TESTIMONY OF

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

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 Biometric Technologies, Part II”

February 6, 2020
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, the World Travel and Tourism Council, and the Department of Commerce Travel and Tourism Advisory Board.[1] With international air travel growing at 4.9 percent per year and expected to double by 2031, and with an increasingly complex threat posture, CBP must innovate and transform the current travel processes to handle this expanding volume. Facial comparison technology will enable CBP and travel industry stakeholders to position the U.S. travel system as best in class, in turn, driving the continued growth in air travel volume.

As authorized in several statutes and regulations, CBP is congressionally mandated to implement a biometric entry-exit system.[2] 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's (DHS) United States Visitor and Immigration Status Indicator Technology (US-VISIT) Program within the National Protection and Programs Directorate (NPPD) to CBP, the U.S. Government and the private sector were developing independent biometrics-based schemes for administering the entry-exit program responsibilities. These varied and often uncoordinated investments relied on multiple biometrics and required complicated enrollment processes. Public and private sector entities developed separate uses for biometrics, each with varying privacy risks and accountability mechanisms. In 2017, CBP developed an integrated approach to the biometric entry-exit system that other U.S. Government agencies with security functions, such as TSA, as well as travel industry stakeholders such as airlines, airports, and cruise lines, could incorporate into their respective mission space.

---

[1] International Air Transport Association, "Resolution: End-to-end Seamless Travel across Borders Closer to Reality" (June 2, 2019). www.iata.org/en/pressroom/pr/2019-06-02-06/.

World Travel & Tourism Council, "Gloria Guevara: "We must act and assign priority and resources to biometrics" " March 6, 2019. www.wttc.org/about/media-centre/press-releases/press-releases/2019/we-must-act-and-assign-priority-and-resources-to-biometrics/.

United States Travel and Tourism Advisory Board, letter to Commerce Secretary, Wilbur Ross, containing challenges and recommendation on U.S. Government-private industry partnerships on biometric technology (April 29, 2019). https://legacy.trade.gov/ttab/docs/TTAB--Biometrics%20Recommendations%20Letter_042919.pdf

[2] Statutes that require DHS to take action to create an integrated entry-exit system: Sec. 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), P.L. 106-215, 114 Stat. 337; Sec. 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, P.L. 104-208, 110 Stat. 3009-546; Sec. 205 of the Visa Waiver Permanent Program Act of 2000, P.L. 106-396, 114 Stat. 1637, 1641; Sec. 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), P.L. 107-56, 115 Stat. 272, 353; Sec. 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), P.L. 107-173, 116 Stat. 543, 552; Sec. 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108-458, 118 Stat. 3638, 3817; Sec.711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, 121 Stat. 266, 338; and Sect. 802 of the Trade Facilitation and Trade Enforcement Act of 2015, P.L. 114-125, 130 Stat. 122, 199. In addition, through the Consolidated Appropriations Act of 2016 and the Bipartisan Budget Act of 2018, Congress authorized up to $1 billion in visa fee surcharges through 2027 to support biometric entry/exit. P.L. 114-113 129 Stat. 2242 (December 17, 2015); P.L. 115-123 132 Stat. 64 (February 9, 2018).

CBP offered relevant stakeholders an "identity as a service" solution that uses facial comparison to automate manual identity verification, thereby harmonizing the data collection and privacy standards each stakeholder must follow. This comprehensive facial comparison service leverages biographic and biometric data, both of which are key to support CBP's mission, to fulfill the Congressional biometric entry-exit mandate while using the system to support air travel, improve efficiency, and increase the efficacy of identity verification. CBP has been testing options to leverage biometrics at entry and departure, specifically through the use of facial comparison technology.[3] These technologies enhance the manual process used today by making it more efficient, accurate, and secure. Using data that travelers are already required by statute to provide, the automated identity verification process uses facial comparison to identify those who are traveling on falsified or fraudulent documents as well as those seeking to evade screening. These are the individuals who present public safety or national security threats or have overstayed their authorized period of admission.

