United States Government Accountability Office

Testimony

Before the Subcommittee on Border Security, Facilitation, and Operations, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, July 27, 2022

FACIAL RECOGNITION TECHNOLOGY

CBP Traveler Identity Verification and Efforts to Address Privacy Issues

Statement of Rebecca Gambler, Director,
Homeland Security and Justice

July 27, 2022

FACIAL RECOGNITION TECHNOLOGY

CBP Traveler Identity Verification and Efforts to Address Privacy Issues

GAO Highlights

Highlights of GAO-22-106154, a testimony before the Subcommittee on Border Security, Facilitation, and Operations, Committee on Homeland Security, House of Representatives

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. Federal laws require DHS to implement a biographic and biometric data system for foreign nationals entering and exiting the U.S. In response, CBP has been pursuing FRT to verify a traveler's identity in place of a visual inspection of travel identification documents.

This statement addresses the extent to which CBP has (1) incorporated privacy principles in and (2) assessed the accuracy and performance of its use of FRT. This statement is based on a September 2020 report (GAO-20-568), along with updates as of July 2022 on actions CBP has taken to address prior GAO recommendations. For that report, GAO conducted site visits to observe CBP's use of FRT; reviewed program documents; and interviewed DHS officials.

What GAO Recommends

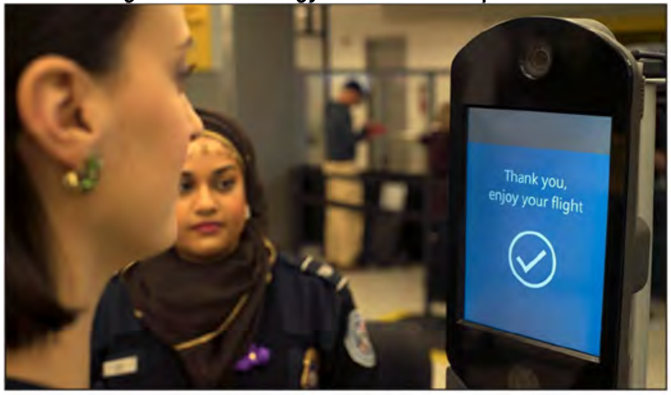
In September 2020, GAO made five recommendations to CBP regarding privacy and system performance of its FRT. DHS concurred with the recommendations and has implemented two of them. CBP is taking steps to address the remaining three recommendations related to (1) current and complete privacy signage, (2) implementing an audit plan for its program partners, and (3) capturing required traveler photos.

View GAO-22-106154. For more information, contact Rebecca Gambler at (202) 512-8777 or gamblerr@gao.gov.

What GAO Found

U.S. Customs and Border Protection (CBP) has made progress testing and deploying facial recognition technology (FRT) at air, sea, and land ports of entry to create entry-exit records for foreign nationals as part of its Biometric Entry-Exit Program. As of July 2022, CBP has deployed FRT at 32 airports to biometrically confirm travelers' identities as they depart the United States (air exit) and at all airports for arriving international travelers.

Facial Recognition Technology in Use at an Airport



Source: U.S. Customs and Border Protection. | GAO-22-106154

In September 2020, GAO reported that CBP had incorporated privacy principles in its program, such as prohibiting airlines from using travelers' photos for their own purposes. However, CBP had not consistently provided travelers with information about FRT locations. Also, CBP's privacy signage provided limited information on how travelers could request to opt out of FRT screening and were not always posted. Since that time, CBP has ensured that privacy notices contain complete information and is taking steps to ensure signage is more consistently available, but needs to complete its efforts to update signs in locations where FRT is used. Further, CBP requires its commercial partners, such as airlines, to follow CBP's privacy requirements and could audit partners to assess compliance. As of May 2020, CBP had audited one airline partner and did not have a plan to ensure all partners were audited. In July 2022, CBP reported that it has conducted five assessments of its air partners and has three additional assessments underway. These are positive steps to help ensure that air traveler information is safeguarded. However, CBP should also audit other partners who have access to personally identifiable information, including contractors and partners at land and sea ports of entry.

