United States Government Accountability Office

Report to Congressional Requesters

September 2020

FACIAL RECOGNITION

CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues

GAO-20-568

GAO Highlights

Highlights of GAO-20-568, a report to congressional requesters

Why GAO Did This Study

Within the Department of Homeland Security (DHS), CBP is charged with the dual mission of facilitating legitimate travel and securing U.S. borders, and TSA is responsible for protecting the nation's transportation system. For both CBP and TSA, part of their inspection and screening responsibilities includes reviewing travel identification documents and verifying traveler identities. Beginning in 1996, a series of federal laws were enacted to develop and implement an entry-exit data system, which is to integrate biographic and, since 2004, biometric records for foreign nationals. This report addresses (1) the status of CBP's deployment of FRT, (2) the extent to which CBP has incorporated privacy protection principles, (3) the extent to which CBP has assessed the accuracy and performance of its FRT, and (4) the status of TSA's testing and deployment of FRT and how TSA has incorporated privacy protection principles. GAO conducted site visits to observe CBP's and TSA's use of FRT, which were selected to include all three travel environments—air, land, and sea; reviewed program documents; and interviewed DHS officials.

What GAO Recommends

GAO is making five recommendations to CBP to (1) ensure privacy notices are complete, (2) ensure notices are available at locations using FRT, (3) develop and implement a plan to audit its program partners for privacy compliance, (4) develop and implement a plan to capture required traveler photos at air exit, and (5) ensure it is alerted when air exit performance falls below established thresholds. DHS concurred with the recommendations.

View GAO-20-568. For more information, contact Rebecca Gambler at (202) 512-8777 or gamblerr@gao.gov.

September 2020

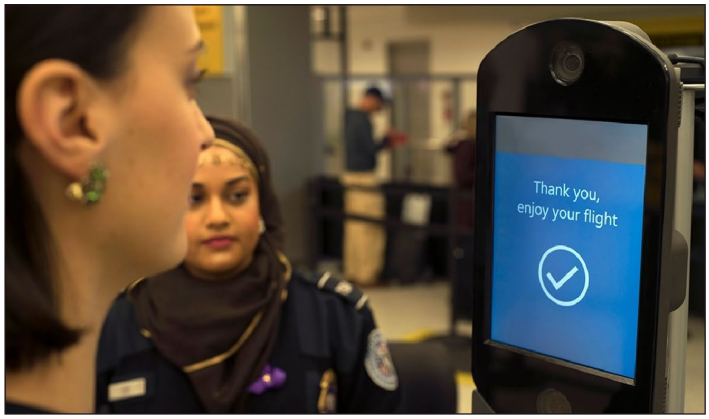
FACIAL RECOGNITION

CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues

What GAO Found

U.S. Customs and Border Protection (CBP) has made progress testing and deploying facial recognition technology (FRT) at ports of entry to create entry-exit records for foreign nationals as part of its Biometric Entry-Exit Program. As of May 2020, CBP, in partnership with airlines, had deployed FRT to 27 airports to biometrically confirm travelers' identities as they depart the United States (air exit) and was in the early stages of assessing FRT at sea and land ports of entry.

Facial Recognition Technology in Use at an Airport



Source: U.S. Customs and Border Protection. | GAO-20-568

CBP has taken steps to incorporate some privacy principles in its program, such as publishing the legislative authorities used to implement its program, but has not consistently provided complete information in privacy notices or ensured notices were posted and visible to travelers. Ensuring that privacy notices contain complete information and are consistently available would help give travelers the opportunity to decline to participate, if appropriate. Further, CBP requires its commercial partners, such as airlines, to follow CBP's privacy requirements and can audit partners to assess compliance. However, as of May 2020, CBP had audited only one of its more than 20 airline partners and did not have a plan to ensure all partners are audited. Until CBP develops and implements an audit plan, it cannot ensure that traveler information is appropriately safeguarded.

CBP has assessed the accuracy and performance of air exit FRT capabilities through operational testing. Testing found that air exit exceeded its accuracy goals—for example, identifying over 90 percent of travelers correctly—but did not meet a performance goal to capture 97 percent of traveler photos because airlines did not consistently photograph all travelers. A plan to improve the photo capture rate would help CBP better fulfill the program's mission of creating biometrically confirmed traveler departure records. Further, while CBP monitors air exit's performance, officials are not alerted when performance falls short of minimum requirements.

The Transportation Security Administration (TSA) has conducted pilot tests to assess the feasibility of using FRT but, given the limited nature of these tests, it is too early to fully assess TSA's compliance with privacy protection principles.

Contents

Tables

Figures

Abbreviations

CBP	U.S. Customs and Border Protection
COVID-19	Coronavirus Disease 2019
DHS	Department of Homeland Security
FIPP	Fair Information Practice Principles
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-Operation and Development
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
TSA	Transportation Security Administration
TVS	Traveler Verification Service

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 2, 2020

The Honorable Ron Johnson
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

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

Facial recognition technology has become increasingly common across business and government sectors as a tool for identifying or verifying customers or persons of interest, for example. Two components within the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) and the Transportation Security Administration (TSA), are pursuing facial recognition technology to automatically verify a traveler's identity in place of a visual inspection of travel identification documents. Traditionally, CBP and TSA have relied on biographic information (i.e., name or date of birth) on travel documents to verify that a traveler is who they claim to be. According to CBP and TSA, automating the identity verification process using facial recognition technology could help increase their ability to detect fraudulent travel identification documents, as well as expedite identity verification processes.

CBP is the lead federal agency charged with the dual mission of facilitating legitimate trade and travel at our nation's borders while also keeping terrorists and their weapons, criminals and contraband, and other inadmissible individuals out of the country. TSA is responsible for protecting the nation's transportation systems, which includes screening airline passengers and their carry-on and checked baggage for prohibited items that could pose a threat to aircraft and passengers. Both CBP and TSA are responsible for inspecting millions of travelers each day—CBP typically inspects more than 2 million international travelers arriving at air,

sea, and land ports of entry each day, while TSA screens more than 2 million passengers traveling through airport checkpoints each day.[1]

CBP officers responsible for inspecting international travelers—foreign nationals and U.S. citizens—arriving at ports of entry review travelers' identification documents, including passports, visas or other entry permits, to verify their identities; determine their admissibility to the United States; and create entry records, among other things. To accomplish these tasks, CBP collects biographic information, such as name and date of birth, from both foreign nationals and U.S. citizens, and biometric information, such as fingerprints and photographs, from foreign nationals as they enter the country.[2] Additionally, CBP is responsible for confirming foreign national departures to determine if their exit occurred by expiration of the authorized period of stay as defined by their temporary status. A foreign national in the United States on a temporary basis who remains in

[1]Ports of entry are facilities that provide for the controlled entry into or departure from the United States. Specifically, a port of entry is any officially designated location (seaport, airport, or land border location) where CBP officers clear passengers, merchandise and other items; collect duties; enforce customs laws; and inspect persons entering or applying for admission into the United States pursuant to U.S. immigration and travel controls.

[2]We use the term foreign national in this report to refer to an alien (someone who does not have U.S. citizenship or nationality) seeking entry into the United States on a temporary basis pursuant to a nonimmigrant category (i.e. foreign visitor), such as tourists, diplomats, international students, or exchange visitors, among other types of nonimmigrant travelers. Lawful permanent resident aliens are also in-scope for biometric collection and included in the definition of foreign nationals. An "in-scope" traveler is any person who is required by law to provide biometrics upon entry to the United States pursuant to 8 C.F.R. § 235.1(f)(1)(ii) or exit from the United States pursuant to 8 C.F.R. § 215.8(a)(1). Under statute, the entry-exit system is to include a requirement for collection of biometric exit data for all categories of individuals who are required to provide biometric entry data. See 8 U.S.C. § 1365b(d). In-scope travelers include any alien other than those specifically exempt, as outlined in the regulation. Among other individuals, travelers younger than 14 or older than 79 on the date of admission or departure are exempt under the regulations. See 8 C.F.R. §§ 215.8(a)(2), 235.1(f)(1)(iv).

the country beyond their authorized period of admission is classified as an overstay.[3]

According to CBP, more than one million international travelers exit the country daily, with approximately 300,000 departing by air. Reliable and accurate data about who exits the country is important for identifying overstays. However, CBP has generally only had access to biographic information—and not biometric information—about foreign nationals exiting the country, which may limit CBP's ability to identify overstays or to determine, for example, if a foreign national has used fraudulent travel identification documents.

Beginning in 1996, a series of federal laws were enacted to develop and implement an entry-exit data system, which is to integrate biographic and, since 2004, biometric records of foreign nationals entering and exiting the country and to identify overstays.[4] CBP is the component within DHS that has primary responsibility for entry-exit policy and operations, including implementation of a biometric entry-exit system. Since 2004, DHS has tracked foreign nationals' entries into the United States as part of an effort to comply with legislative requirements and, since December 2006, a biometric entry capability has been fully operational at all air, sea, and land ports of entry. However, in previous reports we have identified long-standing challenges to DHS developing and deploying a biometric exit capability to create biometric records for foreign nationals when they

[3]A foreign national overstays by: (1) failing to depart by the status expiration date or completion of qualifying activity (plus any time permitted for departure) without first obtaining an extension or other valid immigration status or protection, or (2) violating the terms and conditions of their visitor status at any point during their stay. Certain individuals are allowed to seek admission without a visa, such as citizens of Canada, as well as participants in the Visa Waiver Program, through which nationals of certain countries may apply for admission to the United States as temporary visitors for business or pleasure without first obtaining a visa from a U.S. embassy or consulate abroad. See 8 U.S.C. § 1187; 8 C.F.R. §§ 212.1, 214.6(d), 217.1-217.7; 22 C.F.R. §§ 41.0-41.3.

[4]Under 8 U.S.C. § 1365b(d), the entry and exit data system is to require the collection of biometric exit data for all categories of individuals who are required to provide such entry data, regardless of the port of entry. For categories of individuals required to provide biometric entry and departure data, see 8 C.F.R. §§ 215.8 (DHS authority to establish pilot programs at land ports and at up to 15 air or sea ports, requiring biometric identifiers to be collected from aliens on departure from the United States) 235.1(f) (any alien may be required to provide biometric identifiers on entry, except certain Canadian tourists or businesspeople; aliens younger than 14 or older than 79; and diplomatic visa holders, among other listed exemptions. Additionally, aliens required to provide biometric identifiers on entry may be subject to departure requirements for biometrics under § 215.8, unless otherwise exempted).

depart the country.[5] Most recently, in 2017, we reported that CBP had made progress in testing biometric exit capabilities, including facial recognition technology, but challenges continued to affect CBP's efforts to develop and implement a biometric exit system, such as differences in the logistics and infrastructure among ports of entry. As we previously reported, CBP had tested various biometric technologies in different locations to determine which type of technology could be deployed on a large scale without disrupting legitimate travel and trade, while still meeting its mandate to implement a biometric entry-exit system.[6] Based on the results of its testing, CBP concluded that facial recognition technology was the most operationally feasible and traveler-friendly option for a comprehensive biometric solution. Since then, CBP has prioritized testing and deploying facial recognition technology at airports (referred to as air exit), with seaports and land ports of entry to follow. These tests and deployments are part of CBP's Biometric Entry-Exit Program.

As part of TSA's mission to protect the nation's transportation systems and to ensure freedom of movement for people and commerce, TSA has been exploring facial recognition technology for identity verification at airport checkpoints. Since 2017, TSA has conducted a series of pilot tests—some in partnership with CBP—to assess the feasibility of using facial recognition technology to automate traveler identity verification at airport security checkpoints. In April 2018, TSA signed a policy memorandum with CBP on the development and implementation of facial recognition capabilities at airports.

Some academics and privacy advocates have raised concerns about privacy, accuracy, and individuals' civil liberties. Specifically, they have raised concerns about the privacy of U.S. citizens' information, travelers' rights to refuse biometric screening, the accuracy of this technology, and

[5]See GAO, *Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain*, GAO-17-170 (Washington, D.C.: Feb. 27, 2017); *Border Security: Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System*, GAO-16-358T (Washington, D.C.: Jan. 20, 2016); and *Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program*, GAO-13-683 (Washington, D.C.: July 30, 2013).

[6]Specifically, from 2014 to 2016, CBP tested facial recognition, iris scanning, and mobile fingerprint readers in simulated operational conditions at air and land ports of entry. CBP used the results from each test to gauge the feasibility of real-time biometric identification that is traveler-friendly and easy to deploy for travel industry partners.

whether certain demographic groups are more likely to be mismatched (e.g., minority groups or women).

You asked us to review CBP's and TSA's facial recognition technology capabilities for traveler identity verification. This report addresses (1) the status of CBP's testing and deployment of facial recognition technology at ports of entry, (2) the extent to which CBP's use of facial recognition technology has incorporated privacy principles consistent with applicable laws and policies, (3) the extent to which CBP has assessed the accuracy and performance of its facial recognition capabilities at ports of entry, and (4) the status of TSA's testing of facial recognition capabilities and the extent to which TSA's facial recognition pilot tests incorporated privacy principles.

To address the first three objectives on CBP's facial recognition capabilities for traveler identification, we analyzed Biometric Entry-Exit Program documents such as schedules, pilot testing reports, Privacy Impact Assessments, and a statutorily required CBP-TSA report to Congress on the use of facial recognition technology.[7] We also conducted site visits to the following ports of entry to observe CBP's testing and implementation of facial recognition technology for traveler screening:

Air Ports of Entry

- Hartsfield-Jackson International Airport; Atlanta, Georgia
- McCarran International Airport; Las Vegas, Nevada
- Orlando International Airport; Orlando, Florida

Sea Port of Entry

- Port Canaveral Port of Entry; Port Canaveral, Florida

Land Port of Entry

- Nogales Port of Entry; Nogales, Arizona[8]

[7]Department of Homeland Security, *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies*, Report to Congress (Washington, D.C.: Aug. 30, 2019); Section 1919(c) of the *FAA Reauthorization Act of 2018* (P.L. 115-254).

[8]At the Nogales Port of Entry, we visited the Dennis DeConcini Crossing, Mariposa Passenger Processing Facility, and the Morley Pedestrian Crossing.

We selected these locations because they allowed us to observe CBP's facial recognition pilot-testing or implementation across each of the three travel environments (air, sea, and land).[9] In the air environment, we selected airports that would allow us to observe different types of facial recognition technology equipment and configurations. In the sea environment, we selected Port Canaveral because of the availability of a cruise ship arriving at port during our site visit. In the land environment, CBP was conducting facial recognition pilot-testing at two locations during the time of our review (Nogales and San Luis). We selected Nogales, since that location was the larger of the two and allowed us to observe the identity verification process involved in both pedestrian and vehicle crossings. At these locations, we interviewed local CBP officials about their experiences with facial recognition technology. Although our observations from these site visits are not generalizable to all locations testing or using facial recognition technology, the observations provide useful insights about the status of testing and deployment, how privacy protections were implemented at these locations, and the accuracy of facial matching. We also interviewed officials from CBP's Biometric Entry-Exit Program, which is responsible for developing and implementing biometric solutions for traveler identification.

To obtain stakeholder perspectives on CBP's implementation of facial recognition technology for identity verification at airports, we spoke with officials from Delta Air Lines, which has been a commercial partner for CBP's Biometric Entry-Exit Program since 2016 and recently became the first airline to begin testing the use of facial recognition at the self-service check-in area. We also interviewed officials from Airlines for America, which is an airline industry organization.

To address our first objective, we reviewed statutory requirements for a biometric entry-exit system and analyzed program documentation, including status briefings, schedules, and program requirements. We conducted site visits to observe CBP's pilot tests and deployments of facial recognition technology, as noted above. In addition, we interviewed officials from DHS offices who were involved in testing, implementing, or assessing CBP's facial recognition technology efforts, including the Office

[9]We also selected these locations, and the timing of our site visits, based on CBP's and TSA's facial recognition testing schedules and availability. At the time of our review, only one test demonstration was underway at a sea port of entry. In addition, we selected airports to visit where TSA was also conducting its facial recognition pilot tests—specifically, at Hartsfield-Jackson Atlanta International Airport and Las Vegas McCarran International Airport.

of Biometric Identity Management, the Office of Information and Technology, and the DHS Science and Technology Directorate. We also reviewed prior GAO reports and a DHS's Office of Inspector General report on CBP's previous efforts to develop and implement a biometric entry-exit system.

To address our second objective, we reviewed the Fair Information Practice Principles (FIPP) adopted by the DHS Chief Privacy Officer and assessed the extent to which CBP had included these principles in the Biometric Entry-Exit Program.[10] Specifically, we reviewed CBP privacy documents related to the use of facial recognition technology, including Privacy Impact Assessments and applicable System of Records Notices. We also reviewed the results of a February 2019 report on CBP's air exit operations conducted by the DHS Data Privacy and Integrity Advisory Committee. At the ports of entry we visited, we observed facial recognition technology in use for traveler identification and the privacy notifications (such as signs and announcements) provided by CBP and its commercial partners. At these locations, we spoke with CBP officers and airline and cruise line personnel to understand their experiences with the technology and issues related to traveler privacy protections. We also reviewed examples of notices provided to travelers by CBP or their commercial partners during pilot tests conducted prior to the start of our review. To determine whether CBP's website and call center provided accurate information on the ports of entry where CBP had tested or implemented facial recognition technology, we accessed CBP's website and called the CBP Info Center phone line in November 2019 to inquire about CBP's Biometric Entry-Exit Program. We compared our observations and findings to the FIPPs.

Finally, to gain insight into privacy protections and issues related to CBP's use of facial recognition technology, we spoke with DHS's Privacy Office, CBP's Privacy Office, and privacy advocacy organizations selected on the basis of their expressed concerns with or public testimony on the use of facial recognition technology. These organizations included the American Civil Liberties Union, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and Georgetown University's Center on Privacy and Technology. We selected a nonprobability sample of organizations to interview and, therefore, the information gathered from

[10]See Department of Homeland Security, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,* DHS Privacy Policy Guidance Memorandum 2008-01 (Washington, D.C., Dec. 29, 2008).

advocacy organizations is not generalizable beyond those we interviewed, but provided insights regarding privacy issues.

To address our third objective, we reviewed available testing documentation for all of the Biometric Entry-Exit Program's segments. For air exit, these documents included the Operational Requirements Document, Biometric Air Exit Development Test Final Report, Test and Evaluation Master Plan, Operational Test and Evaluation Report, and a Letter of Assessment written by the DHS Director of Test and Evaluation. In addition, we reviewed reports by the DHS Science and Technology Directorate that analyzed algorithm performance and factors that can affect the accuracy of facial recognition verification. For other segments, we reviewed requirements documents and preliminary evaluation reports, among other documents. Additionally, we interviewed agency officials who contributed to CBP's operational test of air exit and CBP's pilot tests, such as the Biometric Entry-Exit Program office, the Land Systems Operational Test Authority (test agent for air exit), and the Director of Test and Evaluation for DHS.

To understand how CBP assessed the accuracy and performance of air exit—which was the first program capability to progress through the DHS acquisition process and undergo formal testing of accuracy and performance—we compared the requirements in the Operational Requirements Document to the results in the Operational Test and Evaluation Plan and Report. We also reviewed the calculations used to determine the air exit accuracy metrics and compared them to the calculations used by the National Institute of Standards and Technology (NIST) in similar assessments. As a result of our analyses, and interviews with officials involved in CBP's facial recognition accuracy testing, we determined that the data used to measure accuracy in the operational test were sufficiently reliable for the purposes of determining whether CBP adequately assessed the accuracy and performance of its facial recognition capabilities. To understand how CBP's facial matching algorithm will be tested for demographic effects on accuracy, we interviewed program officials about their internal assessments and reviewed the interagency agreement between CBP and NIST, which outlines the testing NIST will perform. We also interviewed officials from NIST and DHS's Office of Biometric Identity Management to obtain additional perspectives on factors to consider during facial recognition technology testing. We also reviewed NIST's *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* to better understand

demographic effects in facial recognition technology more generally.[11] Finally, we assessed CBP's process for monitoring the accuracy and performance of air exit against guidance in DHS's Systems Engineering Life Cycle Guidebook, which provides technical guidance for DHS components responsible for planning and executing systems engineering activities, as well as the *Standards for Internal Control in the Federal Government*.[12]

To address our fourth objective, we reviewed TSA biometric strategy and planning documents, such as TSA's Biometric Roadmap, which serves as TSA's overarching strategy for pursuing biometric technology, as well as test plans and results.[13] We also interviewed officials from TSA's Requirements and Capabilities Analysis office, which is leading TSA's biometrics efforts. In addition, we observed TSA's facial recognition pilot tests at the Hartsfield-Jackson Atlanta International Airport and the Las Vegas McCarran International Airport in July and September 2019 respectively—the two locations where TSA was conducting pilot tests at the time of our review. At these airports, we spoke to TSA officers who were involved in the pilot tests about their experience using the technology. To determine the extent to which TSA's facial recognition pilot tests incorporated privacy principles, we reviewed TSA privacy documents, including Privacy Impact Assessments. We also observed TSA's pilot tests, as noted above, and reviewed the privacy notifications, including handouts provided by TSA officials at these airports. Finally, to gain insight into privacy protections and issues related to TSA's use of facial recognition technology, we spoke to the privacy advocacy organizations mentioned above, as well as DHS's Privacy Office.

We conducted this performance audit from May 2019 to September 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

[11]National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 2019).

[12]Department of Homeland Security, *Systems Engineering Life Cycle Guidebook*, DHS Guidebook 102-01-103-01 (Washington, D.C.: Apr.18, 2016). GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[13]Transportation Security Administration, *TSA Biometrics Roadmap for Aviation Security and the Passenger Experience* (Washington, D.C.: September 2018).