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 Headquarters to CBP, the U.S. Government and the private sector were already developing independent biometric solutions for administering entry-exit programs. For example, from January 2004 through May 2007, DHS placed kiosks between security checkpoints and airline gates to collect travelers' fingerprint biometrics. The traveler had the responsibility to find and use the devices, while airports where the kiosks were deployed provided varying degrees of support. In 2008, DHS issued a Notice of Proposed Rulemaking (NPRM) that proposes 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 comments opposed the adoption of the proposed rule, citing cost and feasibility. Among other comments was the suggestion that biometrics collection should strictly be a Governmental function. The suggestion was made that the highly competitive air industry could not support a major new process of biometric collection on behalf of the Government, and that requiring air carriers to collect biometrics was not feasible and would unfairly burden air carriers and airports. Additionally, as directed by Congress, from May through June 2009, DHS operated two biometric exit pilot programs in which CBP used a mobile device to collect biometric exit data at departure gates while TSA collected it at security checkpoints.

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 information technology infrastructure.

[3] DHS/CBP (November 2018), DHS/CBP/PIA-056 Traveler Verification Service.(945.31 KB).

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

Leveraging CBP's current authorities, we are executing Congressional mandates to create and test an integrated biometric entry-exit system using facial comparison technology. This technology uses existing advance passenger information along with photographs already provided to the Government by international travelers to create "galleries" of facial image templates that correspond with the individuals expected on international flights 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.[4] Once the gallery is created based on the advance information, the biometric comparison technology compares a template of a live photograph of the traveler – taken where there is clear expectation and authority that a person will need to provide documentary evidence of their identity – to the gallery of facial image templates.

For technical demonstrations at the land border, air entry, and some air exit operations, CBP cameras take photographs of travelers. These tests have been extended on a voluntary basis to exempt certain aliens and U.S. citizens.[5] Participation provides a more accurate and efficient method to verify identity and citizenship. In other air exit and seaport demonstrations, CBP does not take the photographs. Instead, specified partners, such as commercial air carriers, airport authorities, and cruise lines, take photographs of travelers and transmit the images to CBP's facial matching service. These partners use their own camera operators and technology that meets CBP's technical and security requirements. These tests occur on a voluntary basis and are consistent with that partner's contractual relationship with the traveler.

Biometric entry-exit is not a surveillance program. CBP does not use hidden cameras. CBP uses facial comparison technology to ensure a person is who they say they are – the bearer of the passport they present. This technology provides a seamless way for in-scope travelers to meet the requirement to provide biometrics upon departure from the United States. Travelers are aware their photos are being taken and that they can opt-out as described below. CBP uses facial comparison technology only where a current identity check already exists. CBP works closely with partner air carriers and airport authorities to post privacy notices and provide tear sheets for

[4] Department of State, Consular Consolidated System, "Privacy Impact Assessment: Consular Consolidated Database" (January 29, 2020). https://2001-2009.state.gov/documents/organization/93772.pdf.

[5] Under Scope of examination, Alien applicants for admission, 8 C.F.R. §235.1(f)(1)(ii) and Requirements for biometric identifiers from aliens on departure from the United States, 8 C.F.R. §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 the requirement to provide biometrics. This includes Canadians, under Sect.101(a)(15)(B), 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 date 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 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 the requirement 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.

impacted travelers and members of the public in close proximity to the cameras and operators, whether the cameras are owned by CBP or the partners.

The imposter threat – or the use of legitimate documents that do not belong to the bearer – continues to be a challenge for CBP. U.S. passports are the most prized version of an imposter document because – until recently – there was no biometric comparison between the person presenting the document and the owner of the document. As document security standards have increased in the past 20 years, it has become much more difficult to plausibly forge or alter a legitimate document. As a result, those who wish to evade detection seek to use legitimate documents that belong to someone else. U.S. citizens are not required to provide fingerprint biometrics for entry into the country whereas foreign nationals may be required to do so.

CBP is authorized to require "in-scope" aliens to provide biometric identifiers.[6] For entry, CBP uses cameras and facial comparison technology during the inspection process. CBP operates facial comparison technology pilots at exit in certain land and sea ports and some airports.[7] This technology provides the travel industry with the tools to verify traveler identity and transmit information to CBP.[8] We have identified best practices from the prior DHS work as well as from our international partners and used them in the biometric exit system design to avoid an inefficient two-step process that requires multiple biometrics to verify traveler identity.

