as it tests checkpoint biometric solutions.

[17] Except for a relatively small number of "super-recognizers," human beings are generally outperformed by facial comparison technologies, especially when presented with the faces of persons not familiar to them such as the thousands of travelers a TSO greets and processes each day. See: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0150036

[18] Per initial modeling conducted by the Homeland Security Systems Engineering & Development Institute (HSSEDI), keeping match error rates low through the use of reliable and accurate biometric systems and ensuring the use of swift error resolution procedures will be key to maintaining and improving checkpoint throughput.

In summary, the operational efficiencies TSA could gain from integrated biometric solutions may be different depending on airport facility layouts, sizes, checkpoint lane counts, and traveler volumes. New procedures and robust workforce training will be required to maximize the operational benefits of biometric solutions.

Security Impacts – TSA uses a multi-layered, risk-based approach to securing the Nation's transportation systems. Today, during the airline reservation process, the traveler provides their first name, last name, date of birth, gender, and, if applicable, known traveler number, or DHS redress number. The airline transmits this information to TSA's Secure Flight system for vetting against intelligence-driven watch lists. The result of this vetting process, known as the Boarding Pass Print Result, is sent to the airline and encoded on the traveler's printed or mobile boarding pass.

When the traveler arrives at the checkpoint, the TSO must quickly perform a series of complex tasks (see *Figure 6*) using a variety of tools. TSOs assess whether the presented ID credential is authentic, determine whether the traveler matches the picture on their ID credential, decide whether the name on the boarding pass matches the name on their ID credential, distinguish between various forms of ID (state driver's licenses, passports, and government IDs, among others), validate the boarding pass, and direct the traveler to the appropriate level of screening based on their Boarding Pass Print Result.

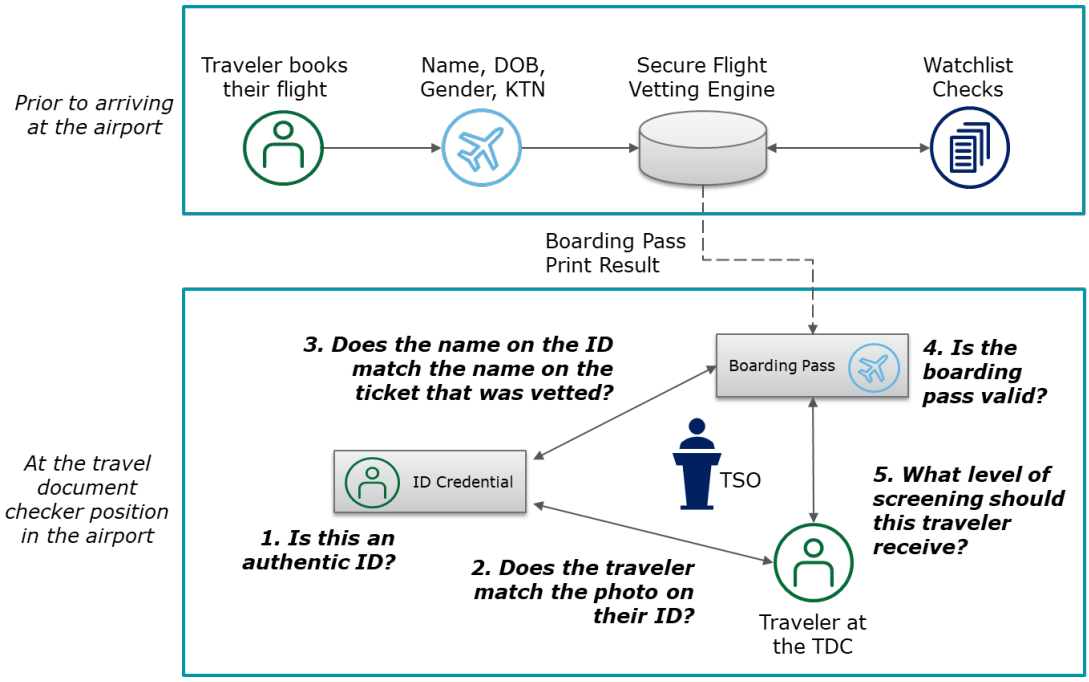

Figure 6 Systems and Operational View of Current TDC

Using an integrated, biometric TDC solution (see *Figure 7*), TSA can automate certain repetitive tasks and enable the system to verify the traveler's identity using the facial image and biographic information encoded on the ID or through the use of previously enrolled biometric and biographic data (for example, Trusted Traveler information). This technology will help

eliminate human errors and biases in face matching, lower TSA's reliance on the boarding pass, and enable a near-real time connection to TSA vetting systems for up-to-date results.

This model shifts the burden of the security decision onto the system while reducing TSO burden of repetitive, manual face comparisons and name matching between travel documents. Automating this process will enable TSOs to focus on the operation of the systems and intervene as needed to resolve problems or process travelers who cannot or do not wish to use the biometric system.[19]