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Statutes Related to the Biometric Entry-Exit System

As previously mentioned, since 1996, a series of federal statutes required the federal government to develop and implement an entry-exit data system to match arrival and departure records and report on its progress to Congress. This system is required to include biographic and biometric information of foreign nationals entering and exiting the country and be able to identify overstays—foreign nationals who come to the United States temporarily but then remain beyond their authorized period of stay.[14] The Intelligence Reform and Terrorism Prevention Act of 2004 required the Secretary of Homeland Security to develop a plan to accelerate full implementation of an automated biometric entry and exit data system that matches available information provided by foreign nationals upon their arrival in, and departure from, the United States.[15] The Consolidated Appropriations Act, 2016, required that DHS develop a comprehensive plan for implementation of a biometric entry and exit system and issue a report on overstay data.[16] The act also established a funding mechanism, making up to $1 billion available to the Secretary of Homeland Security through temporary fee increases for certain visa applications beginning in fiscal year 2017 to develop and implement a

[14]See, e.g., Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, div. C, tit. I, subtitle A, § 110, 110 Stat. 3009-546, 3009-558 to -559 (classified, as amended, at 8 U.S.C. § 1365a); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, tit. VII, subtitle B, § 7208, 118 Stat. 3638, 3817-23 (classified, as amended, at 8 U.S.C. § 1365b). The “authorized period of stay” can be for a specific length of time, which CBP designates by assigning a specific “admit until” date, or for as long as the visitor maintains compliance with the terms of a particular program or activity, the duration of which may be variable.

[15]Pub. L. No.108-458, tit. VII, subtitle B, § 7208, 118 Stat. 3638, 3817-23 (classified, as amended, at 8 U.S.C. § 1365b). A “biometric” refers to a method of identification based on anatomical, physiological, and behavioral characteristics or other physical attributes unique to a person that can be collected, stored, and used to verify the identity of a person.

[16]Pub. L. No.114-113, div. F, tit. I, 129 Stat. at 2493. Reported overstay data are to include overstays from all nonimmigrant categories, delineated by each class and subclass of such categories, and numbers as well as rates of overstays for each class/subclass by country.

biometric entry-exit system.[17] In addition, in 2017, Executive Order 13780 called for the expedited completion of the biometric entry-exit record system.[18]

CBP's Roles, Responsibilities, and Data Systems for Inspecting Travelers and Implementing a Biometric Entry-Exit System

At air, sea, and land ports of entry, CBP officers inspect international travelers arriving in the United States. Prior to their arrival, CBP obtains biographic information for all international travelers from DHS's Advance Passenger Information System, a database that collects passenger manifest data submitted by commercial and private aircraft operators and commercial sea carriers, as well as from other sources.[19] For foreign nationals specifically, CBP collects both biographic information (such as name, date of birth, and country of citizenship) and biometric information (such as fingerprints or a facial photo) to create arrival records.[20] Foreign national biographic data—including passenger manifest data from the Advance Passenger Information System and information collected by CBP officers during inspection—are sent to DHS's Arrival and Departure Information System, where they are stored for matching against departure records. DHS stores the biometric information of foreign nationals and some U.S. citizens in the DHS Office of Biometric Identity Management's

[17]Pub. L. No. 114-113, div. O, tit. IV, § 402(g), 129 Stat. at 3006-07. The act provided for temporary fee increases through September 30, 2027, of $4,500 and $4,000 for L-1 and H-1B visa applications, respectively, for applicants that employ 50 or more employees in the United States if more than 50 percent of such employees are nonimmigrants admitted under 8 U.S.C. § 1101(a)(15)(H)(i)(b), (L). Fifty percent of the amounts collected pursuant to these fee increases are to be deposited as offsetting receipts into the 9-11 Response and Biometric Exit Account up to $1 billion, to be available until expended. For fiscal year 2017 and each fiscal year thereafter, amounts in the account shall be available to the Secretary of Homeland Security without further appropriation to implement the biometric entry and exit data system under 8 U.S.C. § 1365b.

[18]See Exec. Order No. 13780, Protecting the Nation From Foreign Terrorist Entry Into the United States, 82 Fed. Reg. 13,209 (Mar. 9, 2017) (issued Mar.6). Executive Order 13780 revoked and replaced Exec. Order No. 13769, 82 Fed. Reg. 8977 (Feb. 1, 2017) (issued Jan. 27).

[19]These manifests include every individual who actually boarded the airplane or ship bound for the United States. Since 2005, collection of this information has been mandatory. According to CBP, compliance by operators and carriers is nearly 100 percent. CBP also receives manifests for commercial vehicles at land ports of entry and may receive manifests from rail and bus carriers.

[20]U.S. citizens are not considered "in-scope" for the collection of biometric information when entering or exiting the country.

Automated Biometric Identification System.[21] When foreign nationals depart the United States by air and sea, CBP collects their biographic information through passenger manifests via the Advance Passenger Information System and stores it in the Arrival and Departure Information System. CBP can also collect some biographic information from foreign nationals departing by land.[22] Using primarily biographic information, CBP matches foreign nationals' arrival and departure records to determine if they have departed and to identify overstays among those who were visiting the United States on a temporary basis.

To meet its statutory requirement to implement a biometric entry-exit system, CBP has deployed a biometric entry capability (with fingerprints as the biometric) at almost all air, sea, and land ports of entry and is in the process of testing and deploying biometric exit capabilities at ports of entry using facial recognition technology. In May 2013, CBP's Office of Field Operations established an Entry-Exit Transformation Office (renamed the Biometric Entry-Exit Program Office in March 2017) to develop, test, and deploy facial recognition technology that would work across the air, sea, and land travel environments. CBP has divided the Biometric Entry-Exit Program into segments based on these three travel environments and is developing facial recognition capabilities for each segment.

Since 2015, CBP has tested several types of biometric technologies—including handheld fingerprint-scanning devices and iris scanning—before deciding to pursue facial recognition technology as its biometric capability. According to CBP, officials chose facial recognition technology because of its viability in each of the travel environments (air, sea, and land ports of entry) and the availability of existing traveler photos.

[21]The Office of Biometric Identity Management is the lead entity within DHS responsible for biometric identity management services through its management of the Automated Biometric Identification System, or IDENT. IDENT matches, stores, shares, and analyzes biometric information.

[22]In 2013, the United States and Canada began exchanging data on third-country nationals crossing the border at land ports of entry. As of July 2019, CBP receives travel data on all travelers who enter Canada from the United States at a land port of entry. While the United States cooperates with Canada to share information about travelers entering and exiting along the northern border, CBP does not have the same ability to share information with Mexico along the southern border. When CBP receives information about a traveler crossing into Canada from Canadian officials, CBP can record that traveler as having exited the country without needing to process them itself. As we reported in 2013, the southern border poses unique challenges that make a similar approach difficult to implement.

In 2017, CBP developed and implemented the Traveler Verification Service (TVS) as its facial recognition matching service and is testing and deploying TVS in segments, based on the air, sea, and land travel environments at ports of entry. TVS is a facial matching service that compares a traveler's live photo to photos in DHS databases, such as passport photos, or to a photo embedded in a travel identification document. CBP plans to use TVS as the facial matching service for all travel environments but has prioritized testing and deploying facial recognition technology in the air environment.

While regulations limit CBP's collection of biometric information to certain in-scope foreign nationals entering and exiting the United States, CBP's biometric entry-exit capabilities may also capture biometric data (facial images) from exempt foreign nationals and U.S. citizens. However, exempt foreign nationals and U.S. citizens are routinely able to "opt out" of using this technology to verify identity and can instead choose a manual check of documentation for identity verification. As such, we refer to individuals from whom CBP collects facial image data as international travelers or travelers throughout this report. Historically, CBP has not collected biometric data from U.S. citizens on arrival or departure from the United States. Currently, U.S. citizens are not exempt from its facial matching capabilities, although they may opt out, because CBP sees facial recognition technology as transforming the identity verification process generally from a manual document check by airline personnel (on exit) or CBP officers (on entry) into an automated process. According to CBP, automated facial recognition for identity verification can help ensure that U.S. citizen travelers are the person they claim to be when they present their passport.

How Facial Recognition Technology Works

Facial recognition technology uses an image or video of a person's face to identify them or verify their identity. Facial recognition, like fingerprints, is a form of biometric identification that measures and analyzes physical attributes unique to a person that can be collected, stored, and used to confirm the identity of that person. Facial recognition technology uses a photo or video of a person—often called a probe or live photo—and converts it into a template, or a mathematical representation of the photo.[23] For some facial recognition functions, if the technology detects a face, a matching algorithm then compares the template to a template

[23]Templates are generated according to the vendor-provided algorithm, and it is very difficult, if not impossible, to convert back to the original photo.

from another photo and calculates their similarity.[24] Facial recognition matching generally falls into one of two types: the first, known as "one-to-many" or "1:N" matching, compares a live photo against a number (N) of photos in a gallery to determine if there is a match (identification of a particular face among many photos). The second, known as "one-to-one" or "1:1" matching, compares a live photo to another photo of the same person (verification of a face against a source photo).

While NIST has not set standards for how accurate a facial recognition system should be, NIST has conducted research into the accuracy of facial recognition algorithms since 2000. NIST is a government laboratory that has evaluated hundreds of commercial facial matching algorithms for accuracy and speed. A recent NIST evaluation in December 2019 focused on testing the effects of demographics on matching accuracy of over 100 commercially available facial recognition algorithms.[25] NIST found that demographic effects in matching accuracy varied significantly across the algorithms it tested and that many facial recognition systems performed differently among demographic groups. While NIST did not evaluate TVS, it included a version of the algorithm CBP uses with TVS in its evaluation and found it was among the most accurate algorithms on many measures.[26] See appendix I for information about the results of NIST's analysis.

CBP's Implementation of Facial Recognition Technology

CBP has developed and implemented TVS to serve as the facial recognition matching service for the Biometric Entry-Exit Program. TVS is a cloud-based biometric matching service that uses an algorithm to compare live photos against existing photos and is designed to perform both 1:N and 1:1 facial recognition matching. With 1:N matching, TVS compares a live photo of a traveler against photos of multiple travelers in

[24]An algorithm is a set of rules that a computer or program follows to compute an outcome. Private companies have developed hundreds of facial recognition algorithms for a variety of uses. We have ongoing work reviewing commercial and law enforcement uses of facial recognition technology, as well as DHS's development of the Homeland Advanced Recognition Technology, a replacement system for IDENT. For more information on the commercial use of facial recognition technology see GAO, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522 (Washington, D.C.: July 13, 2020).

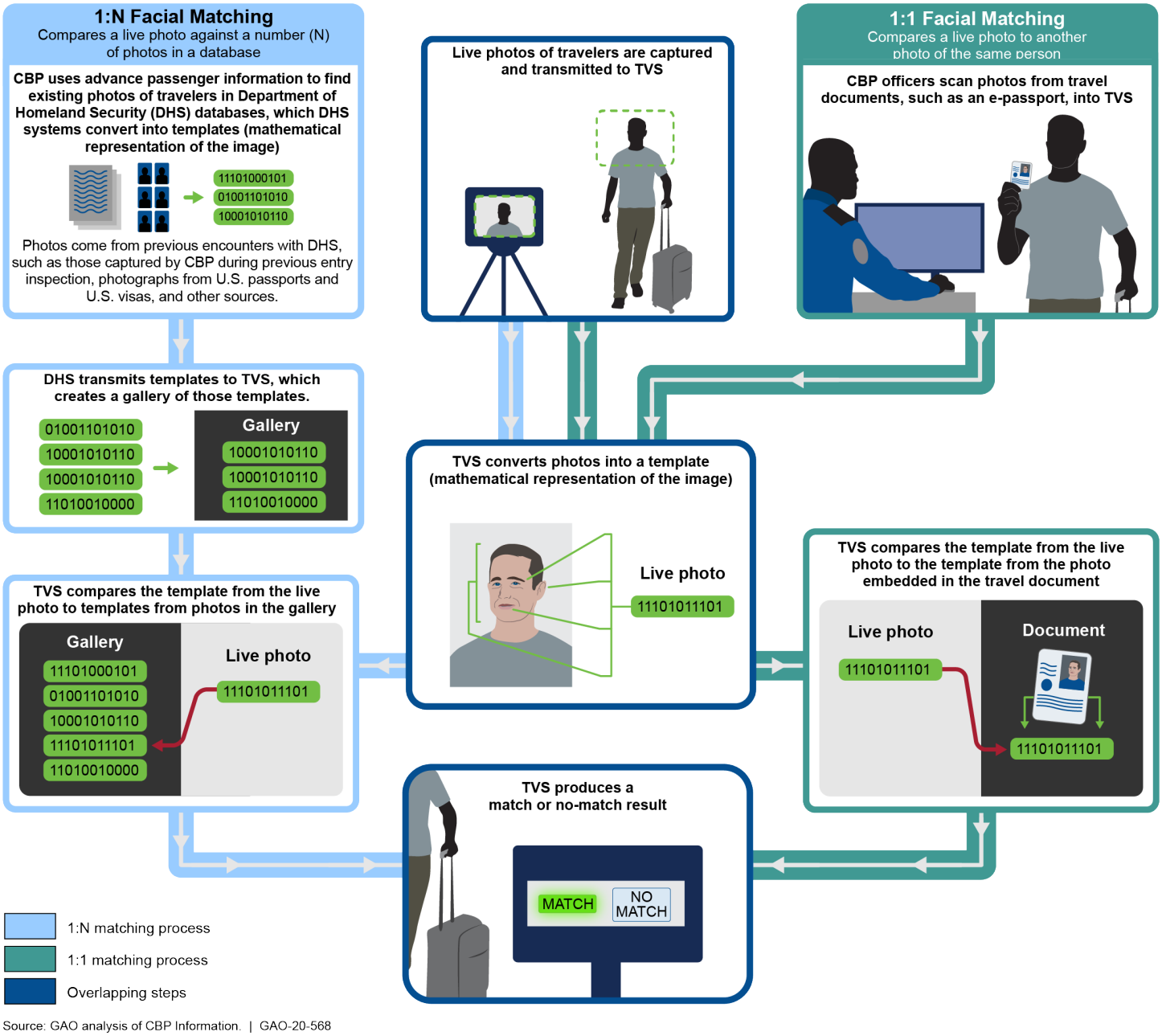
[25]National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (Dec. 2019).

[26]For additional information on the accuracy of facial recognition technology across demographics, see GAO-20-522.

a prestaged photo gallery. As previously mentioned, in the air and sea environments, CBP receives travelers' biographic information in advance of travel through passenger manifests submitted by commercial and private aircraft operators and commercial sea carriers. TVS searches DHS databases of photos associated with travelers listed on the manifest, and TVS then creates a prestaged "gallery" of templates created from those photos.[27] These may include photos previously captured by CBP during entry inspections, photos from U.S. passports and U.S. visas, or photos from other DHS encounters. For 1:1 matching, TVS compares a live photo of a traveler against another photo of that traveler, such as from a passport photo. This type of matching can be used when CBP does not have passenger manifest information and cannot create a gallery in advance or does not have an existing photo available for matching. Figure 1 shows how TVS performs facial matching.

[27]According to CBP officials, CBP has also begun creating galleries from commercial vehicle manifests in the land environment, as well as testing the feasibility of creating galleries based on frequent border crossers.

Figure 1: Illustration of How U.S. Customs and Border Protection's (CBP) Traveler Verification Service (TVS) Performs 1:N and 1:1 Facial Matching



Source: GAO analysis of CBP Information. | GAO-20-568

TSA's Assessment of Facial Recognition Technology for Identity Verification at Checkpoints

As part of its efforts to secure aviation transportation, TSA verifies domestic and international travelers' identities to grant them access to airport sterile areas.[28] At the Travel Document Checker position at the checkpoint, TSA Transportation Security Officers manually verify travelers' identities by comparing travelers to the photos on their travel identification documents and comparing the biographic information on travel identification documents to the biographic information on boarding passes. Transportation Security Officers also examine the security features of traveler credentials, check boarding passes and travel identification documents for authenticity, verify travelers' Secure Flight vetting status, and then direct travelers to the correct screening lane based on their vetting status.[29] TSA expects that facial recognition may help reduce the burden on Transportation Security Officers to verify travelers' identities, expedite security processes—resulting in shorter lines and reduced wait times—and increase TSA's ability to detect fraudulent travel identification documents.

In March 2017, CBP and TSA began evaluating facial recognition technology for identity verification at the TSA checkpoint. TSA's Requirements and Capabilities Analysis office is leading TSA's biometrics efforts. 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. In September 2018, TSA published its *Biometrics Roadmap*, which serves as TSA's overarching strategy for pursuing biometric technology, including its goals and objectives for incorporating facial recognition technology into its traveler screening operations.[30] The *Biometrics Roadmap* lays out four goals:

1. Partnering with CBP on biometrics for international travelers;

[28]The sterile area of the airport is the area that provides passengers access to boarding aircraft and is an area to which access is generally controlled through the screening of persons and property. See 49 C.F.R. § 1540.5.

[29]TSA began using Secure Flight in 2009 to screen passengers against high-risk lists to identify those who should be prohibited from boarding flights, and to identify those who should receive enhanced screening at airport checkpoints. According to TSA, Secure Flight screening is also designed to identify individuals presenting a lower risk to security for whom expedited screening may be appropriate.

[30]Transportation Security Administration, *TSA Biometrics Roadmap for Aviation Security and the Passenger Experience* (Arlington, VA: September 2018).

2. Operationalizing biometrics for TSA Pre✓® travelers;
3. Expanding biometrics to additional domestic travelers; and
4. Developing support infrastructure for biometric solutions.

Privacy Principles and Requirements

Several principles and requirements govern the protection of personal information by federal agencies, including CBP's and TSA's use of traveler photos. The Fair Information Practice Principles are internationally recognized voluntary principles that were first proposed for protecting the privacy and security of personal information in the United States in 1973 by a U.S. government advisory committee.[31] This advisory committee recommended enactment of a federal "Code of Fair Information Practice" applicable to automated personal data systems. In 1980, the Organisation for Economic Co-Operation and Development (OECD), an organization of 37 member countries, including the United States, developed a revised version that was widely adopted. While these principles are nonbinding and therefore not legal requirements, they provide a framework for balancing privacy with other interests. In 2013, the OECD developed a revised version of the principles.[32]

The FIPPs served as the basis for the Privacy Act of 1974, which governs the collection, maintenance, use, and dissemination of personal information by federal agencies.[33] The Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The Privacy Act requires agencies to publish a notice—known as a System of Records Notice—in the *Federal Register* identifying, among other things, the categories of individuals whose information is in the system of records and the type of

[31]The Fair Information Practice Principles include the following eight principles, which we explain in detail later in this report: transparency, purpose specification, individual participation, data minimization, use limitation, security, data quality and integrity, accountability and auditing.

[32]Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Paris, France: Sept. 23, 1980). OECD has been considering whether to revise or update its privacy guidelines to account for changes in the role of personal data in the economy and society.

[33]See Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a). The act generally prohibits (with a number of exceptions) the disclosure by federal entities of records about an individual without the individual's written consent and provides U.S. persons with a means to seek access to and amend their records.

data collected. Also, the E-Government Act of 2002 requires agencies to conduct Privacy Impact Assessments (PIA) that analyze how personal information is collected, stored, shared, and managed in a federal system.[34] Agencies are required to make their PIAs publicly available, if practicable.

DHS privacy policies also govern CBP's and TSA's use of facial recognition technology. For example, it is DHS policy to follow the FIPPs, which provide a framework for balancing the need for privacy with other public policy interests, such as national security and law enforcement.

DHS Acquisition Management Process

DHS's overall policy for acquisition management is outlined in Acquisition Management Directive 102-01 and its associated Instructional Manual 102-01-001.[35] DHS's Under Secretary for Management is currently designated as the department's Chief Acquisition Officer and, as such, is responsible for managing the implementation of the department's acquisition policies and acting as the acquisition decision authority for the department's largest acquisition programs.[36] DHS's acquisition life cycle includes a series of acquisition decision events that provide the acquisition decision authority with an opportunity to assess whether the program is ready to proceed. DHS requires programs to complete certain acquisition documents—such as life-cycle cost estimates, test and evaluation master plans, and acquisition program baselines—throughout the acquisition life cycle. A critical aspect of DHS's acquisition process is conducting tests and evaluations of capabilities to ensure they meet technical specifications and performance requirements before being handed over to end users, such as CBP officers. One type of testing—operational testing—is a field test used to identify whether a system can perform as required in a realistic environment against realistic threats. In June 2017, DHS approved the initiation of the Biometric Entry-Exit Program as a major acquisition program, and in May 2018, DHS approved air exit as its first capability for development. As a major acquisition program, CBP and the Biometric Entry-Exit Program are

[34]Pub. L. No. 107-347, title II, § 208, 116 Stat. 2899, 2921-23 (codified at 44 U.S.C. § 3501 note).

[35]Department of Homeland Security, *Acquisition Management Directive*, 102-01, Rev. 3.1 (Feb. 25, 2019); and *Acquisition Management Instruction*, 102-01-001, Rev. 1.1 (May 3, 2019).

[36]DHS's Under Secretary for Management serves as the acquisition decision authority for programs with life-cycle cost estimates of $300 million or greater.

required to follow DHS acquisition policy and guidance to test and deploy air exit capabilities.

Prior Audit Reports on CBP's Efforts to Develop a Biometric Entry-Exit System

Since 2013, we and the DHS Office of Inspector General have issued several reports on DHS's progress in developing a biometric exit capability, as well as its ability to track and report on overstays. These reports identified long-standing challenges related to funding and inadequate planning. Most recently, in September 2018, the DHS Office of Inspector General reported, among other things, that CBP had made progress in developing and implementing a facial recognition capability to track passengers as they depart the United States by air, but CBP was unable to biometrically match 15 percent of all passengers in its pilot program.[37] In our February 2017 report, we found that CBP made progress in testing biometric exit capabilities, but long-standing planning, infrastructure, and staffing challenges continued to affect CBP's efforts to develop and implement a biometric exit system.[38] In July 2013, we reported on DHS's progress in developing and implementing a biometric exit system, as well as DHS's efforts to identify and address potential overstays.[39] In our prior reports, we made recommendations to help ensure that a biometric exit capability was planned, designed, developed, and implemented in an effective and efficient manner and to strengthen DHS's efforts to identify and address overstays. DHS generally agreed with our recommendations and implemented or took actions to implement some of these recommendations.