CBP understood the need to build a system that all stakeholders within the travel continuum could participate in without building their own independent system – one that could expand to other mission areas outside of the biometric exit process. To address these challenges and satisfy the Congressional mandate, we are working closely with our partners to integrate biometrics with existing identity verification requirements to the extent feasible.[9] Facial comparison technology can match more than 97 percent of travelers through the creation of facial galleries.[10] The match rate is based on the percentage of travelers with a valid encounter photo who were successfully matched to a gallery photo.[11]

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

---

[6] "In scope" aliens may be required to provide biometric identifiers to confirm their admissibility, or, at specified airports, their departure in accordance with Inspection of Persons Applying for Admission, Scope of examination, Alien applicants for admission, 8 C.F.R. §235.1(f)(1)(ii) and Requirements for biometric identifiers from aliens on departure from the United States, 8 C.F.R. §215.8(a)(1).

[7] Requirements for biometric identifiers from aliens on departure from the United States, 8 C.F.R. §215.8(a)(1).

[8] Numerous statutes require advance electronic transmission of passenger and crew member manifests for commercial aircraft and commercial vessels. These mandates include, but are not limited to Sec. 115 of the Aviation and Transportation Security Act (ATSA), P.L. 107-71, 115 Stat. 597; Passenger manifests, 49 U.S.C. §44909 (applicable to passenger and crew manifests for flights arriving in the United States); Sec. 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA), P.L. 107-173, 116 Stat. 543; List of alien and citizen passengers arriving and departing, 8 U.S.C. §1221; and Examination of merchandise, 19 U.S.C. §1499.

[9] Ibid.

[10] *Department of Homeland Security Fiscal Year 2018 Entry/Exit Overstay Report,* https://www.dhs.gov/sites/default/files/publications/19_0417_fy18-entry-and-exit-overstay-report.pdf.

[11] DHS/CBP (November 2018), DHS/CBP/PIA-056 Traveler Verification Service.(945.31).

national security concern head-on by enhancing identity verification but to simultaneously improve the traveler experience throughout the travel continuum. CBP engineered a biometric exit solution that gives not only CBP, but TSA and industry stakeholders such as airlines and airports, the ability to automate manual identity verification. This may include departure gates, debarkation (arrival) areas, airport security checkpoints, and Federal Inspection Services areas.

CBP uses only 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. In August 2019, CBP and TSA provided this committee a comprehensive report on the program that included material on the operational and security benefits of the biometric entry-exit system, CBP and TSA's efforts to address privacy concerns and potential performance differential errors, and a comprehensive description of audits performed.[12]

CBP Authorities

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 to verify their identities, and authenticates travel documents. Most recently, in 2017, Executive Order 13780 called for the expedited completion of the biometric entry-exit data system.[13] DHS has broad authority to control alien travel and to inspect aliens under various provisions of the *Immigration and Nationality Act of 1952* (INA), as amended.[14] As part of CBP's authority to enforce U.S. immigration laws, CBP is responsible for interdicting individuals illegally entering or exiting the United States; facilitating and expediting the flow of legitimate travelers; and detecting, responding to, and interdicting terrorists, drug smugglers,

---

[12] DHS, "Transportation Security Administration and Customs and Border Protection: Deployment of Biometric Technologies, Report to Congress" (August 30, 2019) www.tsa.gov/sites/default/files/biometricsreport.pdf.

[13] Other statues that require DHS to create an integrated entry-exit system include: Sect.2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), P.L. 106-215, 114 Stat. 337; Sec. 205 of the Visa Waiver Permanent Program Act of 2000, P.L. 106-396, 114 Stat. 1637, 1641; and Sec. 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), P.L. 107-56, 115 Stat. 272, 353.

[14] Biometric entry and exit data system, 8 U.S.C. §1365b mandates the creation of an integrated and comprehensive system. The entry and exit data system shall include a requirement for the collection of biometric exit data for all categories of individuals required to provide biometric entry data. 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 individuals 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 (December 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.

human smugglers, traffickers, and other persons who may undermine the security of the United States at entry.

To effectively carry out its responsibilities under the INA for both arrivals and departures from the United States, CBP must be able to conclusively determine if a person is 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 person to enter, reenter, pass through, or reside in the United States, or concerning any matter material or relevant to the enforcement or administration of the INA.[15] 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.[16]

To further advance the legal framework, CBP is working to propose and implement regulatory amendments. CBP is working on a biometric entry/exit regulation, which will only impact foreign nationals. In November 2019, CBP transmitted its proposed regulation on biometric entry/exit to the Office of Management and Budget; we are awaiting clearance. The rule will go through the full rulemaking process, which includes a public comment period.