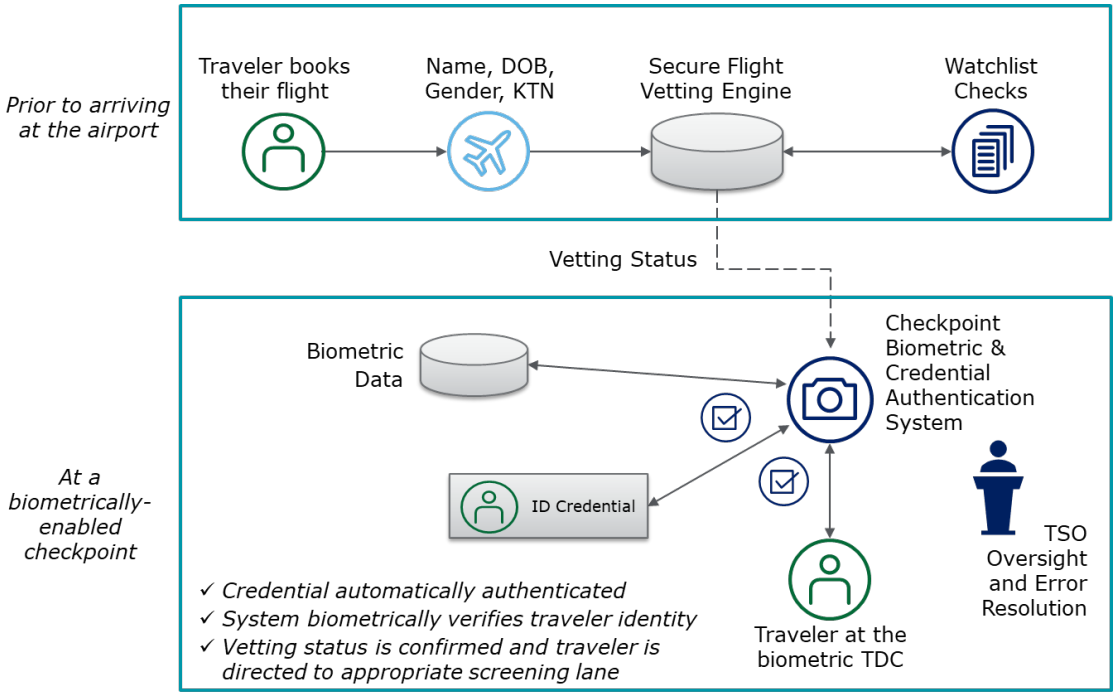

Figure 7 Systems and Operational View of Biometric TDC

Applying a biometric TDC to TSA Pre✓® and standard lanes would measurably increase security effectiveness and deter adversaries, or force a shift in their tactics. For example, individuals hoping to avoid detection using a fake ID or impostors using an authentic, stolen ID would be prevented from gaining access to the sterile area of the airport. In addition, integrated biometric solutions will help ensure individuals receive the correct level of screening based on their vetting status; making it more difficult for adversaries to avoid higher levels of screening by falsifying their identity.

While the rate of adversaries attempting to gain access to the checkpoint is difficult to determine, TSA can look to intelligence estimates and the experience of other organizations that use similar biometric solutions. CBP, for example, has used biometric facial comparison technology to identify more than 130 impostors trying to gain entry through air and pedestrian environments. Integrating biometrics into the checkpoint will enable TSA to further strengthen its security

[19] For example, minors under age 16 without state-issued driver's licenses would still be processed using traditional boarding pass scans. Travelers who opt out to a biometric experience will also require TSO assistance to proceed into the screening lane.

baseline, more effectively deter and detect bad actors, and better measure performance of security measures against adversaries trying to gain access to the airport sterile environment.

IV. Potential Effects on Privacy and Mitigation Methods

As they evaluate biometric technologies, CBP and TSA are committed to protecting travelers' information and privacy. In accordance with Office of Management and Budget (OMB) Directives 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*,[20] any use of personally identifiable information (PII), including use of facial comparison technology, requires a thorough analysis of its privacy impact through a Privacy Impact Assessment (PIA). Both CBP and TSA have submitted and published a number of PIAs on related pilots and programs to the DHS Privacy Office for adjudication and publication. DHS PIAs use the Fair Information Practice Principles (FIPPs) to assess and mitigate any impact on an individual's privacy. These principles are rooted in the *Privacy Act of 1974* and govern the use of PII.[21] The FIPPs help guide CBP and TSA as they seek to protect privacy and improve the traveler experience while gaining the operational and security benefits of biometrics technology.

TSA and CBP collaborate regularly with their respective Privacy Offices and DHS's Privacy Office. On September 11, 2017, the DHS Privacy Office commissioned the DHS Data Privacy and Integrity Advisory Committee (DPIAC) to advise the Department on best practices for the use of facial comparison technology. CBP briefed the DPIAC in September 2017, May 2018, and July 2018, when CBP provided a tour of biometric entry and exit operations at Orlando International Airport, and again in December 2018. The DPIAC published its report 2019-01 of the *DHS DPIAC: Privacy Recommendations in Connection with the Use of Facial Recognition Technology*,[22] on February 26, 2019. CBP has implemented, and is working to implement many of the DPIAC recommendations. CBP also met with privacy and civil liberties advocates twice since 2017 to discuss the biometric entry-exit program, including technical demonstrations, the future biometric vision, privacy and security protections, notice to the public, retention policies, and alternative screening procedures. Each meeting included a lengthy question and answer session. Similarly, in August 2019, TSA held a privacy roundtable with privacy and civil liberties groups to discuss its exploration of biometrics technology.

It also noted that "it is critical for the success of the Biometric Exit Program and/or other biometric programs that data intended to be used only for screening purposes is not further transferred, shared, or used for other purposes, including without limitation private-sector purposes (e.g. marketing) or other government purposes (e.g. law enforcement or intelligence purposes)." The DPIAC's detailed recommendations will be particularly helpful as TSA and CBP consider the privacy impacts of biometrics technology.[23] For instance, TSA and CBP consider issues such as timely and transparent notice; alternative screening processes; data

[20] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf
[21] https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf ; see: DHS Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, available at: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.
[22] https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf
[23] https://www.dhs.gov/publication/dpiac-recommendations-report-2019-01

minimization; reliability testing; data quality and integrity; accuracy; and accountability and auditability of facial comparison technology. Both agencies will address the FIPPs in their biometric technology efforts and associated privacy compliance documentation, to ensure the protection of personal information at all stages of the information lifecycle.