CBP Has Begun Testing and Deploying Facial Recognition Technology at Ports of Entry

CBP is at varying stages of testing and deploying facial recognition technology for identity verification across the air, sea, and land travel environments. CBP has prioritized testing and deploying facial recognition technology in the air environment (the air segment of the Biometric Entry-Exit Program). According to CBP, as of March 2020, CBP, in partnership with airlines and airport authorities, has deployed facial recognition technology to 27 airports (at least one gate) for travelers exiting the United States and 18 airports for travelers entering the United States. With regard to the sea environment, CBP has been conducting pilot tests of facial recognition technology at six seaports since 2018. With regard to the land environment, CBP has also been conducting pilot tests of facial

[37]Department of Homeland Security Office of Inspector General, *Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide*, OIG-18-80 (Washington, D.C.: Sept. 21, 2018).

[38]GAO-17-170.

[39]GAO-13-683.

recognition technology for entry and exit identity verification. CBP is in the early stages of evaluation in the sea and land environments, given the logistical challenges specific to those environments, as discussed below.

Each travel environment has unique characteristics and logistics that affect CBP's testing and deployment of facial recognition technology. For example, international travelers can enter and exit the United States by various modes, such as walking or driving across land border crossings, debarking or embarking cruise ships and other vessels at sea ports, or taking international flights to or from U.S. airports. While CBP has infrastructure in place at ports of entry to support inspecting international travelers as they enter the United States, such as inspection booths at international airports, it does not have infrastructure in place at many ports of entry to collect biographic or biometric information from international travelers as they exit. Additionally, in the air and sea environments, CBP knows who will be entering or exiting in advance from passenger manifests, but for the land environment, CBP does not receive manifests for international travelers crossing the land border on foot or in personally owned vehicles, thus limiting its ability to create galleries for matching photos.

CBP plans to use TVS as its facial matching service for all travel environments. If CBP has access to advance passenger manifest information, such as for international travelers entering or exiting the country by air or sea, TVS will build galleries of photos based on upcoming flight or vessel arrivals or departures. If CBP does not have access to advance passenger information, such as for pedestrians or privately owned vehicles at land ports of entry, TVS can build galleries using photos of frequent crossers for that specific port of entry, although CBP has not begun testing this capability.

In general, the facial matching process is similar across travel environments. When travelers present themselves for entry or exit, they will encounter a camera connected to TVS. U.S. citizens and otherwise exempt travelers can request to opt out of facial recognition identity verification, and CBP may grant such requests on a case-by-case basis.[40] The camera may be owned by CBP; the air or vessel carrier; or another

[40]U.S. citizens, children (both U.S. citizen and non-U.S. citizen) under the age of 14, adults over 79, some Canadian citizens, and other limited categories of foreign travelers can request to opt out of facial recognition identity verification. For air exit, foreign nationals can also opt out when facial recognition is conducted by a third party, such as an air carrier, but may still be required to provide some form of biometrics.

government agency, such as TSA. Once the camera captures a quality photo and TVS successfully matches it with a photo in the gallery associated with that particular manifest, travelers proceed to inspection for admissibility by a CBP officer or exit the United States.

Air Exit

Beginning in 2017, CBP partnered with airlines and airport authorities to deploy facial recognition for identity verification at airport departure gates. CBP designed TVS to integrate with existing airline and airport systems and minimize disruptions during the boarding process. CBP's program partners are responsible for purchasing the cameras to capture facial images from departing international travelers and facilitating the facial recognition identity verification process at gates.[41] As a formal DHS acquisition program, in December 2019, CBP received approval from DHS leadership to fully deploy air exit, with a total life cycle cost of $1.241 billion for the air environment, according to CBP.[42]

Status. According to CBP, as of May 2020, CBP had deployed facial recognition capabilities to 27 airports (at least one gate or air carrier conducting facial recognition identity verification at each airport). As of May 2020, over 7 million travelers departing the United States on 54,000 flights have been biometrically verified. See appendix II for a list of airport locations using facial recognition technology to verify passenger identities as of May 2020.

Process. TVS stages photo galleries of international travelers on a departing flight 6 hours in advance and continuously updates the gallery in case travelers are added to the flight. During boarding, each traveler stands for a photo in front of a camera connected to TVS. Aided by airline gate agents or airport personnel, the camera attempts to capture a usable live photo of the traveler and submits the photo to TVS. TVS compares the live photos to the photos in the prestaged gallery and produces a

[41]As of April 2020, CBP officers had conducted facial recognition identity verification for international travelers boarding flights at 12 airports where an airline had not yet partnered with CBP, according to CBP officials. For example, we observed CBP officers conducting facial recognition identity verification at one air exit gate at the Las Vegas McCarran International Airport. CBP officials said they do this as a way to introduce airports or airlines who have not yet partnered with CBP to the process and to encourage them to participate.

[42]This is an increase of $524.5 million from CBP's earlier baseline cost goal of $716.8 million in May 2018. According to CBP, costs associated with program and project management, system deployment and implementation, technology, and the inclusion of additional air entry costs, contributed to the increase.

match or no-match result (displayed as a blue or green light).[43] Travelers who are not matched by TVS after repeated attempts are manually verified by airline agents.[44]

Evaluations. CBP conducted developmental testing of air exit capabilities in June 2016 and established system accuracy and performance requirements in December 2017.[45] According to DHS policy, acquisition programs, such as the Biometric Entry-Exit Program's air exit facial recognition capability, must be assessed against program requirements in an operationally realistic environment before they can be fully deployed. An independent test agent conducted formal testing of air exit's accuracy and performance in an operational environment from May to June 2019. (This testing is described in more detail later in this report.)

Future plans. CBP's next formal acquisition milestone for air exit is to achieve full operational capability, meaning full delivery of the system according to program requirements. As of the time of this report, CBP's goal was to achieve full operational capability by the end of fiscal year 2021, though officials noted that this date was subject to change because of the Coronavirus Disease 2019 (COVID-19) pandemic, among other factors.[46] According to CBP officials, CBP has already met some of the program requirements needed to achieve full operational capability. For example, CBP has deployed biometric matching for international air departures at the 20 largest U.S. airports (by passenger volume) and demonstrated the ability to use facial recognition technology to verify the identities of 97 percent of all international travelers, according to CBP

[43]Facial recognition equipment at air exit does not display any personal information about the traveler.

[44]Airline agents may make multiple attempts to capture a useable photo of a traveler before resorting to manual identity verification.

[45]In addition to testing required by the acquisition process, CBP asked the DHS Science and Technology Directorate to analyze the algorithm used in TVS. From 2018 to 2019, the DHS Science and Technology Directorate performed testing to determine how different factors, such as gallery size and flight destination, can affect accuracy.

[46]According to CBP officials, the COVID-19 pandemic has slowed these efforts, as the air travel industry is facing severe financial hardships that could make investments in biometric technology harder to justify. Officials added that CBP is continuing to evaluate an alternative where CBP owns, operates, and maintains biometric matching technology at the departure gates for those airlines and airports unable or unwilling to enter into the public-private partnership.

officials.[47] CBP officials said that because airlines and airport authorities currently participate voluntarily, CBP does not require that they use facial recognition technology to verify the identity of every in-scope international traveler that boards a flight.[48] As such, CBP officials said that full operational capability for air exit is defined as the *ability* to biometrically process 97 percent of in-scope travelers departing the United States (as opposed to actually processing 97 percent of travelers). Nevertheless, officials said they continue to engage with airlines and airport authorities to expand the number of commercial partners and international flights participating in the program to increase the number of international travelers whose identities are biometrically confirmed.[49]

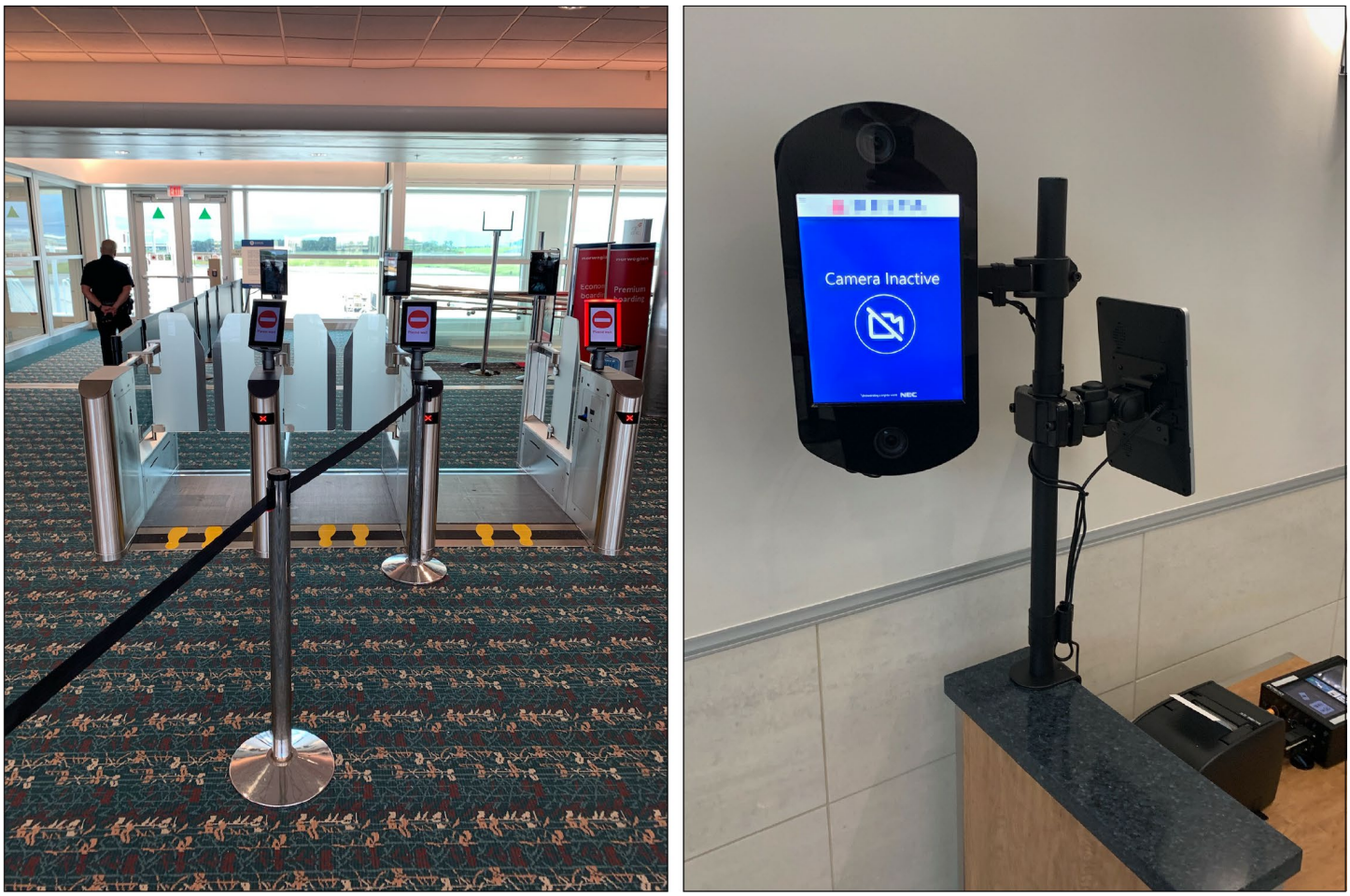
See figure 2 for examples of the facial recognition equipment we observed during our site visits to the Orlando International Airport in August 2019 and the Hartsfield-Jackson Atlanta International Airport in July 2019.

[47]According to CBP officials, TVS currently builds photo galleries for all international flights departing and arriving at U.S. airports daily, whether or not travelers on those flights are biometrically processed.

[48]An "in-scope" traveler is any person who is required by law to provide biometrics upon entry to the United States pursuant to 8 C.F.R. § 235.1(f)(1)(ii) or exit from the United States pursuant to 8 C.F.R. § 215.8(a)(1). Under statute, the entry-exit system is to include a requirement for collection of biometric exit data for all categories of individuals who are required to provide biometric entry data. See 8 U.S.C. § 1365b(d). In-scope travelers include any alien other than those specifically exempt, as outlined in the regulation. Among other individuals, travelers younger than 14 or older than 79 on the date of admission or departure are exempt under the regulations. See 8 C.F.R. §§ 215.8(a)(2), 235.1(f)(1)(iv).

[49]8 U.S.C. § 1365b provides that the biometric entry-exit system is to be integrated and comprehensive. Biometric exit screening is mandated for all travelers who are required to provide biometric entry data. See 8 U.S.C. §1365b (d); 8 C.F.R. § 215.8 (f). 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 the entry and departure of, and inspect, aliens and citizen travelers under sections 215 and 235 of the Immigration and Nationality Act (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)); and 8 U.S.C. § 1365b. Pursuant to section 215(a) of the INA (8 U.S.C. § 1185(a)), and Exec. Order No. 13323, 69 Fed. Reg. 241 (Dec. 30, 2003), 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.

Figure 2: Examples of Cameras Used for Air Exit Facial Recognition



Source: GAO. | GAO-20-568

Air Entry

In 2017, CBP introduced TVS into its entry inspection process for international travelers entering the United States by air. Both U.S. citizens and foreign nationals arriving in the United States on international flights are subject to inspection by CBP officers for compliance with immigration, customs, and agriculture regulations. CBP officers at primary inspection booths review travelers' documents and any information about them in DHS databases and, for foreign nationals, they create records of entry in the Arrival and Departure Information System. Since 2004, CBP has collected fingerprints and a facial photo from in-scope travelers entering the United States (foreign nationals, with some exceptions) as part of the

inspection process, which are added to their records of entry. With the integration of facial recognition technology, CBP officers use travelers' photos (for both U.S. citizens and foreign nationals) to initiate the inspection process—instead of their passport, for example—and verify their identity, before proceeding with their inspection.

Status. According to CBP, as of May 2020, CBP had deployed facial recognition technology to 18 airports for air entry.[50] As of December 2019, CBP officials said that they had verified over 16 million travelers on 210,000 arriving flights using facial recognition technology. Additionally, officials said facial recognition technology at air entry airports helped to identify seven impostors as of December 2019. CBP has also incorporated facial recognition technology into its Global Entry program.[51]

Process. TVS stages a photo gallery of all the travelers arriving on international flights at an airport in 1 day. At air entry locations, arriving air travelers proceed to CBP inspection areas, where cameras connected to TVS capture travelers' photos at primary inspection booths. TVS compares the live photos to the photos in the active prestaged gallery and produces a match or no-match result for the CBP officer. CBP officers attempt 1:1 facial matching using the photo in the traveler's passport or other travel identification document, if the 1:N match attempt is unsuccessful. According to CBP officials, travelers who are not matched by TVS are referred to secondary inspection, where they are verified manually by a CBP officer.[52]

Evaluations. CBP has tested the accuracy of TVS facial matching for air entry to determine system configurations and reviews air entry operational data on an ongoing basis to monitor performance, according

[50]Fourteen of these airports are within the United States, and four are abroad as part of CBP's preclearance program, where CBP personnel are stationed overseas to inspect travelers prior to boarding U.S.-bound flights. While CBP has the capability to use facial recognition technology for air entry identity verification at these 18 airports, CBP does not use this technology for all flights at all times.

[51]Global Entry is a CBP program that allows expedited clearance for preapproved, low-risk travelers upon arrival in the United States. CBP uses Global Entry kiosks to process eligible travelers entering the United States through designated airports. With the addition of facial recognition, travelers' photos are used to retrieve their record and verify their identity in place of their fingerprints.

[52]During the manual verification process, a CBP officer will conduct an inspection of the traveler, which includes a visual review of the traveler's documents to confirm that the traveler matches the photo on the travel document.

to CBP officials.[53] CBP officials said they were also evaluating the feasibility of "on-the-move" cameras (cameras that automatically capture a person's photo as they approach), as opposed to the existing "pause-and-capture" cameras (cameras that require a person to stop in front of it in order to capture their image) at inspection booths. CBP considers its air entry facial recognition operations to be an upgrade to CBP's existing entry process and infrastructure—a "technology refresh"—rather than a new system that would require formal operational testing.

Future plans. CBP officials told us that they have not set specific time frames for deploying facial recognition technology at additional airports. CBP officials said they are currently considering linking future deployments of air entry with air exit—that is, as additional airports partner with CBP for air exit, CBP would also deploy air entry facial recognition capabilities at those airports. Officials noted that because the information technology and communication systems requirements are similar for air entry and air exit, it may be more efficient and cost-effective to deploy both together at an airport.

See figure 3 for an example of the facial recognition equipment we observed during our site visit to the Las Vegas McCarran International Airport in September 2019.

[53]While configuring TVS for air entry in January 2018, CBP analyzed its accuracy by determining the false match rate (the rate photos were incorrectly matched) and the false non-match rate (the rate photos were not matched when they should have been). For 1:N facial matching at air entry, CBP found the false match rate was 0.023 percent, and the false non-match rate was 21.786 percent. For 1:1 facial matching at air entry, CBP found the false match rate was 0.014 percent, and the false non-match rate was 8.407 percent. The analysis used operational photos from 24 flights.

Figure 3: Example of a Camera Used for Air Entry Facial Recognition, Above a Fingerprint Scanner

Source: GAO. | GAO-20-568

Seaports

To create biometric entry-exit records in the sea environment, CBP is partnering with the cruise line industry to test and deploy a facial recognition capability similar to air exit. Cruise lines, like airlines, provide CBP with passenger manifests, which allows CBP to stage photo galleries of international travelers in advance of their arrival or departure from the United States. In 2018, CBP began testing facial recognition for identity verification using TVS for travelers reentering the United States on closed-loop cruises (sea entry). Closed-loop cruises are cruises that begin and end at the same U.S. port with the same travelers and are the most common type of cruise.[54] According to CBP officials, CBP's sea entry pilot tests are intended to help them evaluate the overall feasibility of facial recognition for identity verification in the sea environment, as well as to establish cost and system requirements.

Status. Six seaports and five major cruise lines are partnering with CBP on its sea entry pilot tests (that is, partners are purchasing cameras and operating facial recognition technology to verify arriving international travelers' identities on closed-loop cruises). CBP officials said, as of December 2019, over 2.6 million travelers from 702 vessels had been verified using facial recognition technology.

Process. TVS stages photo galleries of cruise line travelers arriving at seaports in advance of debarkation. Travelers stand for a photo in front of a camera connected to TVS as they debark (either on the ship or in the terminal). Aided by cruise line operators, the camera attempts to capture a usable live photo of the traveler and submits the photo to TVS. TVS compares the live photo to the photos in the prestaged gallery and produces a match or no-match result. Travelers who are not matched by TVS after repeated attempts are manually verified by CBP officers located at the port terminal. Travelers with young children, or those with no photo in the prestaged gallery, are guided to a separate line, where CBP officers manually verify the identities of travelers.[55]

Evaluations. CBP is conducting technical demonstrations (testing a working model of new technology in an operational environment) in the sea environment and has not formalized system requirements or program documents. CBP officials said that, as of May 2020, they are continuing to

[54]As of May 2020, CBP has not tested facial recognition technology for travelers exiting the United States (sea exit).

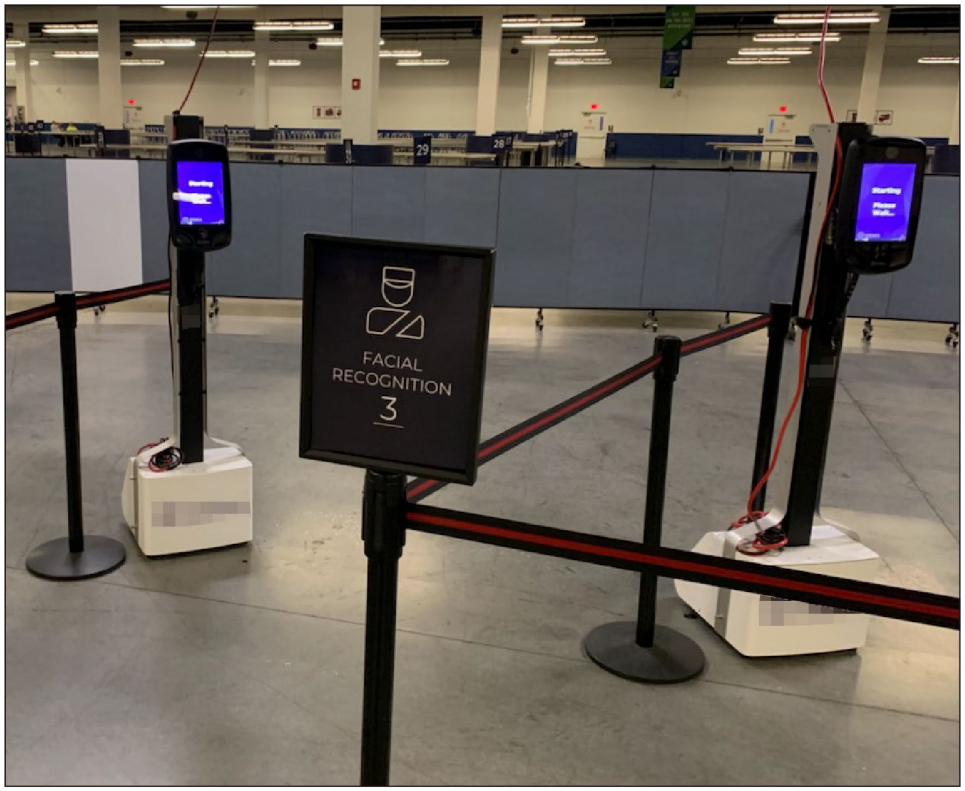
[55]During manual verification, a CBP officer will visually review a traveler's identification document to confirm that the traveler matches the photo on the document.

evaluate the results of facial recognition technology tests at seaports. CBP officials said the results will inform the final system design.

Future plans. CBP officials said they are working to expand the number of participating seaport locations, focusing on debarkation for closed-loop cruises. Officials said they will consider testing facial recognition technology for closed-loop embarkation and open-loop cruise routes (embarking in the United States and debarking in another country) in the future. Officials noted that cruise line and port authority participation in the program is voluntary, and they continue to engage with the industry to discuss privacy safeguards, cost considerations, and the benefits of the program. As of May 2020, officials said they were coordinating with DHS to develop a formal acquisition approach for the sea environment.

