TESTIMONY OF

John P. Wagner
Deputy Assistant Executive Commissioner
Office of Field Operations
U.S. Customs and Border Protection

For a Hearing

BEFORE

U.S. House of Representatives
Committee on Homeland Security

ON

"About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Technologies"

July 10, 2019
Washington, DC

Chairman Thompson, Ranking Member Rogers, and Members of the Committee, thank you for the opportunity to testify before you on the efforts of U.S. Customs and Border Protection (CBP) to better secure our nation by incorporating biometrics into our comprehensive entry-exit system, and to identify overstays in support of our border security mission.

CBP has received public support for its use of biometrics from the International Air Transit Association (IATA),[1] the World Travel and Tourism Council,[2] and the Department of Commerce Travel and Tourism Advisory Board.[3] With air travel growing at 4.9% per year, and expected to double by 2031, and an increasingly complex threat posture, CBP must innovate and transform the current travel processes in order to handle this new volume without significant personnel and infrastructure investments. Facial comparison technology will enable CBP and travel industry stakeholders to position the U.S. travel system as best in class, which will in turn drive the continued growth in air travel volume.

As authorized in several statutes and regulations,[4] CBP is congressionally mandated to implement a biometric entry-exit system. Prior to the Consolidated and Further Continuing Appropriations Act of 2013 (Public Law 113-6), which transferred the biometric exit mission from the Department of Homeland Security (DHS) generally to CBP, the U.S. Government and the private sector were developing independent biometrics-based schemes. These varied, and often uncoordinated, investments relied on multiple biometrics and required complicated enrollment processes.[5] DHS, the Transportation Security Administration (TSA), legacy United States Visitor and Immigrant Status Indicator Technology, and several private sector companies developed separate uses for biometrics, creating different guidelines and business rules, which increased privacy risks and decreased accountability, as each stakeholder had distinct responsibilities.

In 2017, CBP developed an integrated approach to the biometric entry-exit system that stakeholders, including other U.S. government agencies with security functions, such as TSA, and travel industry stakeholders, such as airlines, airports, and cruise lines, could incorporate into their respective mission space. We offered relevant stakeholders an "identity as a service" solution that uses facial comparison to automate manual identity verification thereby

[1] https://www.iata.org/pressroom/pr/Documents/resolution-one-id-agm-2019.pdf
[2] https://www.wttc.org/about/media-centre/press-releases/press-releases/2019/we-must-act-and-assign-priority-and-resources-to-biometrics/
[3] https://www.trade.gov/ttab/docs/TTAB--Biometrics%20Recommendations%20Letter_042919.pdf
[4] The following statutes require DHS to take action to create an integrated entry-exit system: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215, 114 Stat. 337; Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546; Section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106-396, 114 Stat. 1637, 1641; Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272, 353; Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. No. 107-173, 116 Stat. 543, 552; Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638, 3817; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 338; and Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, 130 Stat. 122, 199.

harmonizing the data collection and privacy standards each stakeholder must follow. This comprehensive facial comparison service leverages both biographic and biometric data (which is key to supporting CBP's mission), fulfilling the congressional mandate and using the system to support air travel, and improve efficiency and the efficacy of identity verification, as stated below.

CBP has been testing various options to leverage biometrics at entry and departure.[6] These technologies will make the process for verifying the identity of individuals for this system more efficient, accurate, and secure by using facial comparison technology. However, the use of this technology allows CBP to improve identity verification. Using data that travelers voluntarily provide, we are simply automating the manual identity verification process done today. Facial comparison allows CBP to better identify those who are traveling on falsified or fraudulent documents, which improves our ability to identify those who are seeking to evade screening in order to enter the United States, including those who present public safety or national security threats, and visitors who have overstayed their authorized period of admission. Moreover, stakeholders have attested that using biometrics could lead to faster boarding times, enhanced customer service, better use of our CBP staffing, and faster flight clearance times on arrival.