A. CBP Approach to Mitigating Privacy Impacts

CBP is fully committed to protecting privacy and ensuring the integrity of its facial comparison matching service. In developing and expanding the use of the TVS, CBP is implementing a privacy by design[24] approach to ensure that privacy protections are embedded into its use of facial comparison technology. CBP employs four primary safeguards to secure the data, including secure storage, brief retention periods, irreversible biometric templates, and strong encryption during data storage and transfer.

CBP complies with the requirements of the *Privacy Act of 1974*, as amended, the *E-Government Act of 2002*, and Departmental and government-wide policies governing the collection, use, and maintenance of PII. As with other biometric collections, facial comparison poses privacy risks that are mostly mitigated. CBP's phased deployment has illustrated the success of the use of facial comparison technology in a variety of operational scenarios, meeting CBP's business requirements while requiring minimal infrastructure investments and space redesign as well as minimal impacts upon travelers. Additionally, the approach has allowed CBP to ensure that biometrics are collected, maintained, and used consistent with privacy law and best practices. CBP analyzes the privacy impact of its collection, use, dissemination, storage, and sharing of PII through the lens of the DHS FIPPs as described above.[25] The eight FIPPs principles, rooted in the tenets of the *Privacy Ac*t, have served as the framework for privacy policy at DHS for more than a decade.

When a traveler presents himself or herself for entry, exit, or at a TSA security checkpoint, the traveler will encounter a camera connected to the biometric cloud matching service via a secure, encrypted connection. The biometric matching service converts the live photos into secure templates and matches them against templates of gallery images, which travelers have already provided to the U.S. Government for travel purposes. The templates cannot be reverse engineered to reconstruct the photo. Finally, CBP does not share any photos with travel stakeholders, but rather provides the travelers and partner airlines with the results of the biometric match (match or no-match) through a response message data value. In implementing biometric matching through the TVS, CBP is simply replacing the existing document checks with a biometric facial comparison process, which will greatly reduce the need for travelers to continually present identity documentation at multiple stops along their journey.

---

[24] *See* DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), *available at* www.dhs.gov/privacy.
[25] Additionally, the DHS Privacy Office conducted a Privacy Compliance Review of CBP's Southwest Border Pedestrian Exit Field Test that resulted in 10 recommendations to improve the privacy of individuals' biometric information, including facial and iris images. Available at: https://www.dhs.gov/sites/default/files/publications/SW%20Border%20PCR%20report%20FINAL%2020161230.pdf.

CBP provides transparency and general notification to the public through program information, such as frequently asked questions, available on the CBP website at www.cbp.gov/biometrics, and the TVS Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) published at www.dhs.gov/privacy.[26] The PIAs and SORNs for the TVS and its predecessor projects explain all aspects of CBP's biometric entry-exit programs, including policies and procedures for the collection, storage, analysis, use, dissemination, retention, and deletion of data. These PIAs and SORNs describe in detail CBP's approach to ensuring both the processes and systems integrate controls to mitigate privacy risks.

Following the DHS FIPP of transparency, CBP works closely with airline, airport, and cruise line partners to incorporate notifications and processes into their current business models, such as gate announcements or visible signage that explain the facial matching process and alternative inspection procedures. If processes or procedures change, CBP will update these channels to ensure all outreach material is current and clear for the traveling public. Because facial comparison can be performed quickly with minimal instruction and with a high degree of accuracy, the approach implemented represents the best operational means of verifying the identity of the traveler, and the data is collected in a manner perceived as less invasive to the traveler. Facial comparison requires no actual physical contact to collect the biometric data, and there is less risk of the loss of traveler documents that contain the date of birth and other sensitive PII.

Prior to admission into the United States, CBP must ensure that each traveler is a U.S. citizen, lawful permanent resident, or is otherwise an alien eligible for admission, and that the traveler is not attempting to import any merchandise in violation of U.S. laws. Similarly, CBP officers may inspect travelers departing the United States in order to create exit records and as required for law enforcement operations. The website www.cbp.gov/biometrics, along with signage, verbal announcements, tear sheets, and the TVS PIA contain details on the current biometric entry-exit process, including alternative procedures. In accordance with the FIPP of individual participation, a U.S. citizen and otherwise exempt aliens[27] may notify either the CBP officer or the airline boarding agent that he or she would like to opt out at the time of boarding and, instead, present credentials for a manual identity verification using their travel document. In adherence to the FIPP of purpose specification, CBP stipulates that PII collected through the biometric entry-exit program be used primarily to verify that the traveler attempting to board the flight or cross the border is, in fact, the rightful bearer of the travel document he or she is presenting.

Throughout its history, CBP has maintained productive partnerships with the travel industry, where the flow of PII between entities is well-defined in law and regulations. In line with the FIPPs, data minimization and use limitation, CBP has taken noteworthy steps to protect privacy,

---

[26] *See* DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), *available at* www.dhs.gov/privacy. www.dhs.gov/privacy. The SORNs associated with CBP's Traveler Verification Service are: DHS/CBP-007 Border Crossing Information, DHS/CBP-021 Arrival and Departure Information System, DHS/CBP-006 Automated Targeting System, DHS/CBP-011 U.S. Customs and Border Protection TECS.