See figure 4 for an example of the facial recognition equipment we observed during our site visit to the Port Canaveral Terminal in Port Canaveral, Florida, in August 2019.

Figure 4: Example of Cameras and Display Screens Used for Facial Recognition at the Port Canaveral Seaport



Source: GAO. | GAO-20-568

Land Entry

While CBP has infrastructure in place for officers to inspect international travelers entering the United States at land ports of entry, whether on foot or in vehicles, there are no traveler manifests to support creating a gallery of known travelers in advance of their crossing. In 2018, CBP began testing facial recognition technology options using TVS for travelers entering the country through pedestrian and vehicle border crossings (referred to as pedestrian entry and vehicle land entry). CBP officials said the agency's pilot tests are intended to evaluate the feasibility of upgrading existing CBP equipment at primary inspection booths (similar to its efforts at air entry) to enable comparison of a live photo of a traveler to the photo on their travel identification document, or 1:1 facial matching. For travelers entering the United States in vehicles, CBP has conducted pilot tests to evaluate the feasibility of capturing travelers' photos while they drive through ports of entry.

Pedestrian entry

Status. As of May 2020, CBP had conducted pilot tests of facial recognition identity verification for pedestrians entering the United States at five southern border crossings.[56] According to CBP officials, between September 2018 and December 2019, CBP officials said using facial recognition, they had verified approximately 4.4 million travelers entering the country and had identified 215 impostors.[57]

Process. As travelers approach the primary inspection booth and present their travel identification documents, such as passports or visas, cameras connected to TVS attempt to capture live photos. CBP officers scan the traveler's identification document, which allows CBP's TECS system to locate the document photo.[58] Once the photo has been located, CBP's system sends the photo to TVS. TVS then compares the live photo against the document photo to produce a match or no-match result.[59] Travelers who are not matched by TVS instead have their identities verified manually (a visual inspection) by a CBP officer.

Evaluations. CBP is conducting technical demonstrations (testing a working model of new technology in an operational environment) in the land environment and has not formalized system requirements or program documents. CBP officials said one of the goals of the pilot tests was to evaluate whether "on-the-move" cameras (cameras that automatically capture a person's photo as they approach) could capture a sufficiently high-quality photo of a traveler as they approached the

[56]These border crossing were San Luis, Arizona (pilot began September 2018); Nogales, Arizona (pilot began October 2018); El Paso, Texas (pilot began November 2019); Laredo, Texas (pilot began December 2019); and Progreso, Texas (pilot began February 2020).

[57]According to CBP officials, facial recognition technology has allowed CBP officers to more accurately identify impostors attempting to use someone else's travel identification document. For example, CBP officials showed us photos of a traveler who attempted to cross a land port of entry using a fraudulent travel identification document while wearing Halloween makeup as a distraction. According to CBP officials, facial recognition technology helped confirm that the traveler was an impostor.

[58]The TECS System is the updated and modified version of the former Treasury Enforcement Communications System. TECS is owned and managed by CBP and is the principal system used by officers at the border to assist with screening and determinations regarding the admissibility of arriving persons.

[59]Any valid travel document that has a machine-readable zone or contains a radio frequency identification, including border crossing cards, can be utilized by TVS at the pedestrian entry screening area.

inspection booth to maintain the efficiency of the traveler verification process. CBP officials said that, as of February 2020, they are continuing to evaluate the results of facial recognition technology pilot tests at pedestrian border crossings.

Future plans. CBP officials said their ongoing pilot tests will help them determine how to implement facial recognition technology for pedestrian entry, including the optimal locations for cameras. Officials told us that camera placement in the land environment is challenging because primary inspection booths are arranged differently at different ports of entry. CBP officials also said they are exploring the feasibility of creating galleries of frequent border crossers for 1:N matching, instead of using travel identification documents for 1:1 matching.

See figure 5 for an example of the facial recognition equipment we observed during our site visit to the Nogales, Arizona, port of entry in September 2019.

Figure 5: Examples of Cameras Used for Facial Recognition at the Nogales, Arizona, Port of Entry

Source: GAO. | GAO-20-568

Vehicle Land Entry

Status. From August 2018 to February 2019, CBP conducted the first phase of a facial recognition technology pilot test in both inbound and outbound vehicle lanes of the Anzalduas port of entry in Texas. During this pilot, CBP took photos of approximately 315,000 travelers for facial recognition testing. CBP officials said they will focus testing on inbound

lanes (travelers entering the country) moving forward because CBP already has infrastructure (CBP inspection booths) in place to support it.[60]

Process. During the pilot at the Anzalduas port of entry, CBP installed camera equipment in both inbound and outbound vehicle lanes to capture photos of travelers in the front and back seats of vehicles moving at 20 miles per hour or less. For inbound lanes, CBP installed cameras just prior to the existing vehicle lane infrastructure. Photos captured by the cameras were provided to an offline version of TVS for testing purposes; the photos were not provided to CBP officers at the primary inspection booth and were not used for identity verification or entry decisions, according to CBP officials.

Evaluations. According to CBP program officials, CBP is in the technical demonstration phase (testing a working model of new technology in an operational environment) of program development in the land environment and has not formalized system requirements or program documents. According to CBP officials, the Anzalduas pilot showed that cameras were able to capture usable photos of travelers in the front seats of a vehicle 90 to 95 percent of the time and less than 50 percent of the time for travelers in the back seats.

Future plans. CBP officials said they plan to conduct additional pilots to determine the feasibility of using facial recognition technology to verify the identities of passengers crossing land ports of entry in vehicles. CBP is planning to pilot facial recognition technology for inbound entry lanes at the Anzalduas port of entry by the end of fiscal year 2020. According to CBP officials, this work builds on previous technical demonstrations, and seeks to inform CBP on the next steps to develop and implement a biometric entry-exit capability in the land border vehicular environment. In fiscal year 2020, the pilot will examine how identity information gathered through the cameras could be used to assist CBP officers in conducting border crossing inspections of vehicles and to help close out additional entry-exit records at land border ports of entry. Currently, CBP is working toward developing an acquisition approach for the land segment of the Biometric Entry-Exit Program.

[60]CBP is also testing facial recognition technology for travelers in commercial vehicles in at the Brownsville, Texas port of entry and at the Peace Bridge port of entry in Buffalo, New York.

Land Exit

As we described earlier, there are long-standing infrastructure and operational challenges to implementing a biometric exit capability at land ports. For example, many land ports do not have sufficient space to deploy equipment and staff for obtaining biometric information from individuals leaving the country, either by foot or by vehicle.

Because of these challenges, CBP officials said they have focused their efforts on evaluating facial recognition technology options for land entry. As of May 2020, the only test of facial recognition technology that CBP had conducted at land exit locations was the Anzalduas vehicle test, described above. For the outbound lanes, CBP had installed cameras just beyond the existing license plate reader at the Anzalduas port to test the cameras' abilities to capture photos of travelers in vehicles.[61] Officials said there were several challenges unique to outbound vehicle photo capture. For example, CBP officials said in some cases, drivers travel faster than 30 miles per hour at some border crossings, making photo capture more difficult.

CBP's Biometric Entry-Exit Program Incorporates Some Privacy Protection Principles, but Privacy Notices and Audits Are Inconsistent

CBP has incorporated some privacy protections into its Biometric Entry-Exit Program to protect the personally identifiable information of travelers during facial recognition identity verification. However, CBP has not consistently provided travelers with information about the locations where facial recognition is used, and CBP's privacy signage—which is intended to inform the traveling public of the use of facial recognition—provided limited information on how to request to opt out of facial recognition and were not always posted. In addition, CBP requires its commercial partners (such as airlines) and contractors to follow CBP's data collection and privacy requirements, such as restrictions on retaining traveler photos, and CBP can conduct audits to assess compliance. However, we found that CBP had audited only one of its commercial airline partners and did not have a plan to ensure that all partners are audited for compliance with the program's privacy requirements.

CBP's Biometric Entry-Exit Program Incorporated Some Privacy Protections

In accordance with the FIPPs, CBP has incorporated some privacy protections into its Biometric Entry-Exit Program. The FIPPs, adopted in a 2008 memorandum from DHS's Chief Privacy Officer, are the basis for the department's privacy policy. These principles are Transparency;

[61]According to CBP, travelers and CBP officers were not impacted by the pilot. CBP collected information solely for the purposes of facial match analysis and evaluation.

Individual Participation; Purpose Specification; Data Minimization; Use Limitation; Data Quality and Integrity; Security; and Accountability and Auditing. DHS requires its components—including CBP—to comply with the FIPPs when using personally identifiable information.[62] Examples of actions taken by CBP related to each of these principles are shown in table 1.

Table 1: U.S. Customs and Border Protection (CBP) Actions to Incorporate the Fair Information Practice Principles in the Biometric Entry-Exit Program

Principle and description	Examples of how CBP incorporated the principle in its Biometric Entry-Exit Program
Transparency: CBP should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).	• CBP published an updated Privacy Impact Assessment (PIA) in November 2018 for the Traveler Verification Service—CBP's facial matching system—that included information on privacy protections. • CBP has a website and frequently asked questions for the program. • CBP provides onsite signage to notify travelers about facial recognition. • CBP provides airline gate agents with a script for voice announcements about facial recognition.
Purpose specification: CBP should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.	• CBP's PIA and System of Record Notices identify the specific legal authorities that permit CBP's collection of biometrics to verify travelers' identities.
Individual participation: CBP 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. CBP should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.	• U.S. citizens and otherwise exempt foreign nationals may request to opt out of facial recognition identity verification at exit or entry locations by notifying either a CBP officer or an airline boarding agent and present travel identification documents for manual identity verification instead.[a] • Non-U.S. citizens between the ages of 14 and 79 are considered in-scope and are generally not permitted to opt out of facial recognition identity verification at ports of entry locations. For air exit, foreign nationals are permitted to opt out of facial recognition verification when it is conducted by a third party, such as an air carrier. • Travelers seeking access to their PII may file a Freedom of Information Act request with CBP. • Travelers seeking redress regarding the use of their PII may file an inquiry with the Department of Homeland Security Traveler Redress Inquiry Program.

[62]See Department of Homeland Security, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,* DHS Privacy Policy Guidance Memorandum 2008-01; and *Privacy Policy and Compliance,* DHS Directive 047-01-001 (Washington, D.C.: July 25, 2011). In 2017, DHS began treating all persons, regardless of immigration status, consistent with the FIPPs and applicable law. This step was taken in response to Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*, issued by the President on January 25, 2017, and which provides in relevant part that agencies may no longer extend the protections of the Privacy Act to those other than U.S. citizens and lawful permanent residents. See Exec. Order No.13768, § 14, 82 Fed. Reg. 8799, 8802 (Jan. 30, 2017).

Principle and description	Examples of how CBP incorporated the principle in its Biometric Entry-Exit Program

Data minimization: CBP 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).	• Photos are encrypted and transmitted to the Traveler Verification Service, which converts them into templates (a mathematical representation of the photo).
	• CBP does not permit commercial partners to store photos once they are transmitted to the Traveler Verification Service.
	• CBP's photo retention policies vary:
	  • For U.S. citizens, photos are to be stored in the facial matching system for a maximum of 12 hours, for disaster recovery purposes.[b]
	  • For foreign nationals, photos are to be stored in DHS's biometric information database for up to 75 years.

Use limitation: CBP 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.	• CBP's commercial partners are prohibited from storing or using travelers' photos for their own business purposes. • Commercial partners can only view a match/no match result. • CBP officials stated that PII collected through the Biometric Entry-Exit Program will be used primarily to verify a traveler's identity.
Security: CBP 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.	• CBP has system security plans for the Traveler Verification Service. • CBP uses two-factor authentication and encryption to transfer photos between the camera, the Traveler Verification Service, and CBP systems. • Photos are permanently converted into templates that cannot be converted back into the original photos. • In 2019, we found that it was not possible to fully evaluate cybersecurity and cyber resiliency in CBP's facial recognition system because these metrics are a recent addition to DHS's department-wide testing requirements.[c] In addition, during the operational test and evaluation of air exit, cybersecurity testing could not be conducted, but a follow on cyber resiliency test will be conducted once CBP fulfills all of its cybersecurity requirements.
Data quality and integrity: CBP should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.	• To help ensure higher accuracy rates, CBP compares traveler photos to a gallery of high-quality photos that travelers have already provided to the U.S. government to obtain a passport or visa. • CBP's commercial partners that deploy their own camera operators and camera technology must meet CBP's technical specifications and security requirements to connect with CBP's matching service. • CBP regularly tests the accuracy of its photo matching algorithms for accuracy.
Accountability and auditing: CBP 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.	• CBP's commercial partners must allow CBP to audit their compliance with program privacy and security requirements. • CBP's Privacy Office is conducting a broad review of privacy issues for the program and expects to report by the end of 2020.

Source: GAO analysis of CBP information. I GAO-20-568

[a]Generally, international travelers cannot decline to provide required information when arriving in or departing from the United States. However, there is no specific legal requirement for U.S. citizens to provide biometric identifiers upon entering or exiting the United States. Pursuant to CBP's immigration inspection and admission authority, an individual seeking entry into the United States must satisfy the CBP officer that they are a U.S. citizen, lawful permanent resident, or are otherwise permitted to enter the United States and that they are not attempting to import or export any merchandise in violation of U.S. laws.

[b]In July 2018, CBP reduced the photo retention period from 14 days to 12 hours for U.S. citizens.

[c]GAO, *Homeland Security Acquisitions: Outcomes Have Improved, but Actions Needed to Enhance Oversight of Schedule Goals*, GAO-20-170SP (Washington, D.C.: Dec. 19, 2019).

CBP's Privacy Notices to Inform the Public of Facial Recognition Contained Limited Privacy Information and Were Not Consistently Available

As noted above, CBP uses a variety of methods to provide privacy notices to travelers about the Biometric Entry-Exit Program and the use of facial recognition for traveler identification; however we identified limitations with their content and use. The FIPPs of transparency and individual participation state that individuals should be provided with clear, readable, and comprehensive notices about how their personally identifiable information will be used and have the opportunity to decline to participate if appropriate. These notices are intended to provide travelers with information about CBP's use of facial recognition technology at locations where this technology has been deployed, and how data collected will be used. The notices should also provide information on procedures for opting out, if applicable, among other things. However, we found that CBP's notices were not always current or complete, provided limited information on how to request to opt out of facial recognition, and were not always available. In particular, we identified limitations related to the completeness of information in CBP's online resources and call center, currency of information on signs at airports, information on opting out included in notices, and placement of signs at ports of entry.

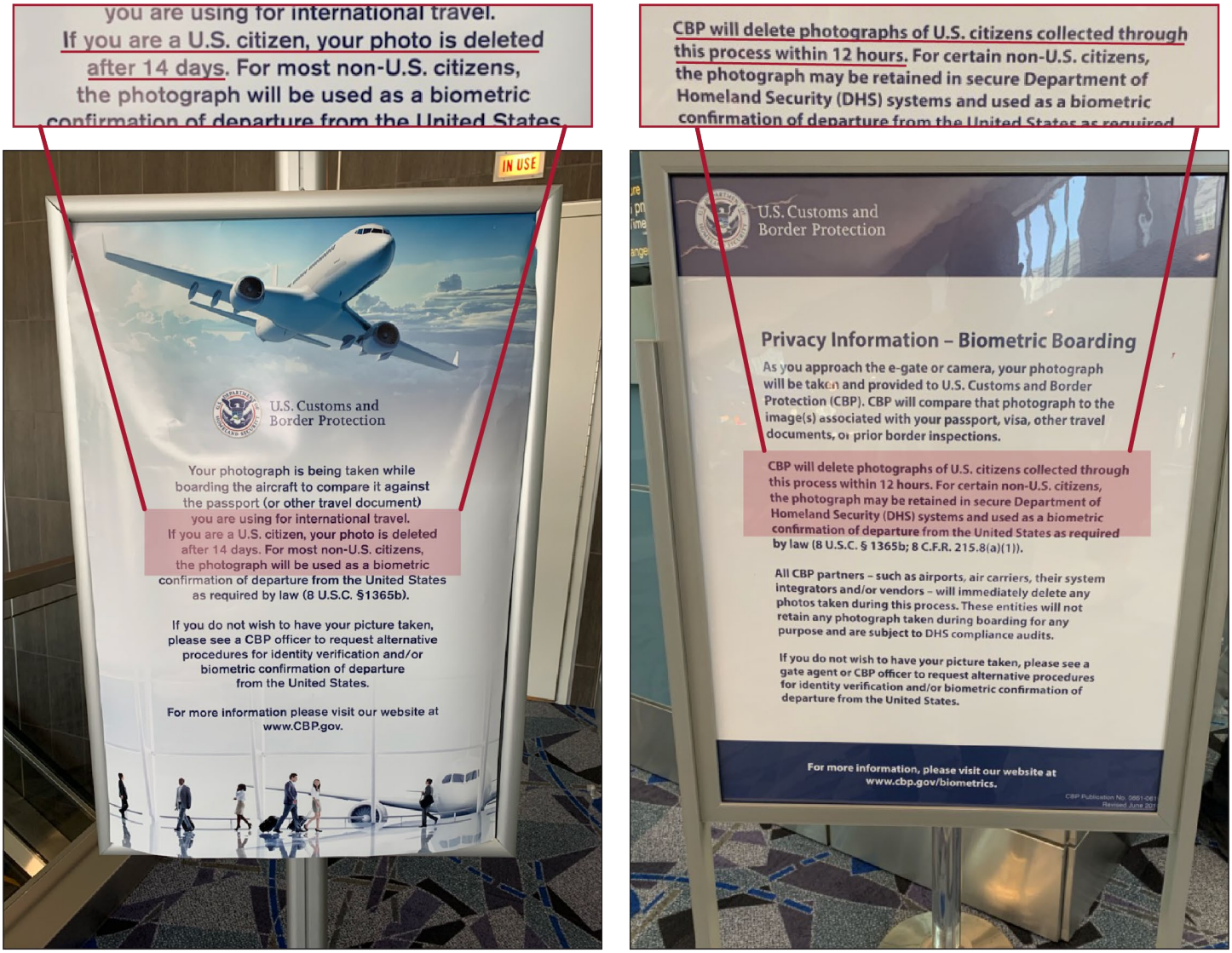
CBP online resources and call center had incomplete information. Although CBP's PIA states that CBP's public website is a source of information travelers can use to learn about the Biometric Entry-Exit Program, we found that the website did not accurately reflect the locations where CBP used or tested facial recognition technology. For example, when we reviewed the website in November 2019, it did not include two locations where CBP was conducting pilot tests of facial recognition technology (Nogales and San Luis, Arizona) even though these pilot tests began in 2018. Therefore, travelers who checked the website would not see a complete list of locations where they may encounter facial recognition technology. We also found that, as of March 2020, CBP's online Information Center—another CBP-recommended resource for information on the Biometric Entry-Exit Program—returned no search results for "facial recognition" or "biometrics" at U.S. ports of entry.

In addition, CBP has a call center for travel or customs questions. When we spoke with a CBP call center operator on November 1, 2019, the operator was not aware of locations where CBP was using facial

recognition technology. Further, we found that CBP's call center information phone line was intermittently in operation during the course of our review. In particular, during five calls placed between November 1, 2019, and January 1, 2020, we found the phone line was either not working or the operator was not aware of the ports of entry where facial recognition was in use or being tested. In response, CBP officials said they continuously monitor and update the website as appropriate and will coordinate with the CBP call center to provide operators with the most up-to-date information. However, we reviewed CBP's website at the end of June 2020, and it had not updated the website to include all locations using facial recognition technology even though we mentioned this issue to CBP officials in May 2020. Ensuring that online resources are functional and provide accurate information and that call center operators are knowledgeable about the locations where CBP is using facial recognition technology for identity verification would help CBP better address the transparency FIPP.

Signs at airports contained outdated information. We found that some signs at air exit locations (airport gates where facial recognition is used for departing travelers) were outdated, while others contained current information. For example, during our visit to the Las Vegas McCarran International Airport in September 2019, we saw one sign that said photos of U.S. citizens would be held for up to 14 days, and a second sign at a different gate that said photos would be held for up to 12 hours (the correct information), as shown in figure 6. The first sign was an outdated notice, as CBP had changed the data retention period for U.S. citizens in July 2018. However, CBP had not replaced all of the signs at this airport with this new information. CBP officials said that printing new signs is costly and they try to update signs when new guidance is issued but said it is not practical to print and deploy a complete set of new signs immediately after each change or update. Ensuring that signs at facial recognition locations consistently include current and accurate information would better reflect the transparency FIPP.

Figure 6: Example of Inconsistent Signs about Facial Recognition at the Las Vegas McCarran International Airport in September 2019



Source: GAO. | GAO-20-568

Notices provided limited information on opting out of facial recognition identity verification. According to the individual participation FIPP, individuals should be able to consent to the use of their personally identifiable information to the extent possible. While CBP allows eligible travelers to request to opt out of facial recognition identity

verification, the CBP notices we observed provided limited information on the process for opting out. For example, as shown in figure 6 above, CBP's privacy signs posted at airports state that travelers who do not want to have their photos taken should see a CBP officer or a gate agent to "request alternative procedures for identity verification." However, the signs do not state what those alternatives are or the consequences of making such requests. In addition, CBP officers are typically not present at boarding gates, so including this information on a sign could potentially be confusing to a traveler or potentially make it less likely they would request to opt out during air exit.

Officials from privacy advocacy groups told us that they, and people they knew, had experienced challenges when requesting to opt out, including being told by CBP officers and airline agents that opting out would lead to additional security scrutiny, increased wait times, and could be grounds to deny boarding.[63] Privacy advocacy groups we spoke with said that travelers would have a better understanding of their rights if specific opt out procedures were posted on signs around the area. In its 2019 report, the DHS Data Privacy and Integrity Advisory Committee also recommended that CBP's notices provide more information about how to opt out and describe any consequences.[64] CBP officials said that providing more information about the opt out process is not necessary because there are no consequences for opting out. Nonetheless, including additional information about how to opt out on CBP's signs and other notices, as appropriate, would better ensure that travelers are aware of their rights and can make informed decisions about consenting to facial recognition identity verification.