CBP assessed the accuracy and performance of air exit FRT capabilities through operational testing. Testing found that air exit exceeded its accuracy goals but did not meet a performance goal to capture 97 percent of traveler photos. As of July 2022, CBP officials report that they are removing the photo capture goal because airline participation in the program is voluntary and CBP does not have staff to monitor the photo capture process at every gate.

Chairwoman Barragán, Ranking Member Higgins and Members of the Subcommittee:

I am pleased to be here today to discuss our work on U.S. Customs and Border Protection's (CBP) use of facial recognition technology (FRT) at ports of entry.[1] FRT has become increasingly common across business and government as a tool for identifying or verifying customers or persons of interest. Within the Department of Homeland Security (DHS), 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. As part of this mission, federal laws require DHS to implement a biographic and biometric data system for foreign nationals entering and exiting the U.S. In response to these laws, CBP has been pursuing FRT to automatically verify a traveler's identity in place of a visual inspection of travel identification documents.[2] Traditionally, CBP has 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, automating the identity verification process using FRT helps increase their ability to detect fraudulent travel identification documents, as well as expedite identity verification processes.

[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] 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 foreign nationals on departure from the United States) 235.1(f) (any foreign national may be required to provide biometric identifiers on entry, except certain Canadian tourists or businesspeople; foreign nationals younger than 14 or older than 79; and diplomatic visa holders, among other listed exemptions. Additionally, foreign nationals required to provide biometric identifiers on entry may be subject to departure requirements for biometrics under § 215.8, unless otherwise exempted). We use the term foreign national in this statement to refer to 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 residents are also in-scope for biometric collection and included in the definition of foreign nationals.

CBP officers are responsible for inspecting international travelers—including foreign nationals and U.S. citizens—arriving at ports of entry. Officers 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. Additionally, CBP is responsible for confirming foreign national departures from the U.S. to determine if their exit occurred by expiration of the authorized period of stay as defined by their temporary status.

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 identify overstays.[3] 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 depart the country, such as differences in logistics and infrastructure among ports of entry.[4]

To meet the requirement to implement a biometric exit capability, over the years CBP has tested various biometric technologies in different locations to determine which type of technology could be deployed on a large scale

[3] 8 U.S.C. § 1365b, 8 C.F.R. §§ 215.8, 235.1. A foreign national in the United States on a temporary basis who remains in the country beyond their authorized period of admission is classified as an overstay. 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] See, for example, 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) and *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).