[27] Certain aliens are exempt from any requirement to provide biometrics upon entry into the United States pursuant to 8 CFR 235.1(f)(ii), or upon exit from the United States pursuant to 8 CFR 215.8.

such as its commitment to prohibit the sharing the photos captured and matched through the TVS with CBP industry partners. Only the results of the "match/no-match" determination are shared. In fact, CBP's business requirements for partner airline and technology vendors do not permit the retention of photos for commercial purposes, following transmittal to CBP for matching. In addition, TVS only utilizes the irreversible biometric templates of source and newly-captured photos for matching and uses a unique identifier[28] to disassociate the biographic information associated with the new facial images.

While CBP does not retain U.S. citizens' images submitted as part of the traveler verification process,[29] photos of foreign nationals (and those dual national U.S. citizens traveling on foreign documentation) are retained for up to 14 days in secure systems to confirm traveler's identities, evaluate the technologies, and to assure continued accuracy of the algorithms. In addition, CBP transmits facial images for in-scope travelers to the DHS Automated Biometric Identification System (IDENT) for retention as the traveler's biometric encounter with CBP. For U.S. citizens, only a confirmation of the border crossing and the associated biographic information is retained.

In line with the FIPP of accountability and auditing, the CBP Privacy Office will conduct a CBP Privacy Evaluation by the end of calendar year 2019 to ensure that all parties, including airlines, airport authorities, and cloud providers, are in compliance with the privacy protections described in the TVS PIA. The results of the evaluation will be shared with the DHS Privacy Office.

B. TSA Approach to Mitigating Privacy Impacts

TSA is committed to protecting traveler privacy and ensuring the traveling public's trust as it modernizes identity verification through its exploration of biometric technology. TSA will comply with DHS privacy policy throughout each phase of TSA's biometric solution development – from initial design to implementation. Solutions will be designed to secure data as it is collected, stored, and transmitted between systems to protect both travelers and system integrity.

TSA recognizes that biometric technologies, particularly facial comparison, pose unique privacy concerns with respect to privacy and passengers' civil rights and civil liberties. There is significant risk to individuals should the facial images be compromised or used for purposes beyond those specified for its collection. There is also a risk to both individuals and transportation security in the event that the biometric technology is not sufficiently accurate. To mitigate these risks, TSA will evaluate issues such as:

- Robust notice of facial comparison deployment for traveler screening;
- Meaningful choice of screening choices for the traveler;
- Robust cyber-security measures to protect traveler data from collection through transmission to receipt; and

[28] The unique identifier is generated by either the travel agent, travel website hosting service, or the airline at the time of the reservation. It is comprised of a sequential number (which is only valid for the particular airline and the specific flight), plus the record locator, a six-digit code used to access additional information about the traveler.
[29] Photos of U.S. citizens are held in secure CBP systems for no more than 12 hours after identity verification, in case of an extended system outage.

- Limitation on the use of the facial images to those necessary for transportation security, consistent with the Privacy Act.

TSA will integrate privacy protections as it continues to partner with CBP on biometrics for international travelers, implement new biometric capabilities for TSA Pre✓® travelers, and explore the expansion of biometric collections, such as use of facial images, to additional domestic travelers. TSA will also adhere to DHS privacy policy in its adoption of new biometric-based vetting solutions for non- traveler groups such as aviation workers, law enforcement officers, and crew members.

Privacy and Facial Comparison for International Travelers

Since beginning to explore the use of facial comparison technology for traveler identity verification, TSA has taken steps to provide notice to the public about its efforts, assess privacy risks, and establish strategies to protect traveler privacy. The challenge of traveler identity verification through facial comparison for TSA is significant for international and domestic travelers for whom established, government-owned facial image databases do not exist. In comparison of this challenge, TSA engaged in several pilots involving international travelers. For instance, in January 2018, a PIA was published for a three-week proof of concept at LAX using passports.[30] The proof of concept was to validate the use of facial comparison technology to automate identity verification during the TDC process.

TSA compared the facial images of aviation passengers with e-Passports on outward-bound international flights and who voluntarily entered the screening checkpoint through automated electronic security gates or "e-Gate." The e-Gate device captured an image of the passenger's face and compared it to the biometric image in the passenger's e-Passport. The e-Gate attempted to replicate the function of the TDC and authenticated the passenger's e-Passport and boarding pass.

Additionally, privacy protections have been embedded in TSA's partnership with CBP on facial recognition pilots. These pilots took place in international terminals at a select number of airports to limit biometric collection to travelers on international flights. They enabled both agencies to collect data, refine solutions, and exchange information on the operational performance of facial comparison technology. Privacy compliance documents for each of these pilots have analyzed the potential effects on privacy and identified methods to lessen privacy risks.

In the first phase of the partnership, which took place in October 2017, TSA and CBP conducted an operational pilot at JFK to test the ability of CBP's TVS to match traveler identities against galleries of pre-staged photos at the TSA checkpoint. The second phase consisted of a pilot at LAX, which tested the TVS with a larger gallery and enhanced automation, from August to October 2018. Additionally, in November 2018, TSA, CBP, and Delta Air Lines began testing

[30] https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-046-tdcautomationusingfacialrecognition-january2018.pdf

biometrics for identity verification at Terminal F at ATL. CBP published PIAs on each phase of the TVS pilot.[31]

Privacy and Biometric Solutions for TSA Pre✓® Travelers and Additional Populations

TSA is using biometrics to modernize the trusted traveler experience for TSA Pre✓® travelers. For first-time enrollees or for individuals renewing their membership in that program in person, TSA started capturing facial images to help verify identity. At this time, a facial image is not required for individuals who renew their TSA Pre✓® Application Program membership online.