Signs were missing or obscured. We found that CBP facial recognition signs were not consistently posted or were posted in such a way that they were not easily seen by travelers. According to CBP program documents, signs should be posted at all locations where facial recognition technology is used to inform the public about the purpose of the facial recognition and provide information on the rights of travelers to opt out.

[63]CBP officials told us that eligible travelers who decide to opt out of facial recognition verification should be allowed to do so without any significant negative impacts and should simply be verified using the standard manual process (i.e., review of their passport, boarding pass, or other relevant documents).

[64]The Data Privacy and Integrity Advisory Committee is a committee that provides advice to the Secretary of Homeland Security and the DHS Chief Privacy Officer on privacy-related policy, operations, and programs. Committee members include representatives from government, academia, and industry.

However, during our visit to the Las Vegas McCarran International Airport in September 2019, no privacy signs were posted at a gate where facial recognition had been in operation for about 2 months. During our visit, local CBP officials said they had the signs in storage but had not had the opportunity to post them, so they posted them at the gates while we were there.

CBP requires that its commercial partners—such as airlines, airports, and or cruise lines—post CBP-approved privacy signs at gates where facial recognition technology is used to provide travelers with notice that their photos are being taken and for what purposes.[65] However, CBP has not enforced this requirement or consistently monitored air exit facial recognition locations to ensure that signs are posted for each flight using facial recognition technology. CBP program officials noted that they have a relatively small office and they do not have the capacity to install signs for all new locations themselves or to conduct inspections to ensure that signs are present and visible. Instead, program officials said they rely on local CBP officers at airports to ensure that signs are posted in the appropriate locations through periodic checks. However, local CBP officers told us they do not have the personnel to check if signs are present for each flight at boarding gates using facial recognition technology since they have other duties and responsibilities and are not required by CBP policy or guidelines to do so. CBP officials also noted airlines often share gates, and airlines that are not participating in CBP's Biometric Entry-Exit Program do not want to have CBP's privacy signs posted during their boarding process and sometimes remove them. When this occurs, the airlines that are using facial recognition technology at the shared gate must remember to post the signs for the boarding process, which CBP officials said does not always happen. Officials added that sometimes signs are taken down or moved by airline personnel or airport authorities without their knowledge. Nonetheless, CBP officials acknowledged that the program is ultimately responsible for informing travelers about facial recognition technology across all environments and

[65]CBP allows commercial partners to use their own signs to provide notice of facial recognition, but these signs must be approved by CBP. CBP's new requirements for commercial partners specify the minimum size for the signs, and specifies that the signs "must be clearly visible and placed at a sufficient distance in front of the camera in order to provide the traveler with a reasonable opportunity to read the content and opt-out before reaching the photo capture area." CBP also allows partners to display e-signage announcing the use of facial recognition technology. CBP's commercial partners may also choose to provide additional notices. For example, one airline official told us that their airline informs travelers about the use of facial recognition technology through emails sent along with reservation information.

locations through signs, handouts, and the CBP website, among other methods.

We also observed signs that were difficult to read or obscured. For example, at CBP inspections locations, we observed signs that were written in small print and located immediately before an area where travelers were not allowed to use their cell phones. Such situations could limit travelers' ability to consult CBP's online resources prior to encountering facial recognition technology. In addition, at the Port Canaveral seaport, we observed that a sign about facial recognition was partially obscured by another CBP sign (see fig. 7). In its 2019 assessment, DHS's Data Privacy and Integrity Advisory Committee made similar observations and recommended that facial recognition privacy signs should be large enough to be clearly visible and placed so that travelers arriving in the country have time to consult online resources before proceeding to the CBP inspections area. Prominently displayed signs in convenient locations would allow travelers time to consider the substance of the notices and determine if they would like to consent to facial recognition technology identity verification.

Figure 7: U.S. Customs and Border Protection Privacy Sign Partially Obscured at the Port Canaveral Seaport in Florida

Source: GAO. | GAO-20-568

The FIPPs of transparency and individual participation state that CBP should be transparent and notify individuals about how their personally identifiable information will be used. In addition, CBP should seek individual consent for the collection of this information, and individuals should have the opportunity to decline to participate, if appropriate. However, CBP has not ensured that it consistently provides travelers with complete and accurate information for its Biometric Entry-Exit Program nor has it ensured that notices are provided at all locations where facial recognition technology is used. Until CBP ensures that privacy notices contain complete and accurate information and that these notices are posted and visible for traveler review, CBP does not have assurance that the privacy protection principles designed to protect the personally identifiable information of the public are fully incorporated into its Biometric Entry-Exit Program.

CBP Has Not Audited Most of Its Partners and Has Not Developed a Plan for Future Audits

CBP requires its commercial partners, as well as contractors and vendors, to follow CBP's data collection and privacy requirements, such as restrictions on retaining or using traveler photos, and CBP can conduct audits to assess compliance. However, as of May 2020, CBP had audited only one of its more than 20 commercial airline partners and did not have a plan to ensure that all partners are audited for compliance with the program's privacy requirements. In addition, following a data breach in 2019, CBP took steps to increase audits of the contractors and vendors involved in the program, but it does not have a plan to determine when all contractors and vendors will be audited for compliance with privacy and security requirements.

Although CBP's commercial airline partners have used facial recognition technology for identity verification since 2017, and cruise lines since 2018, CBP's first audit of a commercial partner occurred in March 2020. At that time, CBP had partnerships with over 20 airlines, airports, and cruise lines, and over 7 million travelers had their identities verified using facial recognition technology. For this initial audit, CBP officials said they reviewed one commercial air carrier's privacy and security controls to ensure its compliance with program requirements. Specifically, according to CBP's requirements, CBP's partners are prohibited from retaining the photos they collect for their own business purposes, and the partners must immediately purge the photos following transmittal to CBP. Officials noted that this initial audit was intended to give them a baseline of how airlines are securing their facial recognition systems and help identify potential vulnerabilities that may apply to other airlines. Officials added that they expected this initial audit to inform how they design and conduct future audits of commercial partners and that they would include audit

processes and standards in the new version of the Biometric Entry-Exit Program's requirements for commercial partners.[66] However, CBP issued the new requirements in January 2020 without including new audit processes or standards. In May 2020, officials told us that they decided not to include specific audit processes in the program requirements document to avoid having to revise and reissue them when updates are made. Instead, officials said they would provide commercial partners with audit rules and requirements prior to each audit. As of May 2020, these audit rules and requirements have not been developed nor has CBP developed a plan that includes time frames for conducting audits of all of its commercial partners. However, according to CBP officials, CBP plans to conduct additional audits once pandemic travel restrictions are lifted.

Similar to CBP's commercial partners, contractors and vendors associated with the program are subject to CBP's privacy and security requirements, including restrictions on their use of photos collected as part of the program, and CBP can audit them to ensure compliance. In its 2019 report, the DHS Data Privacy and Integrity Advisory Committee stressed the importance of CBP conducting ongoing monitoring and compliance reviews of its vendors and contractors to ensure data protection. However, prior to a data breach that occurred in 2019 involving a CBP subcontractor, CBP had not conducted security or privacy audits of its contractors. In 2019, a CBP subcontractor downloaded photos from CBP against CBP protocols and was later the subject of a data breach.[67] CBP information security officials stated that it is unclear if this particular security vulnerability would have been identified

[66]The results of this audit were not available at the time of our review.

[67]According to CBP, a subcontractor employee involved with the pilot test at the Anzalduas port of entry removed facial image data from the pilot site using removable media and then downloaded them to the company's network for the purpose of performing additional analysis of CBP's data. The subcontractor then had data from their network stolen and posted on the dark web. CBP reviewed the dark web data and found no evidence that it included images from Anzalduas. CBP also confirmed that the subcontractor had only removed images; it did not have any associated data, such as names, dates of birth, or Social Security numbers. Officials said that they view this incident as an "insider threat" situation because the data were removed from CBP's systems in a way that was not authorized by policy or by contract. Officials also noted that the agency has a long-standing relationship with the prime contractor, and the subcontractor was vetted and screened by CBP. CBP officials told us that CBP immediately removed the subcontractor's access to CBP's systems after learning of the breach and asked the prime contractor to end the contract with the subcontractor. CBP has subsequently entered into an Administrative Contract Agreement with the subcontractor to improve their security practices but has no plans to resume business with the subcontractor.

through an audit because protocols were in place that prohibited contractors from downloading and removing data. However, now that CBP has identified this vulnerability, CBP information security officials have begun security reviews at some facial recognition testing locations to determine and assess security vulnerabilities. CBP officials also told us that they have made changes to pilot-testing security protocols, such as prohibiting the use of thumb (flash or USB) drives or any other personal drives. While this is a positive step, similar to not having a plan to conduct audits of its commercial airline partners, CBP has not yet developed a plan that identifies the time frames for auditing all contractors and vendors for compliance with privacy and security requirements.

In its August 2019 report to Congress on the deployment of biometric technologies, CBP announced that the CBP Privacy Office would conduct a broad privacy evaluation of the Biometric Entry-Exit Program across air, land, and sea travel environments.[68] According to CBP, this evaluation will assess the program's compliance with established legal and policy requirements, as outlined in the TVS Privacy Impact Assessment. CBP officials said they expect this evaluation will be completed by the end of 2020.[69] This review is a positive step consistent with the FIPPs of accountability and auditing and should provide CBP, Congress, and the public with valuable information on the program's overall privacy compliance. However, CBP's privacy office does not intend to evaluate whether each commercial partner, specific contractor, or vendor has followed CBP's business requirements for privacy and security in this review. These requirements include maintaining updated internal privacy policies and ensuring that all traveler photos are immediately purged after transmission to TVS. According to CBP privacy officials, audits at the partner and contractor level are the responsibility of the CBP program office.

The FIPPs state that agencies should audit the actual use of personal information to demonstrate compliance with all applicable privacy protection requirements. CBP officials acknowledged the importance of audits but said they have generally not been a priority because CBP's contractors and partners do not have access to internal CBP databases

[68]U.S. Department of Homeland Security Report to Congress, *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technology* (Washington, D.C.: Aug. 30, 2019).

[69]In its August 2019 report to Congress, CBP stated that the CBP Privacy Office evaluation would be completed by the end of 2019. However, CBP officials said the report should have stated that the privacy evaluation would be completed by the end of 2020.

and, therefore, cannot access systems that store personally identifiable information. Additionally, officials said they believe that their contractors and partners have no incentives to retain traveler photos for business purposes not explicitly authorized. However, officials from privacy advocacy groups we spoke to expressed concerns that CBP's commercial partners and contractors might use photos for their own purposes not authorized by the program, such as what occurred during the 2019 data breach cited earlier. These privacy groups noted that airline partners could use the photos obtained through the program to offer facial recognition-based access to airline lounges, for example. CBP officials noted that, per CBP's requirements, partners agree they are not permitted to store or use photos obtained from the program in any way. When we spoke to representatives from the airline industry, they said that partner airlines and airports do not want to retain photos of travelers due to the risks and liability involved. However, as of May 2020, CBP has not yet audited the majority of its airline business partners to ensure they are adhering to CBP's privacy requirements.

In addition, while CBP has taken some positive steps by auditing one of its airline partners and some locations where it is pilot-testing facial recognition technology, the privacy risks associated with personally identifiable information will continue to grow as the program expands and CBP collaborates with additional airlines, airports, cruise lines, contractors, and others. As such, developing and implementing a plan for conducting security and privacy audits of all of its commercial partners, contractors, and vendors across all travel environments—air, sea, and land—would better position CBP to ensure that personally identifiable information is being appropriately used, safeguarded, and deleted in accordance with program policies.

CBP Found Its Air Exit Facial Recognition Capability Met Accuracy Requirements, but CBP Has Not Fully Monitored Performance

CBP assessed the accuracy and performance of the Biometric Entry-Exit Program's air exit facial recognition capability (air exit) by conducting an operational test, as required by DHS acquisition policy; air exit was the first program capability to progress through the DHS acquisition process and undergo formal testing of accuracy and performance. The operational test—conducted by an independent test agent within CBP from May to June 2019—concluded that air exit met or exceeded CBP's accuracy requirements but did not meet a performance goal to successfully capture 97 percent of in-scope traveler photos.[70] CBP officials monitor the accuracy and performance of air exit through random sampling, but the current monitoring process does not alert them when performance falls below minimum requirements.

CBP Tested the Air Exit Facial Recognition Capability

Air exit is the first Biometric Entry-Exit Program capability to progress through the DHS acquisition process and undergo formal operational testing and evaluation. As described earlier, CBP has conducted initial evaluations of facial recognition technology in the sea and land environments. However, those evaluations were intended to assess the feasibility of facial recognition technology and inform the development of future program requirements. CBP considers its air entry facial recognition operations to be a technology refresh (upgrade of existing capabilities) and does not intend to conduct formal testing and evaluation.

As a DHS major acquisition program, consistent with DHS acquisition policy, the Biometric Entry-Exit Program's air exit facial recognition capability is to be assessed against program requirements in an operationally realistic environment before it can be fully deployed—referred to as operational testing.[71] From May to June 2019, a test agent for CBP performed an operational test and evaluation of air exit capabilities. According to DHS acquisition guidance, an independent organization—referred to as the operational test agent—plans, conducts, analyzes, and reports independent operational testing and evaluation for

[70]As noted above, CBP's next formal acquisition milestone for air exit is to achieve full operational capability, meaning full delivery of the system according to program requirements, including the photo capture requirement. As of the time of this report, CBP's goal was to achieve full operational capability by the end of fiscal year 2021.

[71]A DHS major acquisition program is one with life-cycle cost estimates of $300 million or greater. DHS policies for managing its major acquisition programs are primarily set forth in its Acquisition Management Directive 102.01 and Acquisition Management Instruction 102.01-001. For more information on DHS major acquisitions, see GAO-20-170SP.

major acquisition programs.[72] The test agent reports its results, which are discussed below, to DHS officials to inform decision-making.

Air Exit Met Accuracy Requirements during Operational Testing but Did Not Meet Its Photo Capture Performance Requirement

CBP's operational testing determined that air exit met its defined accuracy requirements but did not meet one of its performance requirements. See appendix III for a summary of the results from the operational test. In its Operational Requirements Document for the Biometric Entry-Exit Program, CBP identified the capabilities needed to confirm the identities of travelers departing the United States by air, and included accuracy and performance requirements.[73] In August 2019, the test agent for CBP found that air exit met or exceeded its two accuracy requirements—specifically, for the true and false acceptance rates (see table 2). However, the test found that air exit did not meet its performance requirement for capturing a minimum number of traveler photos (described below).

Table 2: Accuracy Requirements and Results of Air Exit Operational Testing

Operational requirement	Minimum requirement	Results of operational testing
True acceptance rate (the percentage of travelers correctly identified)	90 percent	98 percent
False acceptance rate (the percentage of travelers incorrectly identified)	0.1 percent	0.0092 percent

Source: U.S. Customs and Border Protection. I GAO-20-568

As shown in table 2, air exit met the two accuracy requirements defined in the Operational Requirements Document during operational testing. According to the operational test report, the true acceptance rate pertains to the likelihood that a legitimate traveler will be correctly matched to a photo from the gallery. Operational testing showed that air exit was able to correctly match 98 percent of travelers' photos with photo galleries built from passenger manifests, a key capability for the program. The false acceptance rate pertains to the likelihood that a traveler will be matched to a photo from the gallery when it is not of the same person. Operational

[72]The test agent for air exit was the Land Systems Operational Test Authority, which is a division within CBP.

[73]According to the Operational Requirements Document, all Biometric Entry-Exit Program capabilities across all travel environments (air, sea, and land) will ultimately be addressed in the Operational Requirements Document. However, the current version of the document focuses on the implementation of the air exit capability.

testing showed that air exit incorrectly matched a traveler to a gallery photo less than 0.1 percent of the time.

In addition to CBP's accuracy assessment conducted during the operational test of air exit capabilities, in December 2018, NIST—a government laboratory that has studied commercially available facial recognition technology—entered into an agreement with CBP to further assess the accuracy of an algorithm similar to that used in TVS. According to the terms of the agreement, NIST is to assess whether there are differences in the accuracy of TVS based on traveler demographics such as age, gender, or ethnicity. According to CBP officials, CBP's internal analysis of data from air exit showed a negligible effect in matching accuracy based on demographic variables. However, officials noted that this analysis was limited because while CBP has access to data on age, gender, and nationality for travelers entering and exiting the country, it does not have data on race or ethnicity. According to NIST officials, NIST will test an algorithm similar to that used in TVS and will analyze the impacts of gender, ethnicity, and age on matching accuracy.[74] CBP plans to use the same matching algorithm for all travel environments, and NIST's findings on the demographic effects on matching accuracy plan to take into account all travel environments. Per the agreement, NIST is to provide recommendations to CBP related to the algorithm, optimal thresholds, and gallery creation strategies.[75] Initially, NIST planned to complete this work in the spring of 2020 but, due to the COVID-19 pandemic, the new completion date for of this work has not been determined, according to CBP officials.

While air exit met its accuracy requirements during operational testing, it did not meet the photo capture performance requirement—that is, the percentage of in-scope travelers whose photos should be captured during the boarding process (also called biometric compliance rate). The test agent found that air exit successfully captured the photos of approximately 80 percent of in-scope travelers on participating flights, short of the 97 percent minimum requirement. According to the operational testing report, air exit did not meet the photo capture rate requirement due to disruptions to the facial recognition process during

[74]According to CBP officials, NIST is using CBP-owned photos from DHS databases, as well as photos from other sources, such as the Department of State and U.S. Citizenship and Immigration Services, to conduct its analysis.

[75]According to NIST, it will provide recommendations in the form of technical information that CBP can use to make informed decisions about its use of facial recognition algorithms.

boarding. The report found that disruptions were caused by factors such as camera outages, incorrectly configured systems at boarding gates, and airline agents' decisions to exclude certain categories of people out of convenience (to speed up the boarding process), such as families or individuals using wheelchairs. In these cases, airline agents would revert to manual boarding procedures (i.e., visually comparing a traveler to his or her travel identification documents), and travelers' photos were not captured or transmitted to TVS. For example, the test report noted that testing officials witnessed instances of cameras malfunctioning during boarding at all three of the airports they visited.

During our observations of five flights at three airports in 2019, we identified similar photo capture issues with air exit. For all but one of the flights we observed, most travelers had their photo successfully captured by the cameras on the first or second attempt and received a positive match result, meaning that TVS matched the live photo to a photo in the gallery. We also observed that in some cases, gate agents decided to bypass the facial matching process for certain travelers, such as for children or travelers using wheelchairs, and conduct manual boarding procedures. In addition, for one of the flights we observed, TVS was unable to match approximately 25 percent of travelers, even after repeated attempts. According to CBP officials who investigated the issue, the low match rate was caused by problems with the cameras and lighting at the gate—specifically, the photos taken were not of sufficient quality to match to the photos in the TVS gallery.

To help air exit meet its performance requirement for capturing traveler photos, CBP's test agent recommended that the agency develop airline camera system standards to ensure they are capable of capturing photos of travelers of all heights, as well as investigate why partner airlines have issues with cameras during the boarding process. In response, CBP officials said they did not intend to take further action to improve the photo capture rate at this time. Officials suggested that this was one metric of many that is used to assess the status of operational use of this capability. In addition, officials suggested that several factors would gradually improve the photo capture rate over time, including a greater number of airline personnel trained on air exit facial recognition procedures and more efficient traveler interaction with cameras as familiarity with the facial recognition process increases (looking straight at the camera instead of down, for example). Officials added that they do not plan to require certain types of cameras because they did not want to be prescriptive about the types of equipment airlines or airports should buy. Additionally, CBP officials said biometric matching is currently

optional at the boarding gate, and they have no plans to require airline partners to use facial recognition for in-scope travelers.[76] Because airline and airport partners participate voluntarily, they can choose to manually verify travelers' identities (not use facial recognition technology) for any reason. CBP officials said that air exit relies on these voluntary partnerships with airlines and airports, and they want to maintain positive relationships to recruit additional partners.

Air exit depends on the successful capture and submittal of live photos during boarding to fulfill its purpose of biometrically verifying traveler departures. While CBP currently does not intend to require airlines to capture photos of all in-scope travelers (as of May 2020), it does not have a plan to ensure that air exit can meet the 97 percent photo capture requirement defined in the Operational Requirements Document. The DHS Systems Engineering Life Cycle Guidebook also states that program and DHS leadership should determine a course of action to mitigate deficiencies identified during operational testing. CBP officials stated that the photo capture rate will naturally improve as air exit expands throughout airports, but improved familiarity with facial recognition procedures will not ensure that all applicable travelers are biometrically verified if partner airlines revert to manual identity verification, or if the photos they capture are low quality and cannot be matched. Developing and implementing a plan for improving the photo capture rate would help air exit better meet its operational goal of creating biometrically confirmed traveler departure records. Such a plan could include steps to systematically investigate why camera systems at gates may be capturing poor quality photos or how to decrease the frequency by which partner airlines resort to manual processing of travelers.

[76]During a hearing before the House Homeland Security Committee on February 6, 2020, the CBP Deputy Assistant Executive Commissioner for the Office of Field Operations testified that CBP may propose regulatory amendments that would impact foreign nationals. CBP officials clarified that they were in the process of proposing an amendment to require foreign nationals to be biometrically screened as they exit the United States on international flights.

DHS' Assessment of Air Exit Testing Raised Questions about Operational Effectiveness but Agreed Air Exit Fulfilled Congressional Directives

As part of the acquisition process, the Director of the Office of Test and Evaluation for DHS (Director) reviewed the results of CBP's operational testing of air exit capabilities and issued a Letter of Assessment that raised questions about air exit's overall operational effectiveness. According to DHS acquisition policy, the Director's role is to provide independent oversight for major acquisition programs and advise DHS components on test and evaluation activities. As part of this process, the Director writes a Letter of Assessment on the adequacy of the testing conducted, as well as the effectiveness, suitability, and cyber resilience of the program, to inform DHS decision-making. According to the Letter of Assessment, typically, the Director makes one of three determinations about the operational effectiveness of a program: (1) operationally effective; (2) operationally effective with limitations; or (3) not operationally effective.