NIST Facial Comparison Vendor Test: December 2019

CBP has partnered with the National Institute of Standards and Technology (NIST) to explore facial comparison technology capabilities. NIST used CBP data that was contained in the OBIM data in its conclusions issued in a recent demographic differential study. The study supports what CBP has seen in its biometric matching operations – that when a high-quality facial comparison algorithm is used along with high performing cameras, proper lighting and image quality controls, face matching technology can be highly accurate. To ensure higher accuracy rates, as well as efficient traveler processing, CBP compares traveler photos to a very small gallery of high-quality images that those travelers already provided to the U.S. Government to obtain a passport or visa.

CBP uses only *one* of the 189 face comparison algorithms evaluated by NIST and produced by NEC Corporation. As the report demonstrates, NIST confirmed that the NEC algorithm that NIST tested is high performing and ranked first or second in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP.[17] The NIST performance metrics described in the report are consistent with CBP operational performance metrics for entry-exit. CBP's operational data continues to show there is no measurable differential performance in matching based on demographic factors. The NIST report shows a wide range in accuracy across algorithm developers, with the most accurate algorithms producing many fewer errors and undetectable false positive differentials. Since

[15] Powers of immigration officers and employees, 8 U.S.C. §1357(b).

[16] Under Scope of examination, 8 C.F.R. §235.1(b), it is generally unlawful for a U.S. citizen to depart or attempt to depart from the United States without a valid passport. See also Travel control of citizens and aliens, 8 U.S.C. §1185(b); and Passport requirement; definitions, 22 C.F.R. §53.1.

[17] Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects, National Institute of Standards and Technology, U.S. Department of Commerce (December 2019), p.8.

many of the performance rates specified in the report would not be acceptable for use in CBP operations, we do not use them.

CBP is committed to implementing the biometric entry exit mandate in a way that provides a secure and streamlined travel experience for all travelers, and CBP will continue to partner with NIST and use NIST research to ensure the continued optimal performance of the CBP face comparison service. In the upcoming weeks, CBP will directly provide NIST with data for 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. NIST will provide objective recommendations regarding matching algorithms, optimal thresholds, and gallery creation.

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 as part of the entry/exit program 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 its comprehensive November 2018 Privacy Impact Assessment concerning its facial recognition technology, CBP has developed business requirements, or system-wide standards, to document this commitment.[18] Our private sector partners must agree as a condition of participation in the pilots.

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 very seriously and are dedicated to protecting the privacy of all travelers. CBP complies with the requirements of the *Privacy Act of 1974* and all DHS and Government-wide policies.[19] In accordance with DHS policy, CBP uses the Fair Information Practice Principles, or FIPPs, to assess the privacy risks and ensure appropriate measures are taken to mitigate risks from data collection through the use of biometrics. Our partnering stakeholders are also held to the same standards.

CBP strives to be transparent and provide notice to individuals regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). When airlines or airports partner with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP. We notify travelers at these ports using verbal announcements, signs, and/or message boards that CBP takes photos for identity verification purposes, and they are informed of their ability to opt-out. Foreign nationals may opt out of providing biometric data to a third party, and any U.S. citizen or foreign national may

[18] DHS/CBP (November 2018), DHS/CBP/PIA-056 Traveler Verification Service.(945.31 KB).

[19] Records maintained on individuals, 5 U.S.C. §552(a), P.L. 93-579, 88 Stat. 1896.

do so at the time of boarding by notifying the airline-boarding agent that they would like to opt out. The airline would conduct manual identity verification using their travel document, and may notify CBP to collect biometrics, if applicable.

If requested, CBP Officers provide a tear sheet with Frequently Asked Questions, opt-out procedures, and additional information, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information. CBP also posts signs informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States. CBP provides general notification of its biometric exit efforts and various pilot programs through Privacy Impact Assessments (PIAs) and Systems of Records Notices (SORNs) and through information such as Frequently Asked Questions, which are readily available at www.cbp.gov. [20]

CBP published a comprehensive PIA concerning its facial recognition technology, known as the Traveler Verification Service, in November 2018. An appendix to that document, published on January 8, 2020, explains aspects of CBP's biometric use as well as policies and procedures for the collection, storage, analysis, use, dissemination, retention, and/or deletion of data.[21] 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 any differential performance. 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 within the scope 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 in case of an extended system outage or for disaster recovery.[22] CBP reduced the retention period for U.S. citizen photos to no more than 12 hours as a direct result of briefings and consultations with Chairman Thompson.