TSA will also evaluate the possibility of allowing additional trusted travelers to access the TSA Pre✓® lanes (for example, members of the Department of Defense), as well as the general flying public to opt in to biometric screening and verification. However, before making biometric solutions available to these travelers, TSA will work with OBIM and DHS oversight offices, including the DHS Privacy Office and the Office of Civil Rights and Civil Liberties to evaluate options, conduct pilots, and to ensure compliance with privacy law and policy and civil rights and civil liberties requirements.

In any biometric technology solutions involving the collection, maintenance, use, or dissemination of PII, TSA will be transparent by notifying the public and explaining the steps the agency is taking to safeguard individuals' information. In its development of biometric technologies for additional populations, TSA will comply with Section 208 of the *E-Government Act of 2002*, Section 222 of the *Homeland Security Act of 2002,* and DHS' privacy compliance process. As such, TSA will conduct appropriate privacy threshold analyses, PIAs, and system of records notices when considering the use of biometric solutions with potential privacy impacts. TSA will also comply with applicable TSA, DHS, and Office of Management and Budget policies and authorities governing the handling of PII.

TSA will comply with law and DHS privacy policy related to the use of facial comparison technology for identity verification such as notice to travelers, opt-in policies, consent protocols, specific use limitations, and alternative screening procedures for travelers that do not wish to provide their facial image for identity verification purposes. Consistent with information technology security policies and authorities, TSA will also develop biometric solutions that meet cybersecurity protocols so that data is protected at all stages of the information lifecycle. Additionally, public education and outreach will be conducted to provide awareness of the agency's future biometrics efforts.

Stakeholder Engagement on Privacy

As part of its commitment to protecting traveler privacy in the use of biometrics technology, TSA will continue to:

- Engage with non-governmental stakeholders to obtain input on best practices for protecting privacy;

[31] https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf

- Coordinate with internal TSA offices, DHS Headquarters, oversight entities and interagency partners to track compliance with privacy authorities and requirements, develop privacy-protective policies, and appropriately manage identified privacy risks;
- Seek information and feedback from industry, privacy groups, academic institutions, and other privacy professionals and research organizations as it considers the expansion of biometrics solutions to increase to increase security and streamline the passenger experience; and
- Share information with key stakeholders on its development of biometrics technology capabilities.

V. TSA Methods to Analyze and Address Matching Performance Errors

While TSA has been using fingerprints since 2004 to conduct security threat assessments—including checks on an applicant's criminal history, potential ties to terrorism, and citizenship—the use of biometrics to verify traveler identity has begun only recently. As of September 2018, the TSA Pre✓® Application Program has transitioned from single factor enrollment (fingerprints) to multi-modal biometric (fingerprints and facial image) enrollment. See Section II.C for an overview of TSA's biometric testing efforts to date.

TSA's exploration of the use of biometric data, namely facial images, as a means of facilitating secure travel is coming at an ideal time in the biometric industry. According to the most recent National Institute of Standards and Technology (NIST) Face Comparison Vendor Test, facial verification algorithms have become significantly more accurate over the 2013-2018 period. The NIST Interagency Report 8238 states:

> While the industry gains are broad—at least 28 developers' algorithms now outperform the most accurate algorithm from late 2013—there remains a wide range of capabilities. With good quality portrait photos, the most accurate algorithms will find matching entries, when present, in galleries containing 12 million individuals, with error rates below 0.2 percent. The remaining errors are in large part attributable to long-run ageing and injury.[32]

According to NIST, these gains have been largely facilitated by a revolution in algorithm development, fueled by new machine learning approaches. Whereas algorithms of five years ago may have struggled to match images that differed in pose, illumination, and facial expression, today's algorithms are increasingly tolerant of such variations in image quality. Indeed, improvements to the technology are being made in months rather than years.

Despite these gains, however, facial comparison systems are shadowed by reports of variable performance across demographic characteristics; namely race, age, and gender.[33] Much of the discussion has focused on the ability of various facial comparison algorithms to accurately process younger subjects, female subjects, and subjects with darker skin. Indeed, a 2019 article published by DHS S&T and informed by testing conducted in 2018 at S&Ts Maryland Test Facility (MdTF) found evidence of some variation in facial comparison performance along

[32] *See* NIST Interagency Report 8238, available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf
[33] TSA does not collect data on traveler race, ethnicity, or skin color for the purposes of making security and screening decisions; however, TSA may collect such data – in accordance with standard test protocols – during operational testing to ensure systems perform accurately under operational conditions.

demographic lines.[34] Interestingly, however, this performance variation was not solely based on the face comparison algorithm, but resulted from an interaction between the matching algorithm and image acquisition hardware.[35]

S&T tested 11 commercially available facial image acquisition systems using a demographically diverse population of 363 volunteer subjects.[36] The live images ("probes") gathered by each system were matched against historical and same-day enrollment images using a leading commercial algorithm for facial comparison. The variation in facial matching performance across different image acquisition systems versus when images are matched against a single, industry-leading algorithm suggests the hardware used to capture the probe image significantly affects matching accuracy.

As a result, using a superior biometric acquisition system capable of capturing higher quality facial images may significantly reduce or even eliminate performance differences along demographic lines. Logically, it follows that a lower quality acquisition system can increase the likelihood of performance variation along demographic characteristics. This key finding will influence TSA's testing, development, and potential procurement of checkpoint facial comparison capabilities.