CBP has continuously kept Congress abreast of our process through several Congressional reports, hearings, and briefings. Through the Consolidated Appropriations Act of 2016 and the Bipartisan Budget Act of 2018, Congress authorized up to $1 billion in visa fee surcharges through 2027 to support biometric entry/exit.[7]

Previous Efforts to Launch a Biometric Exit System

Prior to the Consolidated and Further Continuing Appropriations Act of 2013 (Public Law 113-6), which transferred the biometric exit mission from DHS to CBP, the U.S. Government and the private sector were already developing independent biometric solutions.

For example, from January 2004 through May 2007, DHS used kiosks placed between the security checkpoint and airline gates that would collect a traveler's fingerprint biometrics. The traveler had the responsibility to find and use the devices, with varying degrees of support from the airports where the kiosks were deployed. In 2008, DHS issued a Notice of Proposed Rulemaking (NPRM) proposing to require that commercial air and vessel carriers collect biometric information from certain aliens departing the United States and submit this information to DHS within a certain timeframe. Most of the comments opposed the adoption of the proposed rule due to issues of cost and feasibility. Among other things, commenters suggested that biometric collection should be a purely governmental function, that requiring air carriers to collect biometrics was not feasible and would unfairly burden air carriers and airports, and that the highly competitive air industry could not support a major new process of biometric collection on behalf of the government. Additionally, as directed by Congress, from May through June 2009, DHS operated two biometric exit pilot programs testing the collection of biometric exit data, first by CBP at the departure gate using a mobile device, and second by TSA at the security checkpoint.

[6] Available at: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0

[7] P.L. 114-113 129 Stat. 2242 (December 17, 2015); P.L. 115-123 132 Stat. 64 (February 9, 2018).

DHS concluded from the NPRM comments and pilot programs that it was generally inefficient and impractical to introduce entirely new government processes into an existing and familiar traveler flow, particularly in the air environment. DHS also concluded that the use of mobile devices to capture electronic fingerprints would be extremely resource-intensive. This information helped frame our concept for a comprehensive biometric entry-exit system that would avoid adding new processes, utilize existing infrastructure, leverage existing stakeholder systems, processes and business models, leverage passenger behaviors and expectations, and utilize existing traveler data and existing government IT infrastructure.

CBP's Integrated Approach to a Comprehensive Biometric Entry-Exit System

Leveraging CBP's current authorities, we are executing Congressional mandates to test technologies to create an integrated biometric entry/exit system using facial comparison technology.[8] This technology uses existing advance passenger information could be used along with photographs already provided by travelers to the government for the purposes of international travel to create "galleries" of facial image templates to correspond with who is expected to be on an international flight arriving or departing the United States. These photographs may be derived from passport applications, visa applications, or interactions with CBP at a prior border inspection[9]. Once the gallery is created based on the advance information, the biometric comparison service compares a template of a live photograph of the traveler to the gallery of facial image templates. Live photographs are taken where there is clear expectation that a person will need to provide documentary evidence of their identity. If there is a facial image match, the traveler's identity has been verified.

These technologies will make the process for verifying the identity of individuals for this system more efficient, accurate, and secure by using facial recognition technology. For technical demonstrations at the land border, air entry, and some air exit operations, CBP takes photographs of travelers on CBP-owned cameras. These tests have been extended on a voluntary basis to exempt aliens[10] and U.S. Citizens. Such participation provides facilitative benefits and a more accurate and efficient method for verifying the identity and citizenship of these individuals. In other air exit and seaport demonstrations, CBP does not take the photographs; but specified partners, such as commercial air carriers, airport authorities, and cruise lines, take photographs of

[8] Available at: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0

[9] U.S. passport and visa photos are available via the Department of State's Consular Consolidated System. See Privacy Impact Assessment: Consular Consolidated Database, available at https://2001-2009.state.gov/documents/organization/93772.pdf.