In the December 2019 Letter of Assessment for air exit, the Director found that air exit as designed and deployed accurately and efficiently collects biometric information on in-scope air travelers exiting the United States, in accordance with law and executive order.[77] However, the Letter of Assessment concluded that air exit did not provide clear, measurable benefits to CBP's existing operations at airports. In other words, air exit did not change or enhance the day-to-day capabilities of CBP officers at airports. As noted in the Letter of Assessment, the Operational Requirements Document originally included requirements that air exit support enforcement actions against travelers who entered the country without inspection or with actionable law enforcement concerns, and identify overstays—foreign visitors who remain in the United States beyond their authorized period of stay. However, CBP officials determined that these functions are not actually performed by air exit alone, and DHS acknowledged the assignment of those requirements to other systems for the purposes of test and evaluation.[78] Specifically, CBP officials noted that air exit was not designed to assist CBP officers in their duties at airports. For example, CBP officers generally are not present during facial recognition identity verification at airline gates and, while they can be notified of no-matches, operational testing found notifications did not contain actionable information. The Letter of Assessment noted

[77]See 8 U.S.C. § 1365b and Executive Order 13780.

[78]Biometric Entry-Exit Program officials wrote a clarification letter in July 2019 that specified that the Unified Passenger System and the Biometric Exit Mobile Air application (a handheld mobile device used by CBP officers) were the CBP systems that would support enforcement actions against travelers who entered the country without inspection or with actionable law enforcement concerns, not air exit.

that when testing shows no operational benefit to a program, the Director would normally conclude that the program was not operationally effective. However, the Director determined that air exit had the *potential* to be operationally effective because air exit improves the reliability and accuracy of traveler departure records. Specifically, by biometrically confirming travelers' identities as they exit the United States, CBP can record their departures as "confirmed" instead of "reported."[79] This provides CBP with more reliable and accurate data on overstays, which has the potential to support postdeparture analysis and follow-on enforcement actions. The Director told us that, as a result, he created a new category for the air exit capability—"potential to be operationally effective."

In response to the Letter of Assessment, CBP officials agreed that air exit alone does not change or improve CBP officers' abilities to enforce customs and immigration laws or execute other assigned responsibilities at airports. However, they emphasized that air exit's primary purpose is to confirm the identity of travelers and fulfill CBP's statutory mandate to create a biometric entry-exit record system, and operational testing demonstrated that air exit supports that outcome. DHS leadership reviewed the Director's findings at an Acquisition Review Board meeting in December 2019 and approved air exit to move forward and fully deploy to airports. CBP officials said they planned to revise key documents, such as the Operational Requirements Document and Concept of Operations, to reflect their current and planned operations and clearly describe how air exit benefits CBP's predeparture, boarding, and postdeparture operations. Officials said they expected to make these changes by August 2020.[80]

[79]Before the Biometric Entry-Exit Program, foreign nationals' departures from the United States were recorded based on airlines' reporting of biographic information. These departures were recorded in DHS' databases as "reported" departures. The airlines also provided notifications regarding which passengers were onboard and not onboard the flight.

[80]Per DHS' acquisition policy, the Biometric Entry-Exit Program developed a Concept of Operations and Operational Requirements Document at the beginning of the acquisition life cycle of the air segment. DHS leadership directed the program to revise these documents after the air segment entered the deployment phase of the acquisition life cycle.

CBP's Process for Monitoring Air Exit Does Not Alert Officials When Performance Falls Below Minimum Requirements

CBP officials conduct monitoring of the accuracy and performance of air exit through random sampling, but the current monitoring process does not alert them when performance falls below minimum requirements (such as the 97 percent photo capture rate described above). CBP officials said they randomly sample two flights per airport per week and review the data from each flight, including the number of matches and the match rate. Officials said that these reviews can help identify problems, such as unusually low match rates or photo capture rates, and they will investigate any identified problems by contacting the airline or airport where they occurred. For example, officials said they identified a location through random sampling where the camera system was producing inversed photos (photos that were a mirror image of the person), which could not be processed by TVS. Officials said they reached out to the airport authority and worked with the airport's camera vendor to adjust the photo capture process and enhance the photo quality. In addition to random sampling, CBP officials can be informed of problems with air exit facial recognition if they are observed or reported by airlines or airports. For example, as previously mentioned, we observed a flight that experienced a high number of no-matches. When we alerted officials to the problem, they reviewed match data from other flights at that airport and identified similar issues. Specifically, CBP officials determined that lighting issues at a particular terminal were affecting the quality of the photos taken at the gate, and they worked with airport officials to address the issue. CBP officials also noted that they generate automated reports of matching rates and usage on a weekly basis, and provide weekly performance reports to stakeholders, such as airline partners. Officials said they use this reporting to gauge system performance.

However, CBP's current monitoring process does not immediately alert officials to problems that affect the performance of air exit. For example, sampling flights for review on a weekly basis may not identify a daily pattern of consistently low-quality photos due to poor lighting in a particular terminal, such as the one we observed, because flights and airports are selected randomly for review. This means a problem at a particular terminal or airport could potentially continue unabated for days or even weeks, for example, without CBP's knowledge. CBP officials said there were several reasons why they chose random sampling to monitor the accuracy and performance of air exit. For example, officials said they have a small team of five analysts dedicated to monitoring air exit's performance, and they do not have the capacity or resources to manually review every flight for anomalies. Additionally, officials said air exit has returned consistently high match rates for photos that are successfully captured, which gave them confidence that more robust or

comprehensive monitoring was not necessary. Further, officials said partner airlines and airports have an incentive to ensure high-quality performance of the photo capture process because they want to avoid delays when boarding travelers.

The DHS Systems Engineering Life Cycle Guidebook states that a system should be continuously monitored while in operation, and problems should be identified and corrected to achieve performance requirements.[81] This includes the use of failure reporting and analysis. Further, according to *Standards for Internal Control*, program management retains responsibility for monitoring the effectiveness of processes performed by service organizations, such as partner airlines, and should obtain reasonable assurance of the effectiveness of the service organization's internal controls over their assigned process.[82] In addition, internal control standards call for agencies to establish and operate a system to continuously monitor the quality of performance over time.

CBP officials agreed it would be helpful if they had automatic alerts or notification when the performance for a flight or airport fell below air exit performance thresholds and acknowledged that their system has the capability to provide these automatic alerts. Officials also said they had considered developing additional reports to evaluate system performance for air exit but had not begun this effort at the time of our review. Ensuring that the agency is alerted when air exit's performance falls below established thresholds would help CBP better monitor the extent to which air exit is achieving its intended goal of creating biometrically confirmed traveler departure records.

[81]Department of Homeland Security, *Systems Engineering Life Cycle Guidebook.*

[82]GAO-14-704G.

TSA Has Conducted Pilot Tests of Facial Recognition Technology for Identity Verification at Airports and Has Incorporated Privacy Protections in Its Pilots

Since 2017, TSA has conducted a series of pilot tests to assess the feasibility of using facial recognition technology for traveler identity verification at airport security checkpoints. TSA plans to continue testing and evaluating facial recognition technology through additional pilot tests prior to making any deployment decisions. TSA's facial recognition pilot tests have incorporated privacy protections consistent with the FIPPS but, given the limited nature of these pilot tests, it is too early to conduct a full assessment of TSA's compliance with privacy protection principles.

TSA Is Exploring Facial Recognition Technology for Identity Verification

TSA is evaluating the potential of facial recognition technology to automate the process of verifying travelers' identities and boarding passes at airports. Currently, Transportation Security Officers at each checkpoint, and airline employees at the check-in desk, visually compare the traveler in front of them to their travel identification document to verify their identity. According to TSA officials, automating current identity verification capabilities through the use of facial recognition technology has the potential to improve this process by better identifying impostors, or travelers using valid travel identification documents for fraudulent purposes at the checkpoint.

Since 2017, TSA and CBP have collaborated on a series of multiphased pilot tests using CBP's facial recognition matching service for identity verification at the TSA checkpoint at three major airports.[83] As part of one of these pilots, TSA and CBP partnered to test facial recognition technology for baggage drop for international travelers at the Hartsfield-Jackson Atlanta International Airport. In addition, TSA has also conducted a pilot at the Las Vegas McCarran International Airport to assess the

[83]TSA and CBP's joint pilot tests matched live photos of travelers against galleries composed of photos from the entire day's flights out of a particular terminal.

possible integration of facial matching with its credential authentication technology devices.[84]

New York's John F. Kennedy International Airport checkpoint pilot (October 2017-November 2017). TSA and CBP conducted a joint pilot test of 1:N facial identification to determine if TSA could use TVS facial matching service for identity verification at security checkpoints. Pilot participants were volunteers who were traveling on international outbound flights. No CBP officers were stationed at the TSA checkpoint during this pilot.

Los Angeles International Airport checkpoint demonstration (February 2018). TSA conducted a 3-week demonstration of 1:1 facial verification to assess the capabilities of an e-Gate (automated gate system), which was designed to process and validate travelers' identification documents at TSA checkpoints using 1:1 facial verification. During this demonstration, volunteer travelers with e-Passports scanned their e-Passports and boarding passes at an e-Gate.[85] The e-Gate validated and cross-checked the traveler's boarding pass and e-Passport, took a photo of the traveler, and compared the live photo to the photo embedded in the e-Passport, using 1:1 facial verification. If the live photo matched the document photo, the e-Gate opened automatically. This demonstration did not involve the TVS facial matching service.

Los Angeles International Airport checkpoint pilot (August 2018-October 2018). Similar to the pilot test conducted at New York's John F. Kennedy International Airport, TSA and CBP conducted a joint pilot test of 1:N facial identification to determine if TSA could use the TVS facial matching service for identity verification at TSA's security checkpoints. Participants were also volunteers traveling on international outbound flights; however, during this pilot, TSA tested the use of TSA tablet

[84]TSA's credential authentication technology provides TSA with the ability to scan and validate a traveler's identification document (e.g., passport, visa) to ensure its authenticity. The credential authentication technology device scans the document using infrared, ultraviolet, and visible white light to verify it has the proper security enhancements. During TSA's 1:1 pilot test, TSA connected a camera to the credential authentication technology machine to test the feasibility of using this system for 1:1 matching.

[85]An e-Passport is a passport that contains an electronic chip with the name, date of birth, and other biographic information embedded in it. The United States requires that e-Passports also contain a digital photo of the holder. All e-Passports issued by Visa Waiver Program countries and the United States have security features to prevent the unauthorized reading or "skimming" of data stored on the e-Passport chip.

devices that displayed match results. TSA also assessed the feasibility of co-locating TSA officers and CBP officers at the checkpoint for processing no match indications.

Hartsfield-Jackson Atlanta International Airport checkpoint pilot (August 2018-ongoing). TSA and CBP are conducting a joint pilot test of 1:N facial identification to assess the feasibility of using CBP's TVS facial matching service at an alternative international airport checkpoint.[86] CBP placed its own cameras at TSA checkpoints and used TVS to match live photos of international travelers against TVS's photo gallery. CBP officers were posted beyond the TSA checkpoint, according to TSA officials. Travelers who received a positive match result proceeded to TSA physical screening, and TSA Transportation Security Officers adjudicated no-match responses by examining travelers' identification documents.

We conducted an onsite observation of this pilot in the international terminal at the Hartsfield-Jackson Atlanta International Airport in July 2019. During our visit, we observed that the matching system was able to capture a photo and successfully match the majority of international travelers who participated in the pilot. For travelers who were unable to be matched by TVS, the Transportation Security Officer conducted manual identity verification (visual confirmation that the traveler's face matched their travel identification document). In some cases, we observed that the Transportation Security Officer adjusted the camera to successfully capture a traveler's photo, particularly for small children or travelers using wheelchairs.

See figure 8 for facial recognition technology equipment used during the pilot test conducted at the Hartsfield-Jackson Atlanta International Airport during our site visit in July 2019.

[86]According to CBP, this pilot initially ran from August 2018 to September 2018, but in October 2018, TSA and CBP elected to continue the pilot. It is ongoing as of May 2020.

Figure 8: Facial Recognition Cameras Used for Facial Recognition during a Joint Transportation Security Administration and U.S. Customs and Border Protection Pilot Test at the Hartsfield-Jackson Atlanta International Airport

Source: GAO. | GAO-20-568

TSA plans to conduct an additional pilot test of 1:N facial matching in calendar year 2020 at the Detroit Metropolitan Wayne County Airport.

Hartsfield-Jackson Atlanta International Airport check-in and checked baggage pilot with Delta Air Lines (November 2018-ongoing). In November 2018, TSA and Delta Air Lines signed an agreement to allow Delta Air Lines to begin testing CBP's facial matching service for international traveler check-in and baggage drop.[87] Traveler participation for this pilot test is voluntary, so during the check-in process, travelers are given the option to opt in to allow Delta to use facial recognition technology. Delta Air Lines officials told us they plan to continue testing this capability prior to making any decisions about expanding to other airports. See figure 9 for the check-in kiosk used by Delta Air Lines for this pilot. The kiosk provides travelers with the option

[87]In order for CBP and Delta Air Lines to test the feasibility of using facial recognition technology at baggage drop areas, TSA approved a request by Delta Air Lines to amend the Aircraft Operator Standard Security Program, which allows for the use of facial recognition using CBP's Traveler Verification Service in place of an airline agent verification.

to participate in facial recognition identity verification at the self-service check-in area. Once a traveler selects the option to participate, the camera on the kiosk is not activated until the traveler selects an acknowledgment button to indicate consent to have their photo taken.

Figure 9: Delta Air Lines Check-in Kiosk at the Hartsfield-Jackson Atlanta International Airport That Provided Travelers with the Option to Participate In Facial Recognition Identity Verification during Self-service Check-in

Source: GAO. | GAO-20-568

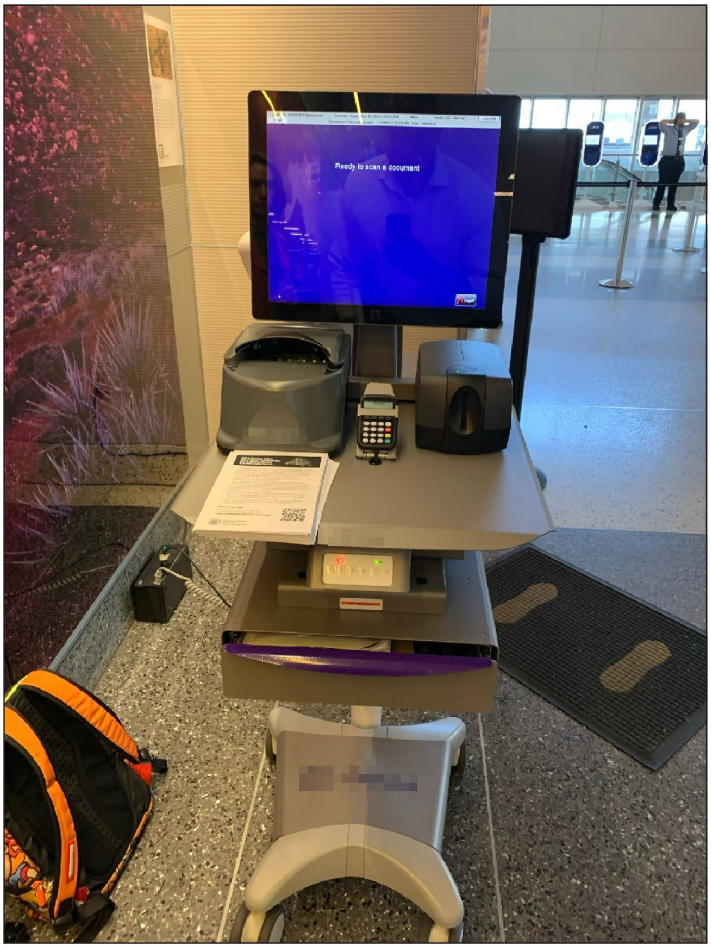
Las Vegas McCarran International Airport checkpoint pilot (August 2019-September 2019). TSA conducted a 30-day 1:1 facial verification pilot to assess its ability to compare a traveler's live photo at the checkpoint against the photo from the traveler's identification document. For this pilot, TSA equipped its credential authentication technology device with a camera—this pilot did not involve CBP or TVS. Participation in the pilot was voluntary for travelers with TSA PreCheck™[88]. For the pilot test, the credential authentication technology device attempted to (1) authenticate the travel identification document; (2) collect the photo and biographic information from the traveler's identification document; (3) capture the traveler's live photo; and (4) compare the live photo to the photo from the traveler's identification document to verify that the document belongs to them.

In September 2019, we observed this pilot for approximately 1 hour. During this time, 10 travelers volunteered to participate, and nine travelers had their photos successfully matched to their travel identification document. One traveler could not be matched because of damage to his travel identification document. According to TSA officials, TSA plans to analyze the data from this pilot over the next several months to help it determine future plans for facial recognition technology capabilities.

See figure 10 for the equipment TSA used during this pilot test in Las Vegas. TSA plans to conduct two more similar pilot tests in fiscal year 2021, according to TSA officials.

[88]TSA PreCheck™ is an expedited security screening program managed by the Transportation Security Administration and is used to gather information about passengers to assess passenger security risk prior to travel. Passengers who are cleared as part of the TSA PreCheck™ program are eligible for expedited screening.

Figure 10: Facial Recognition Equipment Used by the Transportation Security Administration during a Pilot Test at the Las Vegas McCarran International Airport



Source: GAO. | GAO-20-568

TSA officials told us that TSA plans to continue testing and evaluating facial recognition technology through additional pilot tests prior to making any deployment decisions.

TSA's Facial Recognition Pilot Tests Incorporated Privacy Principles

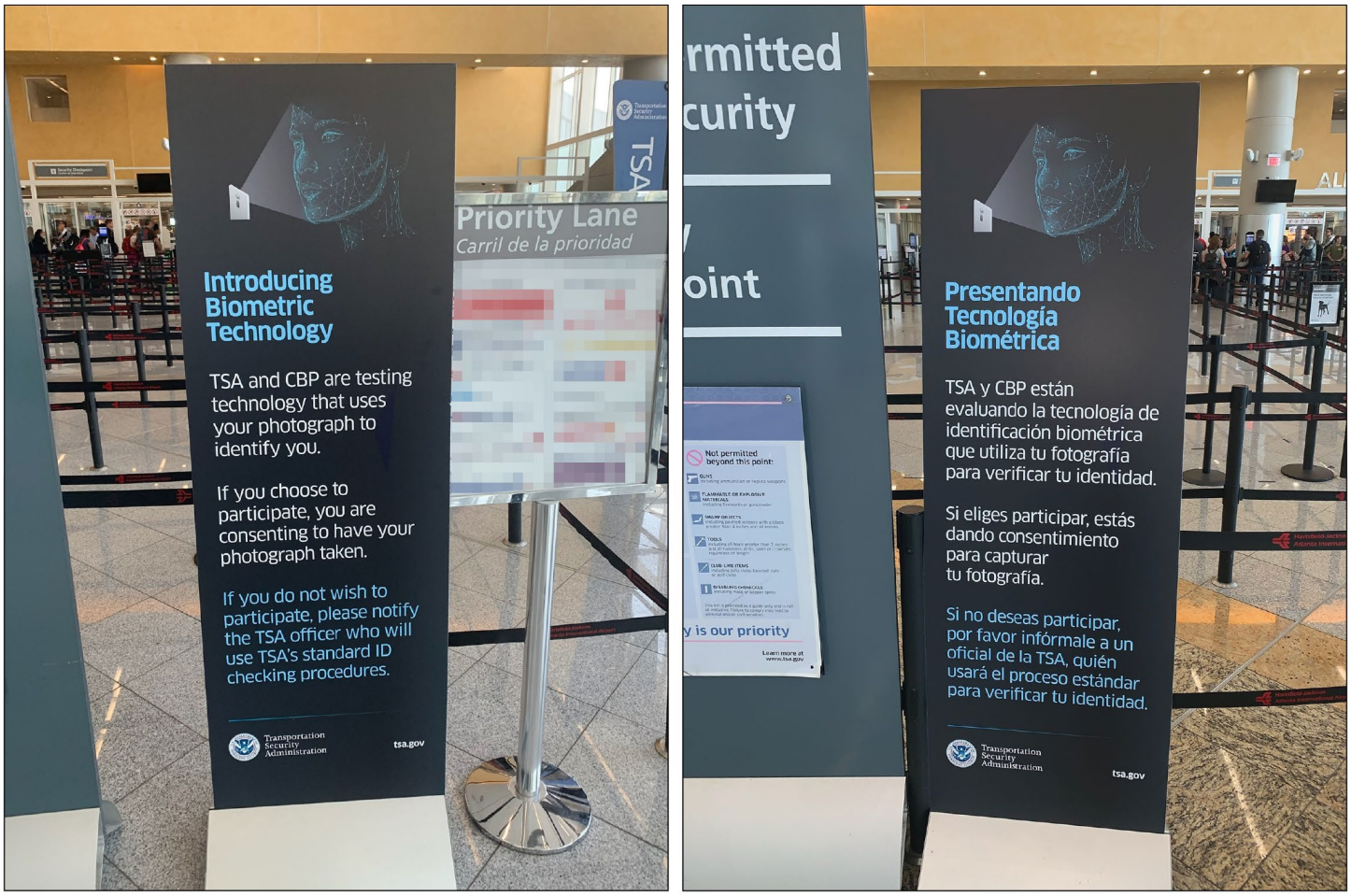
Based on our observations of TSA's pilot tests and review of its privacy documentation, TSA's facial recognition pilot tests have incorporated privacy protections consistent with the FIPPs, such as transparency and individual participation. However, given the limited nature of these pilot tests, it is too early to assess TSA's compliance with the FIPPs overall.