S&T's recent round of testing, which took place in May and June of 2019, examined the performance of an additional 10 commercial facial acquisition systems against eight commercial facial comparison algorithms. When completed, the findings of this research may give more insight into the best mix of hardware and software assets needed to ensure the accuracy of checkpoint biometric systems for the diverse traveling public. Additionally, TSA will join interagency efforts to ensure DHS biometric systems (for example, CBP TVS, OBIM IDENT/HART) are designed to enhance performance across missions, use cases, and demographics.

Other variables encountered in the airport environment can affect system performance as well. Inconsistent lighting (for example, sun glare through large windows), changes in a traveler's facial structure relative to previous encounter images, and eyewear or other face/head wear can affect system performance. This underscores the need for TSA to continue to invest time and energy into ensuring its checkpoint biometric solutions, as well as other transportation security equipment, are designed with the human-system interface in mind. Intuitive, highly usable solutions combined with the right TSO procedures, biometric acquisition hardware, and matching software will help ensure TSA's mission requirements are met while also ensuring a streamlined security experience for air travelers.

---

[34] Note: S&T found "relative skin reflectance" to be a better indicator of system performance than U.S. Census categories (e.g. "White", "Black", and "Other").
[35] *See* Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems, available at https://ieeexplore.ieee.org/document/8636231
[36] For more information on the S&T test facility, protocols, and results *see* https://mdtf.org/rally/.

Given the wide diversity of the millions of travelers moving through airport checkpoints daily, accuracy in biometric solutions is a key issue. Therefore, TSA is grounding its exploration of biometric solutions in rigorous scientific study and analysis to ensure the full benefits of biometrics technology are realized. Efforts will continue to ensure biometric checkpoint solutions are designed to mitigate performance variations based on demographic characteristics.

VI. Performance Assessments and Audits of the Biometric Entry-Exit Program

CBP has a robust process for performing operational assessments of CBP's biometric system performance, including evaluating the performance of biometric transactions performed during arrival and departure operations in the air environment, as well as continual performance assessments of technical demonstrations to determine the best concept of operations in other operational environments such as land and sea. Third parties such as S&T and NIST are also engaged to both evaluate CBP operational data and make recommendations for performance enhancements that include biometric capture and matching.

A. Performance Assessments

Biometric Performance Analysis of CBP Systems

CBP has a rigorous process in place to review data and metrics associated with biometric exit facial comparison matching performance. Biometric Air Exit Key Performance Parameters (KPPs) mandate that the system's True Acceptance Rate (TAR) [37] must equal or exceed 97 percent of all in-scope travelers and that the system's False Acceptance Rate (FAR) [38] must not exceed 0.1 percent of all in-scope travelers.

To establish whether or not TVS is fulfilling these KPPs, CBP is systematically analyzing actual flight data for the airlines using Biometric Air Exit. The evaluation team periodically prepares summary reports that present the actual performance of TVS against its KPPs in production.

On a weekly basis, operational performance analysis of CBP biometric operations are conducted, including Air Entry, Air Exit, Preclearance, and Pedestrian Entry (currently in technical demonstration). CBP's performance analysis is focused on the ability to match travelers captured by airports and airlines against the gallery created using the Advanced Passenger Information System (APIS) manifest. Beginning in November 2018, CBP moved to a sampling method to assess the technical match rate for biometric exit and aspects of the CBP-TSA pilot. The technical match rate is a measure of how well the matching algorithm is performing. It includes U.S. citizens who choose not to opt out and individuals who are in-scope (pursuant to 8 CFR 215 and 235) that had a photo in the CBP gallery from existing DHS sources and were

[37] The **TAR** is the number of valid matches divided by the sum of the valid matches and the invalid non-matches. Note that this sum (valid matches plus invalid non-matches) equals the number of matches that should have occurred, and includes all the travelers with a valid encounter photo and at least one valid gallery photo. This definition of the TAR is generally equivalent to the Technical Match Rate (TMR), as defined by CBP's Office of Field Operations.

[38] The **FAR** is the number of invalid matches divided by the sum of the invalid matches and the valid non-matches. Note that this sum (invalid matches plus valid non-matches) equals the number of matches that should NOT have occurred, and includes all the travelers with a valid encounter photo for whom there is no valid gallery photo.

successfully captured by the camera. The following table shows recent match results for each production mode of operation, as a per day average[39].

Modality	Number of Locations	Flight Count	Number of Travelers	Technical Match Rate
Air Entry	11	446	34,716	99.2%
Air Exit	16	92	11,545	97.6%
Air Preclearance	4	45	6,559	99.4%
Pedestrian Entry	4		12,591	97.7%

The estimated false positive rate based on the internal CBP analysis is .0103 percent, which is within the established KPP target of less than .1 percent. As a comparison, a 2014 study "*Passport Officers' Errors in Face Matching*[40]," found that even individuals with specialist experience and training in the task, passport-issuing officers had a 14 percent false positive rate when conducting a person-to-photo comparison test.

Ensuring Biometric Technologies Do Not Unduly Burden Travelers

CBP continuously monitors the biometric matching service and conducts a variety of statistical tests to bolster performance thresholds and minimize any possible bias impact on travelers of certain race, gender, or nationality.

CBP requires that all airlines submit traveler information to the Advanced Passenger Information System (APIS). Among the data submitted is gender, date of birth, travel document type, number, and nationality. Using a subset of this data, CBP conducted extensive statistical analysis including *chi squared*[41] independence tests to determine whether traveler demographics (age, gender, and nationality) affect facial comparison match rates. 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.