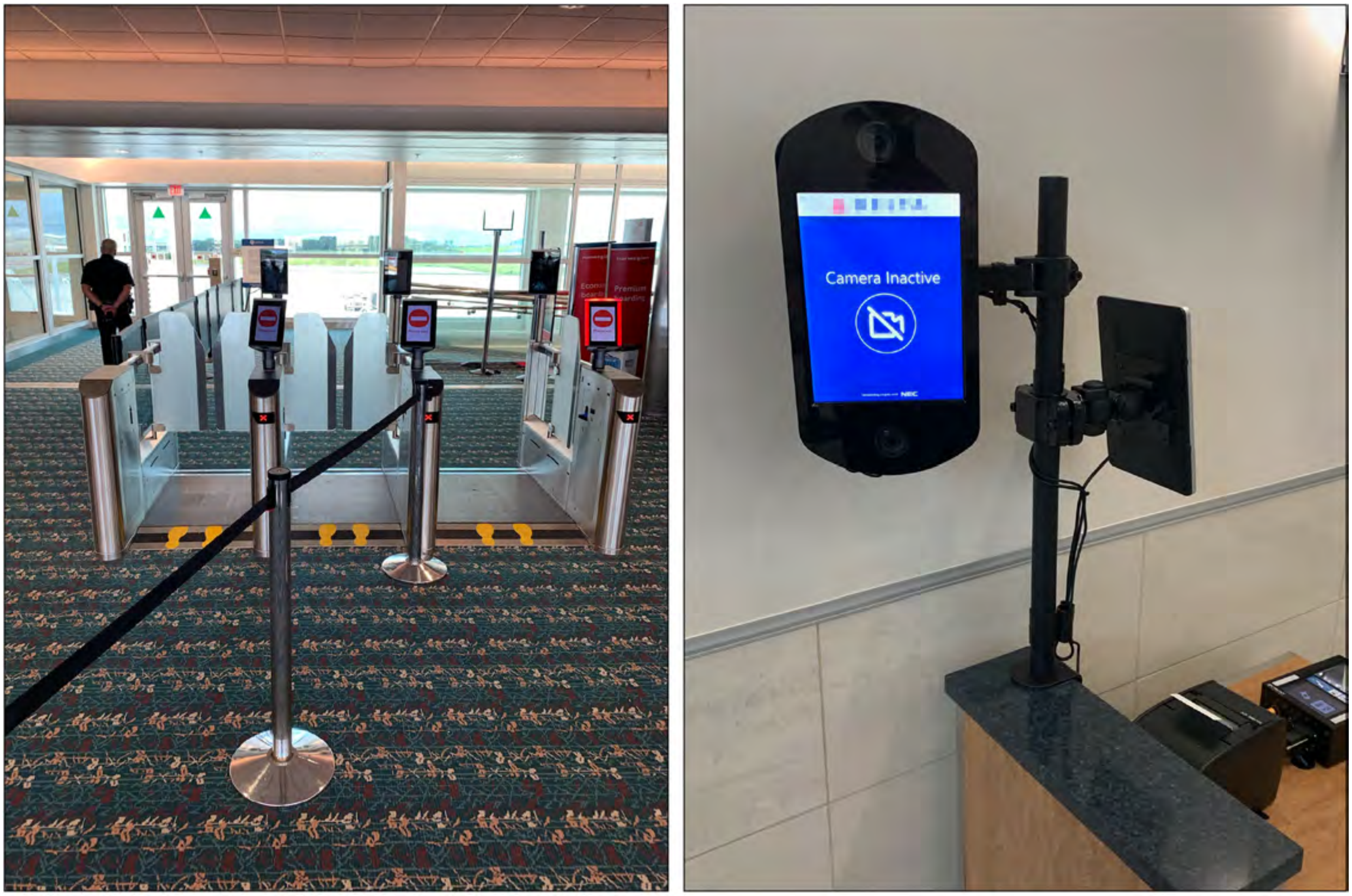
without disrupting legitimate travel and trade.[5] Based on the results of its testing, CBP concluded that FRT was the most operationally feasible and traveler-friendly option for a comprehensive biometric solution for travelers departing the U.S, as well as those entering. Since then, CBP has prioritized testing and deploying FRT for departing and arriving travelers at airports (referred to, respectively, as air exit and air entry), with seaports and land ports of entry to follow. These tests and deployments are part of CBP's Biometric Entry-Exit Program.

As of July 2022, CBP has partnered with airlines and airport authorities to deploy FRT to at least one gate at 32 airports for travelers exiting the United States (air exit) and to all airports for travelers entering the United States (air entry), according to CBP officials.[6] With regard to the sea environment, CBP has deployed FRT at 26 seaports for travelers entering the U.S. (sea entry). With regard to the land environment, CBP has deployed FRT at all 159 land ports of entry for pedestrians entering the U.S. (land entry), and is in the early stages of pilot testing FRT for travelers entering the U.S. in vehicles and departing the U.S. as pedestrians or in vehicles (land exit). Figure 1 shows examples of cameras used for air exit facial recognition.

[5] 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.

[6] As of July 2022, CBP officials said that FRT was currently deployed for air exit at 26 airports. There are an additional 6 airports where FRT was piloted or previously deployed, but where it is not currently deployed or in use.