In accordance with DHS policy, TSA uses the FIPPs to assess and mitigate potential privacy risks from collecting personally identifiable information through biometric identity verification (including facial recognition). We found that TSA took steps to provide notice to the public about its efforts to protect traveler privacy, in accordance with the FIPPs and applicable privacy requirements. TSA's pilot tests were described in various PIAs, as required, and were available on TSA's public website. The PIAs assessed the privacy impacts of each of the pilot tests using the FIPPs and described TSA's efforts to mitigate these impacts. The PIAs included information on the purpose and duration of the pilot tests; how notice will be provided; and how data collected will be used and secured, among other things. For example, the PIA for TSA's pilot test at the Las Vegas McCarran International Airport noted the purpose of the pilot was to assess TSA's ability to compare a traveler's live photo at the TSA checkpoint against the photo from the traveler's identification document. The PIA also described steps TSA would take to secure personally identifiable information, such as using a new hard drive each day to collect data from the pilot, and ensuring data analysts delete the data within 180 days.

In addition to its PIAs, TSA provided onsite notice to travelers through signs and handouts. At the Hartsfield-Jackson Atlanta International Airport, we observed bilingual (English and Spanish) signs at the entrance to the relevant screening lane for each pilot test informing travelers about facial recognition identity verification (see fig.11). We also observed TSA officials standing by the entrance to the screening lanes answering traveler questions on the pilot tests and how personal information would be protected.[89] Such actions are consistent with the transparency FIPP, which states that TSA should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information.

[89]TSA officials said they are always present at the screening lanes to answer questions about the pilot tests.

Figure 11: Privacy Signs Posted in English and Spanish during a Transportation Security Administration Facial Recognition Pilot Test at the Hartsfield-Jackson Atlanta International Airport



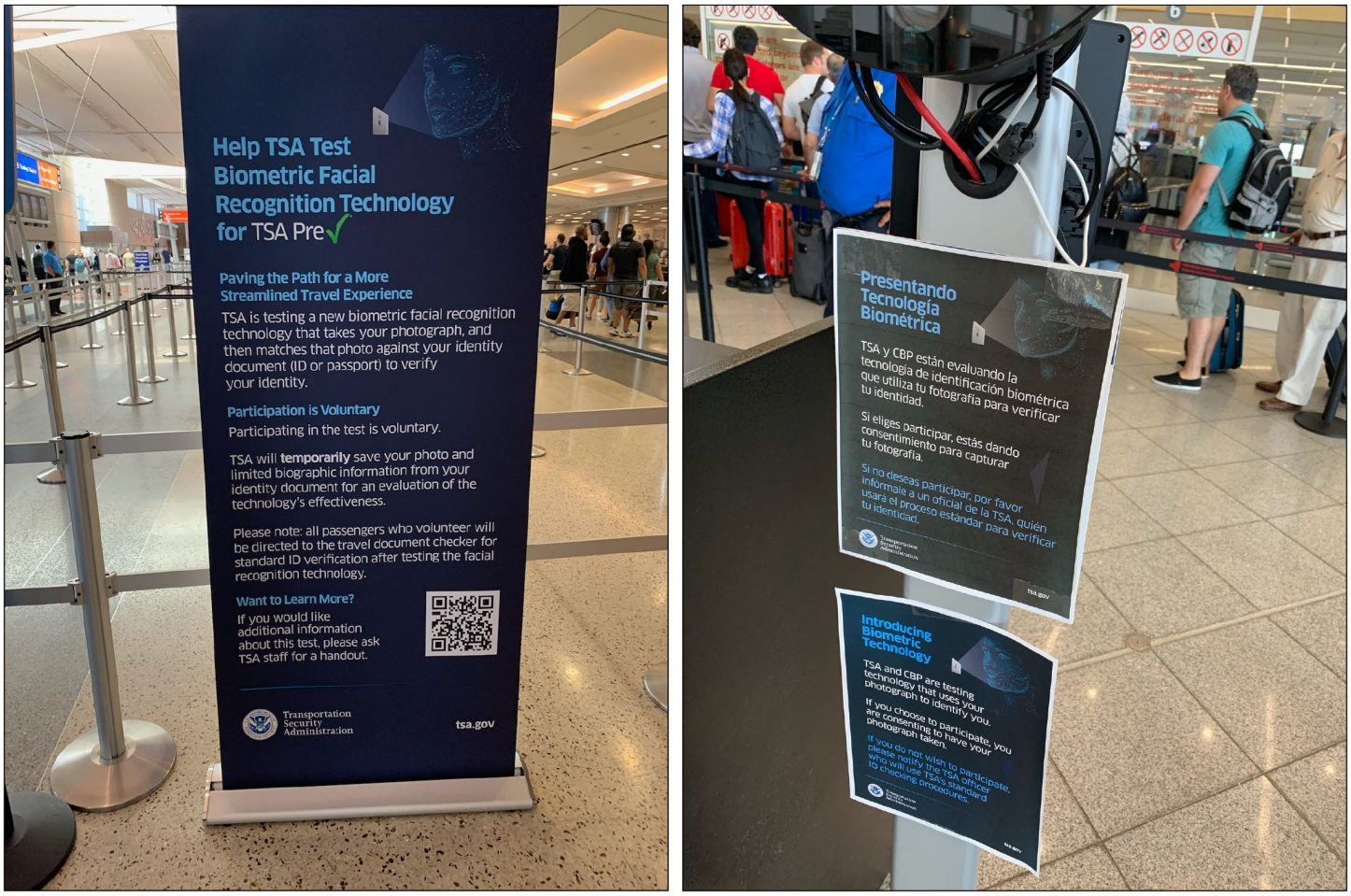
Source: GAO. | GAO-20-568

TSA also took steps to adhere to the individual participation privacy FIPP, which says that individuals should be able to consent to the use of their personally identifiable information to the extent possible. For each of its pilot tests, TSA provided notice to travelers about their ability to consent to facial recognition identity verification. For TSA's 1:1 pilot tests (at the Las Vegas McCarran International Airport and the Los Angeles Airport), participation was voluntary or "opt in," meaning that only travelers who consented to participate in the pilot would have their images captured using facial recognition technology. We observed the pilot at McCarran

International Airport and saw TSA officials ask travelers if they wanted to participate in the pilot test, and provide handouts explaining the purpose of the pilot test and the privacy protections. We also saw that the pilot test area was clearly marked with signs indicating that participation in the pilot test was voluntary (see fig.12).[90] For TSA's 1:N pilot tests conducted in partnership with CBP (and used TVS) travelers could opt out of facial recognition identity verification by notifying a TSA officer. During our observation of the TSA pilot at the international terminal of the Hartsfield-Jackson Atlanta International Airport, we saw that privacy signs were posted at the checkpoint area and included information on how to opt out (see fig.12).

[90]Travelers who participated in the pilot were also screened through the standard identity verification process.

Figure 12: Privacy Signs Posted at the Las Vegas McCarran International Airport and the Hartsfield-Jackson Atlanta International Airport during a Transportation Security Administration Facial Recognition Pilot Test



Source: GAO. | GAO-20-568

During our observation of this pilot test, (which was approximately 1 hour in duration), we saw three travelers ask to opt out of the pilot test.[91]

Privacy advocacy groups we met with expressed concerns about TSA's pilot tests, particularly whether TSA had the legal authority to use facial

[91]TSA officers performing facial identification told us that they typically screened all adults unless they specifically requested to opt out. TSA officials at the airport told us that one or two travelers per day requested to opt out.

recognition technology for domestic travelers, and the possibility of expanded use in the future.[92] However, officials from these groups also noted that TSA's 1:1 facial verification pilots offered greater protection to travelers' privacy, compared to its 1:N facial identification pilot tests conducted in partnership with CBP. Officials explained that with TSA's 1:1 facial verification pilot tests, there is no centralized database used for comparing a traveler's photo. Instead, the traveler's live photo is compared with that traveler's passport or other travel identification document, similar to how Transportation Security Officers manually verify travelers' identities.

As of May 2020, TSA has only pilot tested facial recognition technology, and those pilot tests were generally limited in duration, location, and scope (i.e., for international travelers or for trusted travelers only). Therefore, it is too early to conduct a full assessment of TSA's compliance with privacy protection principles. As of the time of this report, TSA had not decided whether it would implement facial recognition identity verification for checkpoint operations. TSA officials said they will continue to take steps to comply with the FIPPs in any future testing or implementation of facial recognition technology, including developing or updating PIAs, as appropriate. As the agency moves forward with testing facial recognition technology, we will continue to monitor TSA's compliance with DHS privacy principles.

Conclusions

CBP has begun testing and deploying facial recognition technology at ports of entry to fulfill its statutory mandate to create a biometric entry-exit record system. In accordance with DHS's Fair Information Practice Principles, CBP has incorporated some privacy protections into its Biometric Entry-Exit Program to protect the personally identifiable information of travelers. However, we observed instances of outdated or unhelpful informational signs at ports of entry, and online and call center resources had incomplete information. Ensuring that privacy notices for the Biometric Entry-Exit Program contain complete and current information—such as all of the locations where facial recognition is used and how travelers can request to opt out, as appropriate—and are consistently available would help give travelers the opportunity to decline to participate, if appropriate. Doing so would also help CBP improve transparency with the travelling public about how it uses personally identifiable information. Further, CBP has not audited the majority of its

[92]According to TSA program officials, The Aviation and Transportation Security Act of 2001, section 109(a)(7), grants TSA the authority to perform facial recognition verification at airports in the United States.

commercial partners, contractors, and vendors to ensure that they are adhering to CBP's requirements to protect travelers' privacy. As CBP works to increase the number of partners and expand facial recognition to additional locations, the privacy risks associated with the use of personally identifiable information will continue to grow. CBP would be better positioned to protect travelers' information if it developed and implemented a plan for auditing partners who have access to personally identifiable information.

Because air exit is the facial recognition capability furthest along in development, CBP tested the accuracy and performance of air exit capabilities in an operational setting, as required by DHS acquisition policy. While air exit exceeded the program's minimum requirements for matching accuracy, testing showed it did not capture all applicable traveler photos, as required. Developing and implementing a plan to ensure that the program can capture all applicable traveler photos would better position CBP to meet its performance requirements. Further, while CBP conducts some monitoring of air exit's performance, CBP's current monitoring process is not continuous and does not automatically alert program officials when performance falls below established thresholds for a particular flight or airport, such as when there is a high rate of travelers whose photos were not captured. Automatic alerts would help CBP continuously monitor the extent to which air exit is achieving its intended purpose of biometrically confirming travelers' identities upon departure.

Recommendations for Executive Action

We are making the following five recommendations to CBP:

The Commissioner of CBP should ensure that the Biometric Entry-Exit Program's privacy notices contain complete and current information, including all of the locations where facial recognition is used and how travelers can request to opt out as appropriate. (Recommendation 1)

The Commissioner of CBP should ensure that the Biometric Entry-Exit Program's privacy signage is consistently available at all locations where CBP is using facial recognition. (Recommendation 2)

The Commissioner of CBP should direct the Biometric Entry-Exit Program to develop and implement a plan to conduct privacy audits of its commercial partners', contractors', and vendors' use of personally identifiable information. (Recommendation 3)

The Commissioner of CBP should develop and implement a plan to ensure that the biometric air exit capability meets its established photo capture requirement. (Recommendation 4)

The Commissioner of CBP should develop a process by which Biometric Entry-Exit program officials are alerted when the performance of air exit facial recognition falls below established thresholds. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for its review and comment. DHS provided formal, written comments, which are reproduced in full in appendix IV. DHS also provided technical comments on our draft report, which we incorporated, as appropriate.

DHS concurred with our recommendations and described actions planned or underway to address them. Regarding our recommendation that CBP develop a process by which Biometric Entry-Exit program officials are alerted when the performance of air exit facial recognition falls below established thresholds, DHS stated that CBP has a suite of tools for system and operational performance management, and CBP creates three types of performance reports that are automatically generated and distributed on a weekly basis within CBP and to external stakeholders. DHS also stated that CBP monitors these reports for performance issues and addresses any anomalies with stakeholders as they arise. DHS requested that we consider the recommendation implemented. Once we review the documentation supporting these steps, we will assess the extent to which CBP's actions fully address the recommendation.

We are sending copies of this report to the appropriate congressional committees, the Acting Secretary of the Department of Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or gamblerr@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Rebecca Gambler
Director, Homeland Security and Justice

Appendix I: The National Institute of Standards and Technology's Findings on Facial Recognition Technology Accuracy

In December 2019, the National Institute of Standards and Technology (NIST), a government laboratory that studies facial recognition technology, released a report on the effects of demographics on the accuracy of facial recognition technology.[1] NIST found that facial recognition algorithms differed in accuracy based on race or country of birth, sex, and age. The extent of the difference varied based on the type of accuracy error (false positive or false negative), type of use (1:N or 1:1), the quality of the photos, and the developer.[2] NIST tested over 200 facial recognition algorithms and used 18 million images consisting of domestic photos taken when individuals are arrested, application photographs for immigration benefits, visa photographs, and border crossing photos.[3]

[1]National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (Gaithersburg, MD: 2019).

[2]1:N matching compares a live photo against a number (N) of photos in a database to determine if there is a match (identification of a particular face among many photos). 1:1 matching compares a live photo to another photo of the same person (verification of a face against a source photo).

[3]In December 2019, CBP was using an algorithm for the Biometric Entry-Exit Program that was not included in NIST's analysis. According to CBP officials, at the end of March 2020, CBP upgraded its algorithm to an algorithm that was evaluated in NIST's December 2019 report. The algorithm CBP started using in March 2020 was among the most accurate algorithms on many measures in NIST's report. Vendors voluntarily submit algorithms for the NIST testing.

Accuracy Terminology

False positive is when a facial recognition system incorrectly finds two images to be a match when they are actually from two different people. For air exit, U.S. Customs and Border Protection (CBP) uses the term "false acceptance" for this type of incorrect match.

False negative is when a facial recognition system fails to match two images when they are from the same person.

True acceptance is a term used by CBP for when air exit correctly matches two images from the same person.

The false negative rates and true acceptance rates are mathematically related:

True acceptance rate = 1 - false negative rate

For example, if a facial recognition system has a false negative rate of 20 percent, the true acceptance rate would be 80 percent.

Source: GAO. | GAO-20-568

Broadly, NIST found that false positive rates in 1:1 (verification) algorithms were 10 to 100 times less accurate for some demographics. Specifically for false positive rates, algorithms were less accurate for West and East African, American Indian, African American, and Asian populations, and more accurate for Eastern European populations. Also for false positive rates, NIST found algorithms to be less accurate for women, the elderly, and children. NIST did note some exceptions to the general trends in false positives. For example, algorithms developed in China had a lower false positive rate, meaning they were more accurate, for East Asian populations.

For false negatives, NIST did not find as large of a gap as in the false positives but rather found the accuracy rates were specific to each algorithm. In general, NIST found the false negative rates were less than three times as accurate for certain demographics, and varied based on the photo database used in testing. Looking at false negatives with domestic photos taken for individuals when they are arrested, which are generally higher-quality images, the algorithms were less accurate for Asian and American Indian populations, whereas the algorithms were more accurate for Caucasian and African American populations. With poorer-quality photos, such as photos captured at border crossings, false negatives were higher, meaning the algorithms were less accurate, for people born in Africa and the Caribbean.[4] For false negative rates, NIST often found the algorithms were less accurate for women and younger people, though NIST noted many exceptions to this trend.

While the general trend in false positive results for 1:N applications was the same as for 1:1 applications, NIST found several exceptions where false positives did not vary across demographics. NIST found that algorithms from six different developers had uniform scores across different demographics, meaning they performed the same across different demographics. However, for most, but not all, algorithms tested, NIST found the same demographic effects with 1:N applications as with 1:1 applications. The images used for analysis of demographic parity in 1:N testing were arrest photos, which lack the range in quality

[4]According to the NIST report, many domestic photos taken for individuals when they are arrested were collected with a photographic setup specifically standardized to produce high-quality images across races. Images collected at border crossings, however, are generally not captured according to the same quality standards and may have underexposure of dark-skinned individuals due to bright background lighting, for example.

represented by the sets of images used in NIST's testing of 1:1 algorithms.

Appendix II: Ports of Entry Where U.S. Customs and Border Protection Has Tested or Deployed Facial Recognition Technology

As of May 2020, U.S. Customs and Border Protection has tested or deployed facial recognition technology for traveler identity verification at multiple air, sea, and land travel environments in the United States and some international locations. See tables 3 through 7 for a list of these locations.

Table 3: Air Exit Locations Where U.S. Customs and Border Protection Deployed Facial Recognition Technology, as of May 2020

1.	Atlanta Hartsfield-Jackson International Airport (ATL)
2.	Austin-Bergstrom International Airport (AUS)
3.	Boston Logan International Airport (BOS)
4.	Chicago O'Hare International Airport (ORD)
5.	Dallas/Fort Worth International Airport (DFW)
6.	Detroit Metropolitan Wayne County Airport (DTW)
7.	Fort Lauderdale-Hollywood International Airport (FLL)
8.	George Bush Intercontinental Airport (IAH)
9.	John F. Kennedy International Airport (New York) (JFK)
10.	Los Angeles International Airport (LAX)
11.	McCarran International Airport (LAS)
12.	Miami International Airport (MIA)
13.	Minneapolis-St. Paul International Airport (MSP)
14.	Newark Liberty International Airport (EWR)
15.	Orlando International Airport (MCO)
16.	Philadelphia International Airport (PHL)
17.	Portland International Airport (PDX)
18.	Ronald Reagan Washington National Airport (DCA)
19.	Salt Lake City International Airport (SLC)
20.	San Antonio International Airport (SAT)
21.	San Diego International Airport (SAN)
22.	San Francisco International Airport (SFO)
23.	San Jose International Airport (SJC)
24.	Seattle-Tacoma International Airport (SEA)
25.	Tampa International Airport (TPA)
26.	Washington Dulles International Airport (IAD)
27.	William P. Hobby Airport (HOU)

Source: U.S. Customs and Border Protection. I GAO-20-568

Table 4: Air Entry Locations Where U.S. Customs and Border Protection Deployed Facial Recognition Technology, as of May 2020

1.	Abu Dhabi International Airport (AUH)—Preclearance
2.	Aruba–Queen Beatrix International Airport (AUA)—Preclearance
3.	Detroit Metropolitan Wayne Country Airport (DTW)
4.	Dublin Airport (DUB)—Preclearance
5.	Fort Lauderdale-Hollywood International Airport (FLL)
6.	Hartsfield-Jackson Atlanta International Airport (ATL)
7.	Ireland—Shannon Airport (SNN)—Preclearance
8.	John F. Kennedy International Airport (JFK)
9.	Los Angeles International Airport (LAX)
10.	McCarran International Airport (LAS)
11.	Miami International Airport (MIA)
12.	Newark Liberty International Airport (EWR)
13.	Norman Y. Mineta San Jose International Airport (SJC)
14.	Orlando International Airport (MCO)
15.	San Antonio International Airport (SAT)
16.	San Diego International Airport (SAN)
17.	Washington Dulles International Airport (IAD)
18.	William P. Hobby Airport (HOU)

Source: U.S. Customs and Border Protection. I GAO-20-568

Table 5: Sea Ports Where U.S. Customs and Border Protection Tested Facial Recognition Technology, as of May 2020

1.	Cape Liberty Cruise Terminal, Bayonne, New Jersey
2.	Pier 66, Seattle, Washington
3.	Pier 88, New York City, New York
4.	Port Canaveral, Florida
5.	Port Everglades, Fort Lauderdale, Florida
6.	Port Miami, Miami, Florida

Source: U.S. Customs and Border Protection. I GAO-20-568

Table 6: Land Ports Where U.S. Customs and Border Protection Tested Facial Recognition Technology, as of May 2020

1.	El Paso, Texas
2.	Laredo, Texas
3.	Nogales, Arizona
4.	Progreso, Texas
5.	San Luis, Arizona

Source: U.S. Customs and Border Protection. I GAO-20-568

Table 7: Airports Where U.S. Customs and Border Protection Deployed Facial Recognition Technology for the Global Entry Program, as of May 2020

1.	Aruba–Queen Beatrix International Airport (AUA)
2.	Dallas/Fort Worth International Airport (DFW)
3.	Detroit Metropolitan Airport (DTW)
4.	Dublin Airport, Ireland (DUB)
5.	Fort Lauderdale/Hollywood International Airport (FLL)
6.	George Bush Intercontinental Airport, Houston (IAH)
7.	Hartsfield-Jackson Atlanta International Airport (ATL)
8.	John F. Kennedy International Airport, New York (JFK)
9.	Miami International Airport (MIA)
10.	Newark Liberty International Airport (EWR
11.	Orlando International Airport (MCO)
12.	Philadelphia International Airport (PHL)
13.	Phoenix Sky Harbor International Airport (PHX)
14.	Salt Lake City International Airport (SLC)
15.	San Diego International Airport (SAN)
16.	Shannon Airport, Ireland (SNN)
17.	William P. Hobby Airport (HOU)

Source: U.S. Customs and Border Protection. I GAO-20-568

Note: Global Entry is a CBP program that allows expedited clearance for preapproved, low-risk travelers upon arrival in the United States. CBP uses Global Entry kiosks to process eligible travelers entering the United States through designated airports. With the addition of facial recognition, travelers' photos are used to retrieve their record and verify their identity in place of their fingerprints.

Appendix III: Results of the 2019 Operational Test and Evaluation of U.S. Customs and Border Protection's Air Exit Capabilities

In August 2019, the test agent for U.S. Customs and Border Protection (CBP) reported on the results of its operational testing of the Biometric Entry-Exit Program's air exit facial recognition capability (air exit) and found it was "effective with limitations," and "suitable with limitations."[1] According to Department of Homeland Security (DHS) acquisition guidance, an independent organization within DHS called the Operational Test Agency plans, conducts, analyzes, and reports independent operational testing and evaluation for major acquisition programs.[2] Operational testing is formal testing and evaluation of a new capability in an operationally realistic environment and is intended to evaluate its effectiveness and suitability against mission requirements set out in the Operational Requirements Document. From May 20 to June 13, 2019, the test agent performed operational testing of air exit capabilities at three airports: the Detroit Metropolitan Wayne County Airport, John F. Kennedy International Airport, and Orlando International Airport. Operational testing assessed air exit capabilities against three types of operational requirements: (1) key performance parameters, (2) effectiveness, and (3) suitability.