CBP's analysis found a negligible effect in regards to biometric matching based on citizenship[42], age, or gender while achieving a technical match rate (TMR) in the high 90 percentile.[43] As of December 2018, TMR continues to be at a steady state, above 98 percent. Significant improvements to the algorithm and exit operations continue to be made, which has led to a substantial reduction in the initial gaps in matching for ages and genders. On average, U.S.

[39] Data shown indicates the averages per day for the period March 20, 2019 to April 2, 2019.
[40] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0103510
[41] A *chi-squared* ($\chi 2$) independence test is a statistical test applied to sets of categorical data to evaluate how likely it is that any observed difference between the sets arose by chance. The tests can be used to determine whether there is a significant difference between the expected frequencies and the observed frequencies in one or more categories.
[42] While CBP uses citizenship as a general proxy because it does not collect race/ethnicity data, it takes into account in its analysis that this is clearly a more effective proxy when looking at homogenous countries than diverse ones.
[43] Based on June 2017 – November 2018 CBP Air Exit data from biometric exit locations: JFK, MIA, IAH, HOU, ORD, SEA, SFO, LAS, DTW, LAX, IAD, MCO, ATL, BOS, and FLL.

citizens typically match at a lower rate as they have fewer and older photos which decreases matching rates. Travelers between ages 26 and 65 match slightly better than "young" (ages 14 to 25) travelers (0.3 percent) and "old" (ages 66 to 79) travelers (0.1 percent), compared to 2.8 percent and 8 percent, respectively, during the initial pilot period. Similarly, women match slightly better than men (0.2 percent), compared to matching worse initially (1.7 percent) during the pilot period. Much of the bias seen in the initial period also relates to much lower flight volume during that timeframe.

As NIST concluded during its 2018 Face Comparison Vendor Test[44], there have been massive improvements in the accuracy of face comparison algorithms in the last five years (2013-2018). The performance of CBP's TVS continues to improve over time due to technical, operational, and procedural advancements including threshold adjustments and testing multiple vendors. CBP has enhanced the photo selection process used to build the galleries, which reduces the number of travelers with no photos and improves the accuracy of the system.[45] Additionally, CBP has enhanced the manner in which the galleries are populated, ensuring that the information included in the flight manifest is used to its maximum potential to include more higher-quality photographs.[46] CBP has also issued various update to the matching algorithms, which increase the algorithm's ability to create biometric templates from non-frontal images taken during the U.S. entry or exit process.

There have also been software changes to the cameras to allow travelers posing for the photos to receive visual feedback. Furthermore, as CBP continues and expands its usage of TVS, personnel using the technology become more aware of the optimal camera positions to ensure better images and increase the traveler throughput. Some cameras are also now equipped with multiple lenses to capture images for various angles, which may increase photo quality depending on the height of the traveler.

Biometric Technology Impact on Travelers Overstaying Their Lawful Period of Admission

CBP has the ability to accurately report overstay numbers in the air and sea environments today. In FY2018, DHS calculated a total overstay rate of 1.22 percent, or 666,582, overstay events. In other words, 98.78 percent of in-scope nonimmigrant entries in FY2018 departed the United States on time and in accordance with the terms of their admission. Annual statistics on visa overstays are provided by DHS to Congress in the Annual Entry Exit Overstay Report.[47]

Adding biometric verification to an already robust biographic exit capability enables CBP to better detect travelers seeking to depart the country under a false identity, including aliens

---

[44] *See* NIST Interagency Report 8238, available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.
[45] A 2010 NIST evaluation of face comparison showed that considerable accuracy benefits accrue with retention and use of all historical images. See https://www.nist.gov/publications/report-evaluation-2d-still-image-face-recognition-algorithms.
[46] Additional information about CBP's gallery building process can be found in the DHS/CBP/PIA-056, Privacy Impact Assessment for the Traveler Verification Service, issued Nov. 14, 2018, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf.
[47] See FY 2018 Entry-Exit Overstay Report at: https://www.dhs.gov/sites/default/files/publications/19_0417_fy18-entry-and-exit-overstay-report.pdf

seeking to fraudulently use validly issued U.S. travel documents. The addition of biometrics has assisted CBP officers in detecting impostors attempting to gain entry to the United States. As part of the continued expansion of biometric exit capabilities, CBP will measure and report on the number of impostors detected by the biometric exit program.

Utilizing biometric technology, CBP has been able to biometrically confirm more than 14,000 travelers that overstayed their lawful period of admission on exit. As of April 2019, 130 impostors have been positively identified using the TVS system across air entry and pedestrian entry environments. All biometric encounters of in-scope foreign nationals are recorded in the enterprise biometrics system IDENT.

B. Audits Performed

DHS Office of Inspector General

The DHS Office of Inspector General (OIG) audit (OIG-18-80), *Review of CBP Biometric Exit Capability*[48], evaluated CBP's efforts to develop and implement a biometric exit capability and assess whether biometric data collected has improved DHS's ability to verify foreign visitor departures at U.S. airports. The final report was issued on September 24, 2018, and included four recommendations:

1) Develop an internal plan to institute enforcement mechanisms or back-up procedures to prevent airlines from bypassing biometric processing prior to flight boarding;
2) Take steps to coordinate with airport and airline stakeholders to increase bandwidth to meet the operational demands of biometric processing at the Nation's top airports;
3) Continue to refine the TVS algorithm to ensure the highest possible traveler match rate, with allowances for photo age and quality; and
4) Develop internal contingency plans for funding and staffing the program, in the event that airlines do not agree to partner with CBP in implementing the biometric capability nationwide.