Figure 1: Examples of Cameras Used for Air Exit Facial Recognition



Source: GAO. | GAO-22-106154

In September 2020, we reported on CBP's efforts to develop its FRT capabilities at ports of entry, including the extent to which CBP incorporated privacy protection principles and assessed the accuracy and performance of its FRT.[7] My statement today will summarize information from that report, as well as actions CBP has taken, as of July 2022, to address our recommendations from the report. To conduct the work from

[7] GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, D.C.: Sept. 2, 2020).

the September 2020 report, we conducted site visits to observe CBP's use of FRT in all three travel environments—air, land, and sea; reviewed program documents; and interviewed DHS officials. More detailed information on our objectives, scope, and methodology is contained in our September 2020 report.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. These 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

How Facial Recognition Technology Works

FRT uses an image or video of a person's face to identify them or verify their identity. Facial recognition, like fingerprint-matching technology, 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. FRT uses a photo or a still from a video feed of a person and converts it into a template, or a mathematical representation of the photo.[8] For some facial recognition functions, if the technology detects a face, a matching algorithm then compares the template to a template from another photo and calculates their similarity.[9] 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

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

[9] 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. For more information on the commercial use of FRT see GAO, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522 (Washington, D.C.: July 13, 2020).

another photo of the same person (verification of a face against a source photo, such as a passport photo).

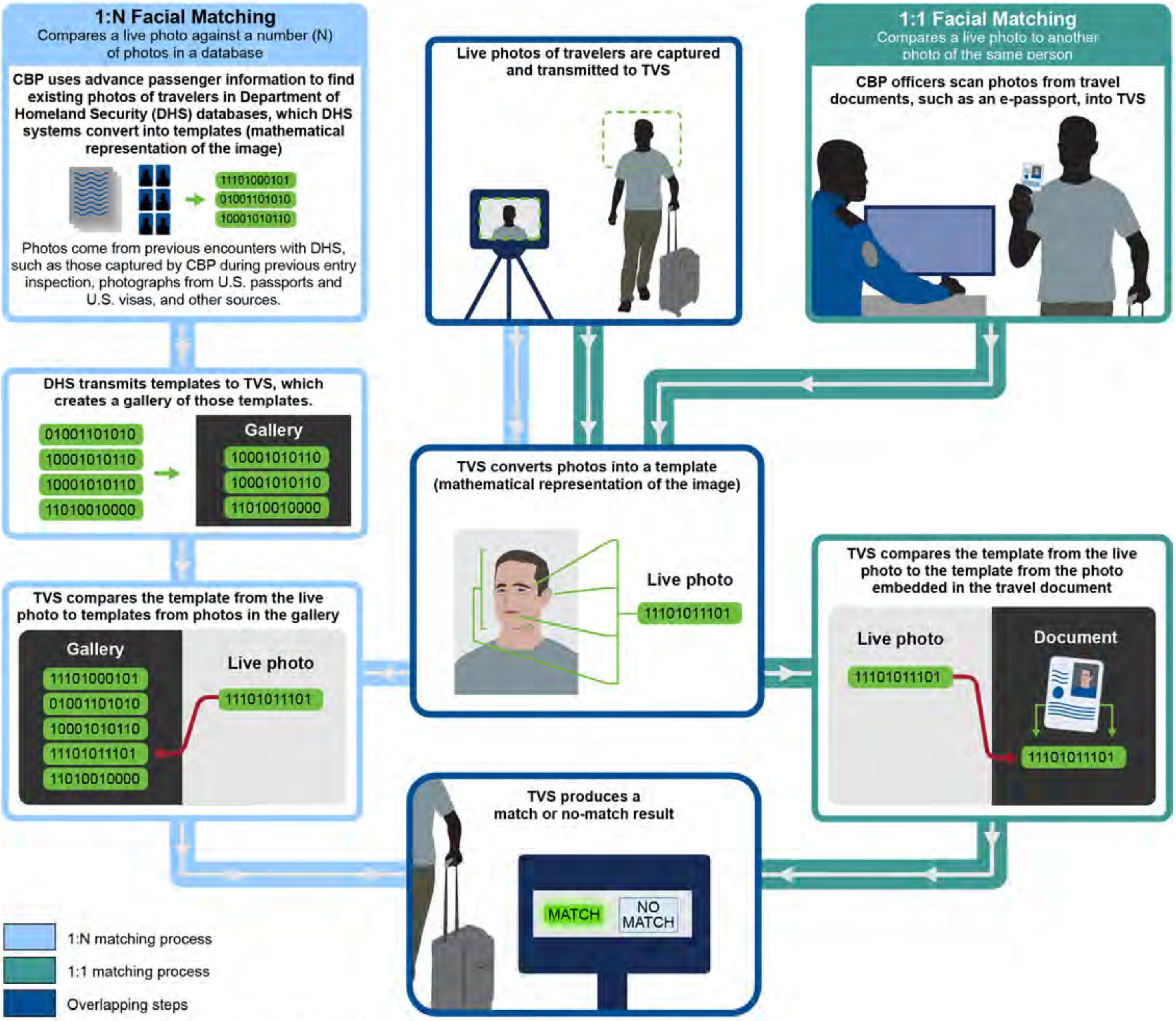
In 2017, CBP developed and implemented the Traveler Verification Service (TVS) as the facial recognition matching service for the Biometric Entry-Exit Program. Since then, CBP has been deploying TVS in segments based on the air, sea, and land travel environments at ports of entry.[10] TVS is a cloud-based 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.