Key Performance Parameters

The Operational Requirements Document for air exit included four key performance parameters.[3] In general, key performance parameters are the operational requirements that are considered essential for the successful accomplishment of a program's mission and are generally linked to an organization's specific mission goals and objectives. The test agent found that air exit met or exceeded all four requirements during operational testing, as shown in table 8 below.

[1]The test agent for air exit was the Land Systems Operational Test Authority, which is a division within CBP. The test agent reports its results to DHS and program officials to inform decision-making. Department of Homeland Security, *Operational Test and Evaluation Report for the Biometric Entry-Exit Program Air Exit Segment,* OPS10-AES-14-000002 (Washington, D.C.: Aug. 26, 2019).

[2]A DHS major acquisition program is one with life-cycle cost estimates of $300 million or greater. DHS policies for managing its major acquisition programs are primarily set forth in its Acquisition Management Directive 102-01 and Acquisition Management Instruction 102-01-001. For more information on DHS major acquisitions, see GAO, *Homeland Security Acquisitions: Outcomes Have Improved but Actions Needed to Enhance Oversight of Schedule Goals*, GAO-20-170SP (Washington, D.C.: Dec. 19, 2019).

[3]Department of Homeland Security, *Biometric Entry-Exit Program, Operational Requirements Document* (Washington, D.C.: May 2017). DHS validated the Operational Requirements Document for air exit in January 2018, along with an action to create separate Operational Requirements Documents for sea and land. In July 2019, Biometric Entry Exit Program officials clarified that three of the operational requirements were fulfilled by systems other than air exit.

Table 8: Key Performance Parameters and Operational Test Results for Air Exit

Key performance parameter	Minimum requirement	Result of operational testing
True acceptance rate (the percentage of travelers correctly identified)	>90 percent	98 percent
False acceptance rate (the percentage of travelers incorrectly identified)	<0.1 percent	0.0092 percent
Availability	>99.75 percent	99.85 percent
Capacity	70 flights, with 9,500 passengers	Averaged 800 flights, with 24,000 passengers

Source: U.S. Customs and Border Protection. I GAO-20-568

True Acceptance and False Acceptance Rates

The true acceptance and false acceptance rate key performance parameters measured the accuracy of CBP's air exit facial recognition capabilities, which uses the Traveler Verification Service (TVS) (CBP's facial matching service). The test agent found that air exit exceeded the minimum requirements for these two key performance parameters. The true acceptance rate is the percentage of travelers with a live photo (real-time photo) successfully captured who are correctly identified against a photo gallery of travelers on a flight. The false acceptance rate is the percentage of travelers who are incorrectly matched to a photo of someone else in a gallery. The test results found that air exit had a true acceptance rate of 98 percent and a false acceptance rate of 0.009 percent, exceeding the minimum requirements described in the Operational Requirements Document.

We reviewed the operational testing documentation and found the accuracy testing results are reliable. We found CBP's test agent tested the accuracy requirements under conditions similar to actual operations and calculated the accuracy metrics similar to the methodology used by the National Institute of Standards and Technology for testing commercial facial recognition technology. Specifically, we found that the test agent used operational data from an appropriate sample size of over 1,800 flights over a 7-month period to calculate the true acceptance rate. To calculate the false acceptance rate, CBP intentionally mismatched travelers from one flight to a previous flight to create an impostor attempt—in other words, to see whether TVS would match any of the travelers from the two flights when, hypothetically, there should be no matches. Any travelers for which TVS returned a match were recorded as a false acceptance. CBP used operational data from a 4-month period and attempted to match over 600,000 travelers to calculate the false acceptance rate.

Availability

The Operational Requirements Document requires that air exit be operationally available (functionally responding to matching requests) at least 99.75 percent of the time (measured annually). CBP calculated TVS's availability based on the number of attempts the system made to match a traveler's live photo to a photo in a gallery. The test agent collected data on the total number of attempts made, and the number of unsuccessful attempts made, from April 1, 2018, to June 11, 2019. The calculated availability was 99.85 percent, which exceeded the minimum requirement.

Capacity

The Operational Requirements Document requires that air exit be capable of processing at least 70 flights with 9,500 passengers total over a 15-minute time period. During the operational test, not enough participating flights were boarding simultaneously to verify that air exit could meet the minimum capability requirements. As a result, the CBP Office of Information and Technology conducted a simulation test to increase the number of photos air exit processed at once. During the simulation test, air exit successfully demonstrated the ability to process approximately 24,000 passengers on 804 flights over a 15-minute time period, which exceeded the minimum requirement.

Effectiveness

The Operational Requirements Document included nine measures of effectiveness. Measures of effectiveness assess whether a system or program has accomplished its mission and achieved desired results. The test agent assessed five of the nine measures of effectiveness and found that air exit was "effective with limitations." (See the results in table 9 below.) Air exit demonstrated the capability to accurately match travelers and provide crossing records to government-owned systems, among other things, but did not meet the minimum required rate of capturing traveler data (taking live photos of travelers as they boarded flights). An explanation of the measures that were found to be not effective or not evaluated is provided below.

Table 9: Measures of Effectiveness and Operational Test Results for Air Exit

Measure of effectiveness	Result of operational testing
Match traveler data against Department of Homeland Security traveler identity data	Effective
Record traveler arrivals and departures	Effective
Identify overstays (entry/exit records)[a]	Effective
Minimize the negative impacts to the air carrier	Effective
Capture required traveler data	Not effective
Support enforcement actions	Not evaluated
Identify travelers who have overstayed the lawful period of admission to the United States	Not evaluated
Improve accuracy and availability of country-by-country immigration statistics	Not evaluated
Cyber resiliency	Not evaluated

Source: U.S. Customs and Border Protection. I GAO-20-568

[a]According to the test agent, the "identify overstays" measure was found effective because biometrically confirmed crossing records can potentially be used by Department of Homeland Security (DHS) to identify travelers who overstayed their visas. In other words, analysts could match biometrically confirmed exit records against entry records to identify travelers who had stayed in the United States longer than their visa allowed. However, air exit itself does not identify overstays; analysts would use the DHS Arrival and Departure Information System to perform this function. The test agent clarified that, when evaluating air exit, they made this distinction by finding that a similar requirement—"identify travelers who have overstayed the lawful period of admission to the United States"—was not able to be evaluated because air exit did not identify overstays directly.

Capture Required Traveler Data

As described earlier in this report, the test agent found that air exit did not meet the photo capture requirement—that is, the percentage of in-scope travelers whose photos should be captured during the boarding process (also called biometric compliance rate).[4] The test agent found that air exit successfully captured the photos of 80 percent of in-scope travelers on participating flights, short of the 97 percent minimum requirement. According to the operational testing report, air exit did not meet the photo capture rate requirement due to disruptions to the facial recognition screening process during boarding.

Support Enforcement Actions

The test agent did not evaluate air exit against the requirement in the Operational Requirements Document that it "support enforcement

[4]An in-scope traveler is any person who may be required by law to provide biometrics to CBP when they enter or exit the country. These are foreign nationals, excluding children under the age of 14 and adults over 79, most Canadian citizens, and other limited categories of foreign travelers.

actions." While TVS is capable of providing notifications to CBP officers at airports when travelers boarding flights receive a no-match result, the test agent found CBP officers did not use or respond to those notifications.[5] The test agent found this was because the no-match notifications did not provide usable information, such as whether travelers had actionable law enforcement concerns. Specifically, TVS does not search DHS databases for derogatory information about travelers; rather, TVS matches live photos against a prestaged photo gallery and produces a match or no-match result, and a no-match does not necessarily indicate derogatory information about the traveler.[6] In July 2019, CBP program officials issued a clarification memorandum specifying that other CBP systems—not air exit—support CBP officers in their enforcement responsibilities.[7] Program officials said this requirement was added to the Operational Requirements Document before they fully understood air exit's capabilities.

Identify Travelers Who Have Overstayed the Lawful Period of Admission to the United States

The test agent did not evaluate air exit against the requirement in the Operational Requirements Document that it "identify travelers who have overstayed the lawful period of admission" (known as overstays). The test agent reported that this capability is performed by DHS's Arrival and Departure Information System, not air exit.[8] Air exit supports this

[5]CBP officers receive no-match notifications on a work-issued mobile device called the Biometric Exit Mobile Application.

[6]If TVS is meeting its 90 percent minimum true acceptance rate, 10 percent of travelers will generate a no-match notification even though they have images in the gallery.

[7]For example, CBP's Automated Targeting System is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals, and other persons who pose a higher risk of violating U.S. law. The CBP National Targeting Center and ports of entry use the Automated Targeting System capabilities to augment a CBP officer's decision-making about whether a passenger or crewmember should receive additional inspection. CBP's Unified Passenger updates and replaces the older functionality of the legacy Automated Targeting System interface. Unified Passenger processes traveler information against other information available in the Automated Targeting System and applies risk-based rules centered on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence from DHS and other government agencies.

[8]The Arrival and Departure Information System consolidates biographic, biometric, and encounter data on foreign nationals from various systems. DHS uses the system to facilitate the investigation of subjects of interest who may have violated their immigration status by remaining in the United States beyond their authorized period of admission. DHS also uses the Arrival and Departure Information System to determine visa or immigration eligibility and to support law enforcement, intelligence, and national security investigations.

capability by providing biometrically confirmed crossing records to the Arrival and Departure Information System, but air exit itself does not identify overstays. Program officials said this requirement was added to the Operational Requirements Document before they fully understood air exit's capabilities.

Improve Accuracy and Availability of Country-by-Country Immigration Statistics

The test agent did not evaluate air exit against the requirement in the Operational Requirements Document that it "improve accuracy and availability of country by country immigration statistics." The test agent reported that immigration statistics can be generated from the Arrival and Departure Information System or other government databases, and air exit supports this function by providing biometrically confirmed crossing records to the system. Program officials said this requirement was added to the Operational Requirements Document before they fully understood air exit's capabilities.

Cyber Resiliency

The test agent reported that air exit previously underwent cybersecurity testing, but that testing was inconclusive and resulted in additional system updates. CBP plans to conduct a follow-on test for cyber resiliency, to be completed by December 31, 2020. In 2019, we reported that department-wide, few programs within DHS conducted cyber resilience testing.[9] In the same report, we noted that CBP did not conduct cyber resilience testing for air exit because the program needed additional time to develop a more rigorous test plan. Program officials told us they proceeded with the operational test because they did not want the cyber test plan to delay the program's progress.

Suitability

The Operational Requirements Document included measures of suitability. Measures of suitability assess whether a system or program is functioning as expected in its intended operational environment, such as airports. The test agent assessed eight of the nine measures of suitability and found that air exit was "suitable with limitations." The test agent found air exit met the reliability, maintainability, and availability requirements, among others, meaning the system functioned consistently. However, the test agent found that air exit's technical support is not handled by CBP (integrated logistics support) and did not provide adequate training to CBP officers. An explanation of the measures that were found to be not suitable or were not evaluated is provided in table 10 below.

[9]GAO, *Homeland Security Acquisitions: Opportunities Exist to Further Improve DHS's Oversight of Test and Evaluation Activities,* GAO-20-20 (Washington, D.C.: Oct. 24, 2019).

Table 10: Measures of Suitability and Operational Test Results for Air Exit

Measure of suitability	Result of operational testing
Reliability	Suitable
Maintainability	Suitable
Availability	Suitable
System salability	Suitable
Survivability	Suitable
Biometric air exit system rules and regulation compliance	Suitable
Biometric air exit system privacy compliance	Not evaluated
Integrated logistic support	Not suitable
Training	Not suitable

Source: U.S. Customs and Border Protection. I GAO-20-568

Biometric Air Exit System Privacy Compliance

The test agent did not evaluate air exit's compliance with system privacy requirements, meaning whether air exit systems were secure and had appropriate access controls. The test agent reported that air exit's system privacy compliance could not be confirmed with the available data and that future operational testing would assess this requirement. Earlier in this report, we discussed steps CBP took to incorporate privacy protections for travelers' personally identifiable information according to DHS's Fair Information Practice Principles (see table 1). As we noted, we did not assess security protection or its oversight in this review.

Integrated Logistic Support

The test agent found that the Integrated Logistic Support requirement (meaning technical support from a help desk) was "not suitable" because it is not handled by CBP. Technical incidents are handled by the airline or airline technical support personnel.

Training

The test agent found the training CBP officers received on how to use the no-match notifications during air exit operations to be "not suitable." The test agent reported that CBP officers at airports received little training on how to use the air exit notifications to support CBP operations at air exit. The officers interviewed during the operational test stated that the training was inadequate, if they recalled air exit training at all. However, the test agent also reported that the lack of training had no impact on operations because the CBP officers did not receive actionable information from no-match notifications, as described above.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 13, 2020

Rebecca Gambler
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-20-568, "FACIAL RECOGNITION: CBP & TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy & System Performance Issues"

Dear Ms. Gambler,

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of progress made by U.S. Customs and Border Protection (CBP) with testing and deploying facial recognition technology (FRT) at ports of entry to create entry-exit records for foreign nationals, as part of its Biometric Entry-Exit Program, and on the Transportation Security Administration's (TSA) pilot tests to assess the feasibility of using FRT. DHS remains committed to facilitating legitimate travel and securing U.S. borders through expanded use of facial recognition matching that sustains privacy protections, while also maintaining high standards of transparency and accountability.

For example, in 2017, CBP developed and implemented the Traveler Verification Service (TVS) as its facial recognition matching service as part of the congressional mandate to implement a biometric entry-exit system. TVS is an efficient, accurate, and secure manner to verify identity. As acknowledged in the draft report, CBP, in partnership with airlines, deployed FRT to 27 airports to biometrically confirm travelers' identities when they depart the United States (air exit) and was in the early stages of assessing FRT at sea and land ports of entry during field work for this report. CBP is currently working to

implement TVS for biometric air exit for 97 percent of in-scope[1] departing commercial air travelers from the United States, by the end of Fiscal Year 2021.

To monitor the progress towards meeting the 97 percent goal, CBP's Office of Field Operations (OFO) generates weekly-automated reports that track usage and biometric confirmation rates, as well as weekly performance reports for each stakeholder to encourage increased TVS usage. As this effort involves usage by airlines, airport authorities, sea cruise lines, and seaport authorities, and other stakeholders, CBP's increase of availability of TVS at all air, land, and sea ports of entry will encourage an increase in the operational use of TVS.

In addition to ensuring the accuracy of TVS, CBP remains committed to ensuring that the use of technology sustains, and does not erode, privacy protections. CBP takes privacy very seriously, and is dedicated to protecting the privacy of all travelers. For example, CBP provides notice to individuals regarding the collection, use, dissemination, and maintenance of personally identifiable information as part of efforts to promote transparency.

To ensure that CBP and its stakeholders take appropriate measures to mitigate privacy and security risks associated with biometric data collection, CBP developed a comprehensive audit plan, which was provided to the GAO in April 2020. The audit plan includes security interviews with partner information technology departments, security scans of biometric processing systems, and penetration tests of those systems. CBP uses the totality of this information to determine whether a system is secure and subsequently, if the information exchanged in the system is equally safeguarded.

Further, TSA's participation in this audit is consistent with its commitment to transparency and accountability regarding the use of biometric technology for identity verification at the TSA checkpoint. As acknowledged in the draft report, it is too early to fully assess TSA's compliance with privacy protection principles. We reiterate, however, our commitment that DHS' Fair Information Practice Principle will continue to guide TSA as it seeks to protect passenger privacy while achieving the operational and security benefits of biometric technology and improving the passenger experience.

It is important to note, however, that DHS believes that many of the performance rates for face recognition algorithms outlined in the National Institute of Standards and Technology (NIST) December 2019 report are not acceptable for use in CBP operations. For example, CBP uses an algorithm evaluated by NIST and confirmed to be high-performing, ranking first or second in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP, calling the

[1] An "in-scope" traveler is any person who is required by law to provide biometrics upon exit from the United States pursuant to 8 CFR 235.1(f)(ii).

demographic differential for "undetectable."[2] The performance metrics described by NIST are consistent with CBP operational performance metrics for entry-exit, and CBP's operational data continues to show there is no measurable differential performance in matching based on demographic factors. Moreover, the NIST FRVT 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 many of the performance rates specified in the NIST report are not acceptable for use in CBP operations, CBP does not use them. CBP believes the only relevant parts of the report, for the purposes of GAO's draft report, are the specific sections on algorithm performance for algorithms that CBP actually uses.

The draft report contained five recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2020.08.13 08:56:03 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

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

Attachment: Management Response to Recommendations Contained in GAO-20-568

GAO recommended that the Commissioner of CBP:

Recommendation 1: Ensure that the Biometric Entry-Exit Program's privacy notices contain complete and current information, including all of the locations where facial recognition is used and how travelers can request to opt out as appropriate.

Response: Concur. CBP's OFO will collaborate with the CBP Office of Public Affairs to publish: 1) Biometric Entry-Exit privacy information; 2) locations where facial recognition is used; and 3) traveler opt-out procedures on CBP's public-facing website, as well as to review and update that information on a monthly basis. CBP's OFO will also ensure that information provided in response to inquiries via the CBP Call Center is also reviewed and updated monthly. Estimated Completion Date (ECD): December 31, 2020.

Recommendation 2: Ensure that the Biometric Entry-Exit Program's privacy signage is consistently available at all locations where CBP is using facial recognition.

Response: Concur. It is important to note that, unlike Federal Inspection Services areas, the airport departure areas are not managed by CBP personnel. However, CBP OFO will continue to work with its airlines/airport partners to ensure that privacy signage is available, on display, and reflective of current privacy messaging for travelers. For example, CBP provides notice to individuals regarding the collection, use, dissemination, and maintenance of personally identifiable information as part of efforts to promote transparency. While CBP acknowledges that operational constraints may affect the placement of signs or the timely posting of updated signage, the overall public is informed that stakeholders are taking photos in coordination with CBP. Further, CBP's OFO regularly conducts periodic signage audits that include local CBP personnel to ensure signs are accurate and placed appropriately.

In addition, CBP notifies travelers at these ports using verbal announcements, signs, and message boards, as appropriate, that CBP takes these photos for identity verification purposes. Travelers are also informed of their ability to request alternative identity verification procedures. Also publicly stated are notifications that, should a traveler decide to request alternative identity verification procedures, the airline would conduct manual identity verification using his/her travel document, and may notify CBP to collect biometrics, such as fingerprints, if applicable. CBP's OFO will also continue to work with airline and airport partners to identify other methods to communicate the use of facial recognition and travelers' privacy rights. ECD: June 30, 2021.

4

Recommendation 3: Direct the Biometric Entry-Exit Program to develop and implement a plan to conduct privacy audits of its commercial partners', contractors', and vendors' use of personally identifiable information.

Response: Concur. In the air exit environment, CBP OFO will continue to conduct security reviews on partner biometric capture equipment and all interfaces with CBP's TVS, as detailed in the Biometric Entry-Exit Program audit plan, provided to GAO in April 2020. This audit plan enables a comprehensive review of compliance with security and privacy requirements on the part of CBP and CBP's partners. As mentioned in the draft report, CBP completed one partner audit thus far. Although, CBP planned additional audits for 2020, due to the COVID-19 global health pandemic and subsequent travel restrictions, CBP paused the planned audit activities. Once pandemic travel restrictions are lifted, CBP's OFO and Office of Information Technology (OIT) will resume conducting audits. Further, CBP's Privacy and Diversity Office is finalizing its CBP Privacy Evaluation of TVS, which evaluates TVS program protections identified in previously issued compliance documentation, such as Privacy Impact Assessments.

CBP's OFO and OIT plan to conduct four to six reviews per year that will begin after COVID-19 travel restrictions are lifted. ECD: June 30, 2021.

Recommendation 4: Develop and implement a plan to ensure that the biometric air exit capability meets its established photo capture requirement.

Response: Concur. The CBP's Biometric Entry-Exit Program's Air Exit Segment was granted Acquisition Decision Event 3 in December 2019. One of the action items from this decision was to complete an update to the Operational Requirements Document (ORD). CBP's OFO will update the ORD by removing the photo capture requirement, as this requirement is not applicable to current air exit operations. ECD: June 30, 2021.

Recommendation 5: Develop a process by which Biometric Entry-Exit program officials are alerted when the performance of air exit facial recognition falls below established thresholds.

Response: Concur. CBP's OFO has a suite of tools for system and operational performance management, and OFO creates three types of performance reports that are automatically generated and distributed on a weekly basis within CBP and to external stakeholders. These reports include:

1. Saturation Report: Notes the percentage of flights biometrically processed out of the total number of possible international departures segmented by airport.
2. Biometric Air Exit Overview Report: Includes a daily synopsis of operational performance data including numbers of biometrically processed flights and travelers together with biometric match rates.

5

3. Stakeholder Raw Data Reports: Provides Air Exit stakeholders with operational performance data by flight number, passenger counts, and biometric match rates.

The OFO's Biometric Entry-Exit Air team monitors these reports for performance issues and addresses any anomalies with stakeholders as they arise. These reports are also used to promote/increase usage by stakeholders.

CBP's OFO also conducts random sampling to determine the technical match rates and identify any system or equipment issues. The random sampling is conducted on a weekly basis and includes two flights per airport per week.

Finally, CBP's OFO receives alert notifications if TVS experiences an outage, and has a Gallery Assembly System monitor that provides notifications when a flight gallery is not created. Depending on the severity and impact to end users, OFO generates stakeholder notifications, as appropriate.

We request that GAO consider this recommendation resolved and closed, as implemented.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact:

Rebecca Gambler, (202) 512-8777 or gamblerr@gao.gov

Staff Acknowledgments:

In addition to the contact named above, Adam Hoffman (Assistant Director), Jason Jackson (Analyst-in-Charge), Jennifer Beddor, Kelsey Burdick, Ann Halbert-Brooks, Richard Hung, and Sasan J. “Jon” Najmi, made significant contributions to this report. Also contributing to the report were Rick Cederholm, Benjamin Crossley, John de Ferrari, Alexis Olsen, Kevin Reeves, and Terry Richardson.