The OIG conducted fieldwork from September 2017 to January 2018 and reviewed data from the earliest start of the technology demonstrations, which were never intended to be a final implementation model. However, regarding recommendation three and as addressed previously in this report, CBP continues to monitor and improve algorithm performance through incremental updates and improvements with system development and image quality requirements. CBP data analytic teams are evaluating any anomalies and providing feedback to development teams to improve entity resolution and refine matching performance

DHS Science and Technology (S&T) Directorate

In order to continually improve upon the quality of the images, DHS S&T is assisting CBP by testing the efficiency, effectiveness, user satisfaction, and equitability of biometric systems. This

[48] Available at: https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

includes performing independent scenario testing of state of the art commercial biometric systems at the MdTF as well as performing analyses using a sample of operational TVS images.

Starting in 2018, DHS S&T has performed independent biometric analyses using a sample of operational TVS probe and gallery facial images[49][50]. These analyses focused on answering specific questions regarding biometric performance. DHS S&T found that the algorithm used in TVS was superior in performance to all other algorithms tested.

Calculating standard biometric performance metrics in operational systems is challenging. DHS S&T developed a method for estimating the false positive identification rate (FPIR) using operational TVS system data. DHS S&T presented the new method, termed "Virtual Red Team" analysis, to CBP. DHS S&T used this method to estimate FPIR. DHS S&T concluded that FPIR for TVS varies by flight, such that some flight routes could have FPIR values 6-fold higher than others.

Based on these analyses, DHS S&T made specific recommendations to CBP including:

1. To ensure that only ticketed travelers are allowed to use TVS for boarding OR to increase match thresholds used for biometric exit; and
2. To carry out an exhaustive "Virtual Red Team" analysis to calculate the risk of false matches based on the demographics (age, country of origin, gender) of travelers on individual flights.

National Institute of Standards and Technology

CBP is also collaborating with NIST to perform an independent and comprehensive scientific analysis of CBP's operational face matching performance, including impacts due to traveler demographics and image quality. This independent study will help verify results and provide a more in-depth analysis on various factors. Upon analyzing a comprehensive set of data, NIST will provide objective recommendations regarding matching algorithms, optimal thresholds, and gallery creation, optimizing face matching performance for large-scale traveler ID at air, land, and sea entry and exit ports of entry. CBP will continue to actively monitor and refine the performance of this process and associated algorithms in order to make incremental improvements and minimize signs of bias, and ensure the high accuracy of facial matching for all travelers.

[49] DHS S&T Port of Entry- People Screening. February, 2018. Analysis of Data and Algorithms Related to the Traveler Verification System: Estimating Effects of Gallery Size and Traveler Demographics on False Positive Identification Rates.

[50] DHS S&T Biometric and Identity Technology Center. January, 2019. Analysis of Data and Algorithms Related to the Traveler Verification System: Estimating False Match Rate and False Positive Identification Rate.

VII. Conclusion

Biometric technologies have the potential to greatly enhance operational efficiencies and security for both CBP and TSA. CBP has made significant progress in implementing biometric solutions across air, land, and sea since receiving the biometric entry-exit mission in 2013. Following publication of the joint policy memorandum on CBP and TSA's partnership on the development and implementation of biometric technologies, particularly facial comparison, both agencies have worked together on a number of operational pilots. These volunteer-based pilots have allowed both agencies to test, evaluate, and continue to refine biometric technology solutions, while working to achieve a more streamlined traveler experience. CBP and TSA's efforts have been grounded in transparency and a commitment to traveler privacy. CBP and TSA will continue to work together and seek input from their stakeholders as they examine the impact of biometric technology and work to align with DHS initiatives, strategies, and capabilities on biometrics.

VIII. Appendices

Appendix A. DHS Fair Information Practice Principles

Transparency	DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
Individual Participation	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.
Purpose Specification	DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose(s) for which the PII is intended to be used.
Data Minimization	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).
Use Limitation	DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
Data Quality and Integrity	DHS should to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
Security	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.
Accountability and Auditing	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.

Appendix B. Acronyms

Acronym	Definition
APIS	Advance Passenger Information System
ATL	Hartsfield-Jackson Atlanta International Airport
CAT	Credential Authentication Technology
CBP	U.S. Customs and Border Protection
DCA	Ronald Reagan Washington National Airport
DHS	U.S. Department of Homeland Security
DPIAC	Data Privacy and Integrity Advisory Committee
FAR	False Acceptance Rate
FIPP	Fair Information Practice Principles
FOUO	For Official Use Only
FPIR	False Positive Identification Rate
FY	Fiscal Year
HART	Homeland Advanced Recognition Technology
HSSEDI	Homeland Security Systems Engineering & Development Institute
ID	Identification
IDENT	DHS Automated Biometric Identification System
JFK	John F. Kennedy International Airport
KTN	Known Traveler Number
KPP	Key Performance Parameters
LAX	Los Angeles International Airport
MdTF	S&Ts Maryland Test Facility
NIST	National Institute of Standards and Technology
OBIM	Office of Biometric Identity Management
OIG	DHS Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	personally identifiable information
S&T	DHS Science and Technology Directorate
SORN	System of Records Notices
TAR	True Acceptance Rate
TDC	Travel Document Checker
TMR	Technical Match Rate
TSA	Transportation Security Administration
TSO	Transportation Security Officer
TVS	Traveler Verification Service