[10] Under 8 CFR 235.1(f)(ii) and 8 CFR 215.8(a)(1), CBP may require certain aliens to provide biometric identifiers to confirm their admissibility or, at specified airports, their departure. Some aliens are exempt from any requirement to provide biometrics, including: Canadian citizens under section 101(a)(15)(B) of the Act who are not otherwise required to present a visa or be issued a form I-94 or Form I-95; aliens younger than 14 or older than 79 on the data of admission; aliens admitted A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines this requirement shall not apply.

travelers and share the images with CBP's facial recognition technology. These partners that deploy their own camera operators and camera technology must meet CBP's technical and security requirements. These tests occur on a voluntary basis, and are conducted consistent with that partner's contractual relationship with the traveler.

CBP is authorized to require "in-scope"[11] aliens to provide biometric identifiers.[12] For entry, CBP is using facial comparison technology with CBP cameras during the inspection process.[13] For exit, CBP is operating pilot programs at certain land and sea ports of entry, and airports using facial comparison technology.[14] This technology provides the travel industry with the tools to use facial comparison to verify traveler identity and transmit information to CBP.[15] We have identified best practices from the prior work done by DHS as well as from our international partners that have informed the design of a biometric exit system that does not require an inefficient two-step process or require multiple different biometrics for traveler identity verification purposes.

CBP understood the need to build a system that all stakeholders within the travel continuum could participate in – without building their own independent system – that could expand to other mission areas outside of the biometric exit process. To address these challenges and satisfy the congressional mandate, we work closely with our partners to integrate biometrics with existing identity verification requirements already required, to the extent feasible.[16]

The facial comparison technology utilized by CBP is currently able to match travelers at a rate of greater than 97 percent,[17] which is accomplished by comparing against a limited number of faces through the creation of galleries. Travelers who do not match to the system simply show their passport documents to a CBP officer or airline gate agent, and upon confirmation of identity, board the aircraft.

While CBP's primary responsibility is national security, we must also facilitate legitimate trade and travel. The use of facial comparison technology has enabled CBP to not only address a national security concern head on by enhancing identity verification but also to simultaneously improve the traveler experience throughout the travel continuum. CBP engineered a biometric exit solution that gives CBP, TSA, and industry stakeholders, such as airlines and airports, the ability to automate manual identity verification with facial comparison technology at locations

---

[11] "In scope" aliens are aliens may be required to provide biometric identifiers to confirm their inadmissibility, or, at specified airports, their departure, under 8 CFR 235.1(f)(ii) and 8 CFR 215.8(a)(1).
[12] *See* 8 CFR 215.8(f)(ii), 235.8(a)(1).
[13] Available at: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0
[14] *See* 8 C.F.R. 215.8(a)(1).
[15] Numerous statutes require the advance electronic transmission of passenger and crew member manifests for commercial aircraft and commercial vessels. These mandates include, but are not limited to Section 115 of the Aviation and Transportation Security Act (ATSA), Public Law 107-71, 115 Stat. 597; 49 U.S.C. 44909 (applicable to passenger and crew manifests for flights arriving in the United States); Section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA), Public Law 107-173, 116 Stat. 543; 8 CFR 217.7; 8 CFR 231.1; 8 CFR 251.5; and 8 U.S.C. 1221.
[16] Ibid.
[17] Department of Homeland Security Fiscal Year 2018 Entry/Exit Overstay Report, available at https://www.dhs.gov/sites/default/files/publications/19_0417_fy18-entry-and-exit-overstay-report.pdf

where identity verification is present today. This may include the departure gates, debarkation areas, airport security checkpoints, and Federal Inspection Services (FIS) area. CBP only uses photos collected from cameras deployed specifically for this purpose and does not use photos obtained from closed-circuit television or other live or recorded video. As the facial comparison technology automates the manual identity verification process in place today, it allows CBP and its stakeholders to make quicker and more informed decisions.