CBP is committed to transparency in this process as well as to improving its public messaging to help the public better understand the technology. We welcome the Committee's input. CBP collaborates regularly with the DHS Privacy Office to ensure compliance with privacy laws and policies. 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. The DPIAC published its report on February 26, 2019.[23] CBP has implemented or is actively working to implement all of the DPIAC recommendations. CBP continues outreach

---

[20] 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. https://www.dhs.gov/system-records-notices-sorns.

[21] DHS/CBP (November 2018), DHS/CBP/PIA-056 Traveler Verification Service. (945.31 KB).

[22] Controls of aliens departing from the United States; Electronic visa update system, 8 C.F.R. §215; Inspection of persons applying for admission, 8 C.F.R. §235.

[23] Report 2019-01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology Privacy Recommendations in Connection with the Use of Facial Recognition Tech nology.pdf.

efforts with privacy advocacy groups regarding the biometric entry-exit program, most recently meeting with them in December 2019. CBP also hosted the Privacy and Civil Liberties Oversight Board (PCLOB) for a tour of biometric processes at Atlanta/Hartsfield International Airport on January 15, 2020.[24]

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

Biometric Entry-Exit in the Air Environment

Facial comparison technology is enhancing the arrivals process, enabling more efficient and more secure clearance processes that benefit airports, airlines, and travelers with shorter connection times and standardized arrival procedures. It is an additional tool to reduce imposter threat while increasing the integrity of the immigration system. Since initiating the use of facial comparison technology in the air environment on a trial basis, CBP has identified seven imposters, including two with genuine U.S. travel documents (passport or passport card), using another person's valid travel documents to seek entry into the United States.[25]

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 on how they can be incorporated into the comprehensive entry-exit system continues, 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 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 DHS's desire to implement the use of biometrics without negatively affecting cross-border commerce, CBP plans to take a phased approached to land implementation.

---

[24] The Privacy Civil Rights Oversight Board is an independent, bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act, P.L. 110-53, https://www.pclob.gov/. Nextgov, Inside the CBP-Build 'Backbone' of Atlanta's Biometric Terminal, (January 21, 2020) inside-cbp-built-backbone-atlantas-biometric-terminal.

[25] Updated January 7, 2020.

Facial comparison technology, similar to what is used in the air environment has been deployed at entry operations at the Nogales and San Luis POEs in Arizona and at the Laredo and El Paso POEs in Texas. CBP plans to expand to additional locations along the southern border in 2020. By using the facial comparison technology in the land environment, CBP has identified 247 imposters, including 45 with criminal records and 18 under the age of 18, attempting to enter the United States. Additionally, CBP tested "at speed" facial biometric capture camera technology on vehicle travelers.[26] From August 2018 to February 28, 2019, CBP conducted a technical demonstration on people inside vehicles moving less than 20 miles per hour entering and departing Anzalduas, Texas.

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 points at seaports.[27] 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 seven sea entry sites and five major cruise lines that are operating facial comparison cameras to confirm arriving passenger identity on closed-loop cruises, which begin and end in the same city. Cruise lines report passenger satisfaction feedback that indicate the debarkation process is significantly better than feedback from vessels not using the technology during debarkation. CBP continues engagement with cruise lines and port authorities to expand the technology to other businesses and locations.

Conclusion

DHS, in collaboration with the travel industry, is assertively moving forward in developing a comprehensive biometric exit system in the land, air, and sea environments that replace manual identity checks with facial comparison technology. Travelers are well aware that their picture is being taken for facial comparison purposes, and they have access to both basic and detailed information regarding CBP's collection of biometric information. Not only is CBP congressionally mandated to implement a biometric entry-exit system, such a system will enhance CBP's ability to accomplish its mission: to safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel. CBP's collaborative biometric efforts address the recommendations of *The 9/11 Commission Report*, specifically, 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."[28]

[26] DHS/CBP (November 2018), DHS/CBP/PIA-056 Traveler Verification Service (945.31 KB).

[27] Ibid.

[28] The 9/11 Commission, *The 9/11 Commission Report*, pp. 385-386, http://govinfo.library.unt.edu/911/report/911Report.pdf. (7.22MB).