CBP Authorities and Regulatory Updates

As described above, numerous federal statutes require DHS to create an integrated, automated biometric entry and exit system that records the arrival and departure of aliens, compares the biometric data of aliens to verify their identity, and authenticates travel documents presented by such aliens. Most recently, in 2017, Executive Order 13780 called for the expedited completion of the biometric entry-exit data system.[18]

DHS also has broad authority to control alien travel and to inspect aliens under various provisions of the Immigration and Nationality Act of 1952, as amended (INA).[19] As part of CBP's broad authority to enforce U.S. immigration laws, CBP is responsible for ensuring the interdiction of persons illegally entering or exiting the United States, facilitating and expediting the flow of legitimate travelers, and detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States at entry. CBP also has responsibility to facilitate and expedite the flow of legitimate travel and trade and detect individuals attempting to illegally enter or exit the United States.

To effectively carry out its responsibilities under the INA upon both arrival and departure from the United States, CBP must be able to conclusively determine whether a person is in fact a U.S. citizen or national, or an alien by verifying that the person is the true bearer of his or her travel documentation. CBP is authorized to take and consider evidence concerning the privilege of any

[18] Numerous other statues require DHS to take action to create an integrated entry-exit system including: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215, 114 Stat. 337; Section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106-396, 114 Stat. 1637, 1641; and Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272, 353.

[19] 8 U.S.C. § 1365b mandates the creation of an integrated and comprehensive system. This statute further provides that the entry and exit data system shall include a requirement for the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data. 8 U.S.C. 1365b(d). As a result, if a certain category of individuals is required to provide biometrics to DHS on entry as part of the examination and inspection process, the same category of individuals must be required to provide biometrics on exit as well. DHS may require persons to provide biometrics and other relevant identifying information upon entry to, or departure from, the United States. Specifically, DHS may control alien entry and departure and inspect all travelers under §§ 215(a) and 235 of the INA (8 U.S.C. 1185, 1225). Aliens may be required to provide fingerprints, photographs, or other biometrics upon arrival in, or departure from, the United States, and select classes of aliens may be required to provide information at any time. *See, e.g.*, INA 214, 215(a), 235(a), 262(a), 263(a), 264(c), (8 U.S.C. 1184, 1185(a), 1225(a), 1302(a), 1303(a), 1304(c)); 8 U.S.C. 1365b. Pursuant to § 215(a) of the INA (8 U.S.C. 1185(a)), and Executive Order No. 13323 of Dec. 30, 2003 (69 FR 241), the Secretary of Homeland Security, with the concurrence of the Secretary of State, has the authority to require aliens to provide requested biographic information, biometrics and other relevant identifying information as they depart the United States.

person to enter, reenter, pass through, or reside in the United States, or concerning any matter, which is material or relevant to the enforcement or administration of the INA.[20] A person claiming U.S. citizenship must establish that fact to the examining officer's satisfaction and must present a U.S. passport or alternative documentation.[21] Manual review of passports has historically been used to carry out this responsibility, but facial comparison technology can do so with greater consistency and accuracy.

CBP is statutorily mandated to fully implement a biometric entry/exit system, and has clear statutory authority to undertake all appropriate actions in support of the use of biometrics. To further advance the legal framework described above, CBP is working to propose and implement regulatory amendments and will provide progress updates in the Unified Agenda, as appropriate.

Data Security

There are four primary safeguards to secure passenger data, including secure encryption during data storage and transfer, irreversible biometric templates, brief retention periods, and secure storage. Privacy is implemented by design, ensuring data protection through the architecture and implementation of the biometric technology.

CBP prohibits its approved partners such as airlines, airport authorities, or cruise lines from retaining the photos they collect under this process for their own business purposes. . The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement. As discussed in the November 2018 Privacy Impact Assessment,[22] we have developed Business Requirements to document this commitment, to which the private sector partners must agree as a condition of participation in the pilots. Unlike with the pilots in the early 2000s, CBP has established these common system-wide standards (business requirements), which support CBP's integrated approach to the use of biometrics.

Regarding the recent subcontractor data breach incident, CBP is very concerned that the unauthorized access of CBP data will undermine congressional and public confidence in CBP at a time in which we are pursuing transformative and innovative initiatives to enhance lawful trade and travel. We are aggressively investigating the breach of the subcontractor's systems and potential exposure of traveler and license plate images. There are two events that are under investigation: a) a malicious cyberattack that impacted the systems of a Federal subcontractor; and b) the unauthorized access of CBP data by the same Federal subcontractor.

This incident did not impact any of the air entry/exit partnerships discussed earlier and is limited solely to certain pilot program data collected in the land border environment. Airlines are trusted partners of CBP, given the various statutory airline collection mandates[23] in place. Airlines have

[20] 8 U.S.C. 1357(b).

[21] 8 CFR 235.1(b). It is usually unlawful for a U.S. citizen to depart or attempt to depart from the United States without a valid passport. See 8 U.S.C. 1185(b); 22 CFR 53.1.

[22] Available at: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0

[23] Numerous statutes require the advance electronic transmission of passenger and crew member manifests for commercial aircraft and commercial vessels. These mandates include, but are not limited to Section 115 of the Aviation and Transportation Security Act (ATSA), Public Law 107-71, 115 Stat. 597; 49 U.S.C. 44909 (applicable

been reliably providing CBP with advance electronic transmission of passenger and crew member manifests, as well as authenticating and verifying the identity of all passengers and ensuring that the travelling passengers are correctly documented to enter the receiving country.

While the data breach investigation is ongoing, preliminary evidence indicates several violations of CBP privacy and security policies and violation of specific contract clauses. CBP is taking several actions to ensure the security of CBP systems, to include: deploying cyber-enhanced technology (e.g., audit tracking, logging, and enhanced encryption) to all vehicle lanes to further protect license plate image data;; conducting threat assessments to proactively identify vulnerabilities; restricting removable media usage and rolling out enhanced insider threat capabilities; and, updating all contractual, policy and security requirements. Additionally, CBP required that the prime contractor immediately terminate its subcontracting agreement and its work thereunder. As such, the subcontractor no longer has access to CBP data.

Privacy, Transparency, Civil Rights and Future Assessments

CBP is committed to ensuring that our use of technology sustains and does not erode privacy protections. We take privacy obligations very seriously and are dedicated to protecting the privacy of all travelers. CBP complies with all requirements under the Privacy Act of 1974[24] (Pub.L 93-579), as well as all DHS and government-wide policies. In accordance with DHS policy, CBP uses the Fair Information Practice Principles (FIPPs) to assess the privacy risks and ensure appropriate measures are taken to mitigate any risks from its collection of data through the use of biometrics. As CBP is bound by the above mentioned privacy laws and policies, as well as data collection requirements, partnering stakeholders are also held to the same standards, which increases accountability with the use of biometrics.

CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). When airlines or airports are partnering with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP. We provide notice to travelers at the designated ports of entry through both physical and either LED message boards or electronic signs, as well as verbal announcements in some cases, to inform the public that CBP will be taking photos for identity verification purposes and of their ability to opt-out of having their photo taken.

Upon request, CBP Officers provide individuals with a tear sheet with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the particular demonstration, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information. Additionally, in the FIS, CBP posts signs informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States.

---

to passenger and crew manifests for flights arriving in the United States); Section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA), Public Law 107-173, 116 Stat. 543; 8 CFR 217.7; 8 CFR 231.1; 8 CFR 251.5; and 8 U.S.C. 1221.

[24] 5 U.S.C. 552a.

Any U.S. citizen or foreign national may notify the airline-boarding agent that they would like to opt out at the time of boarding. The airline would conduct manual identity verification using their travel document, and may notify CBP to collect biometrics, if applicable. .

CBP provides general notification of its biometric exit efforts and its various pilot programs through Privacy Impact Assessments (PIAs) and Systems of Records Notices (SORNs),)[25] published at www.dhs.gov/privacy, and through information, such as Frequently Asked Questions, readily available at www.cbp.gov. We published a comprehensive PIA called the "Traveler Verification Service" in November 2018, to explain all aspects of CBP's biometric usage through the program, to include policies and procedures for the collection, storage, analysis, use, dissemination, retention, and/or deletion of data.[26]

The PIA and the public notices specifically highlight that facial images for arriving and departing foreign nationals (and those dual national U.S. citizens traveling on foreign documentation) are retained by CBP for up to two weeks, not only to confirm travelers' identities but also to assure continued accuracy of the algorithms and ensure there are no signs of bias. As always, facial images of arriving and departing foreign nationals are forwarded to the IDENT system for future law enforcement purposes, consistent with CBP's authority. As U.S. citizens are not in-scope[27] for biometric exit, photos of U.S. citizens used for biometric matching purposes are held in secure CBP systems for no more than 12 hours after identity verification, and are held for this time period only in case of an extended system outage or for disaster recovery and are then deleted. We reduced the retention of U.S. citizen photos to no more than 12 hours as a direct result of briefings and consultations with Chairman Thompson.

Additionally, as described above, private sector partners must agree to specific CBP business requirements, many of which are outlined in the recent PIA. CBP is simplifying the information flow to the traveling public by developing one set of business standards and privacy guidelines, thereby enabling more comprehension of and transparency and accountability in the biometric process.

While CBP's commitment to transparency has been demonstrated by the above efforts, CBP is committed to improving its public messaging and helping the public better understand the technology. CBP welcomes the Committee's input.

CBP collaborates regularly with the DHS Privacy Office to ensure compliance with applicable privacy laws and policies, and to build in privacy protection best practices surrounding CBP's use of biometric technology. 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

[25] 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. Those SORNs can be found at https://www.dhs.gov/system-records-notices-sorns.

[26] Available at: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0

[27] Pursuant to 8 CFR 215 and 235.

facial comparison technology. The DPIAC published its report on February 26, 2019[28]. CBP has implemented or is actively working to implement all of the DPIAC recommendations.

CBP is fully committed to the fair, impartial and respectful treatment of all members of the trade and traveling public. CBP has rigorous processes in place to review data and metrics associated with biometric entry and exit facial comparison performance to assess and guard against improper bias. Significant variance in match rates that can be attributed to demographic variables have not been detected. Additionally, CBP is partnering with the National Institute of Standards and Technology (NIST) to conduct a comprehensive analysis of facial comparison technologies in CBP's biometric entry-exit efforts, in order to improve data quality and integrity, and ultimately the accuracy of technology that informs agency decision-making that affects people. NIST will provide guidance and data that allows CBP to set a threshold, given CBP's security and facilitation goals for large-scale face recognition of travelers at air, land, and sea POEs.

CBP's Progress towards Implementing a Comprehensive Biometric Entry-Exit System

Biometric Entry-Exit in the Air Environment

CBP is also enhancing the arrivals process by using facial comparison technology. With more efficient and more secure clearance processes, airports, airlines, and travelers benefit from shorter connection times and standardized arrival procedures. Security is increased by adding facial comparison as an additional tool to reduce imposter threat while increasing the integrity of the immigration system. Since initiating this facial comparison technology in the air environment on a trial basis, CBP has already identified six imposters[29], including two with genuine U.S. travel documents (passport or passport card), who were using another person's valid travel documents as a basis for seeking entry to the United States.

CBP is working towards full implementation of biometric exit in the air to account for over 97 percent of departing commercial air travelers from the United States. Stakeholder partnerships are critical for implementing a biometric entry-exit system, and airports, airlines, and CBP are collaborating to develop a process that meets our biometric entry-exit mandate and airlines' business needs. These partnerships help ensure that biometric entry-exit does not have a detrimental impact on the air travel industry, and that the technology is useful and affordable. Stakeholders have attested that using biometrics could lead to faster boarding times, enhanced customer service, better use of our CBP staffing, and faster flight clearance times on arrival. Engagement with additional stakeholders continues on how they can be incorporated into the comprehensive entry-exit system, and CBP is ready to partner with any appropriate airline or airport that wishes to use biometrics to expedite the travel process for its customers.

Biometric Entry-Exit in the Land Environment

In the land environment, there are often geographical impediments to expanding exit lanes to accommodate adding lanes or CBP-staffed booths. The biometric exit land strategy focuses on implementing an interim exit capability while simultaneously investigating what is needed to

[28] https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf

[29] Number of imposters updated as of June 11, 2019.

implement a comprehensive system over the long term. Biometrically verifying travelers who depart at the land border will close a gap in the information necessary to complete a nonimmigrant traveler's record in CBP's Arrival and Departure Information System, and will allow us an additional mechanism to better determine when travelers who depart the United States via land have overstayed their admission period. Given the limitations outlined above and DHS's desire to implement the use of biometrics without negatively affecting cross-border commerce, CBP plans on taking a phased approached to land implementation.

Facial comparison technology, similar to what is used in the air environment has been deployed at entry operations at the Nogales and San Luis, Arizona POEs. CBP plans to expand to additional locations along the southern border in 2019. By using the facial comparison technology in the land environment, CBP has identified 138 imposters, including 45 with genuine U.S. travel documents (passport or passport card), attempting to enter the United States.

Additionally, CBP tested "at speed" facial biometric capture camera technology on vehicle travelers.[30] From August 2018-February 28, 2019, CBP conducted a technical demonstration of facial comparison technology on persons inside vehicles moving less than 20 miles per hour entering and departing Anzalduas, Texas.

Later in 2018, CBP began testing facial comparison technology at the Peace Bridge in Buffalo, New York in conjunction with the Buffalo and Fort Erie Public Bridge Authority (PBA)) to facilitate the development of a demonstration project to test the viability of taking images from moving commercial trucks and comparing them against gallery images. From fall 2018 to early June 2019, PBA took photographs of truck drivers and sent them to CBP to assist with calibrating the project. The development is currently on pause.

Biometric Entry-Exit in the Sea Environment

Similar to efforts in the air environment, CBP is partnering with the cruise line industry to use facial biometric processing supported by CBP's biometric comparison service in the debarkation (arrival) points at seaports.[31] Facial biometric processing at seaports replaces the current manual comparison performed by the CBP officer using the travel document. Automating identity verification allows us to shift officer focus to core law enforcement functions and reallocate resources from primary inspections to roving enforcement activities. Currently, there are four sea entry sites and four major cruise lines that are operating facial comparison cameras to confirm the identity of arriving passengers on closed-loop cruises (which originate and terminate in the same city). The sea entry sites are Bayonne, New Jersey; Port Everglades, Florida; Miami, Florida; and Port Canaveral, Florida. Each cruise line conducting facial debarkation operations reports that passenger satisfaction feedback to include the debarkation process is significantly more positive as compared to such feedback from vessels not using facial debarkation. Engagement continues with cruise lines and port authorities to expand the technology to other businesses and locations.

[30] Available at: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0
[31] Ibid.

Conclusion

DHS, in collaboration with the travel industry, is aggressively moving forward in developing a comprehensive biometric exit system in the land, air and sea environments that simply replaces a manual identity check with facial comparison technology. The traveler is well aware that their picture is being taken for facial comparison purposes and more detailed information regarding the program is readily available to the public. CBP's collaborative biometric efforts directly addresses the recommendations of the 9/11 Commission Report, which highlighted that security and protection should be shared among the various travel checkpoints (ticket counters, gates, and exit controls). "By taking advantage of them all, we need not depend on any one point in the system to do the whole job." [32]

[32] The 9/11 Commission Report at 385-386, available at http://govinfo.library.unt.edu/911/report/911Report.pdf.