In the air and sea environments, CBP receives travelers' biographic information in advance of travel through passenger manifests submitted by aircraft operators and sea carriers. TVS searches DHS databases of photos associated with travelers listed on the manifest and then creates a pre-staged "gallery" of those photos.[11] 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. With 1:N matching, TVS compares a live photo of a traveler against photos of multiple travelers in the pre-staged gallery. For 1:1 matching, TVS electronically compares a live photo of a traveler against another photo of that traveler, such as a passport photo from their travel documents. This type of matching can be used when CBP does not have passenger manifest information or does not have an existing photo available for matching. Figure 2 shows how TVS performs facial matching.

[10] For example, beginning in 2017, CBP partnered with airlines and airport authorities to deploy facial recognition for identity verification at airport departure gates. 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.

[11] According to CBP officials, CBP has also begun creating galleries from commercial vehicle manifests at land ports of entry, as well as testing the feasibility of creating galleries of frequent border crossers.

Figure 2: Illustration of How CBP's Traveler Verification Service (TVS) Performs Facial Matching


1:N Facial Matching
Compares a live photo against a number (N) of photos in a database
CBP uses advance passenger information to find existing photos of travelers in Department of Homeland Security (DHS) databases, which DHS systems convert into templates (mathematical representation of the image)
11101000101
01001101010
10001010110
Photos come from previous encounters with DHS, such as those captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and other sources.
Live photos of travelers are captured and transmitted to TVS
1:1 Facial Matching
Compares a live photo to another photo of the same person
CBP officers scan photos from travel documents, such as an e-passport, into TVS
DHS transmits templates to TVS, which creates a gallery of those templates.
01001101010
10001010110
10001010110
11010010000
Gallery
10001010110
10001010110
11010010000
TVS converts photos into a template (mathematical representation of the image)
Live photo
11101011101
TVS compares the template from the live photo to templates from photos in the gallery
Gallery
11101000101
01001101010
10001010110
11101011101
11010010000
Live photo
11101011101
TVS compares the template from the live photo to the template from the photo embedded in the travel document
Live photo
11101011101
Document
11101011101
TVS produces a match or no-match result
MATCH
NO MATCH
🟦 1:N matching process
🟩 1:1 matching process
■ Overlapping steps

Source: GAO analysis of U.S. Customs and Border Protection information. | GAO-22-106154

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

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

In our September 2020 report, we found that CBP’s Biometric Entry-Exit Program incorporated some privacy protection principles consistent with the Fair Information Practice Principles DHS adopted, which serve as the basis for DHS’s privacy policy.[12] For example, CBP’s commercial partners, such as air carriers, are prohibited from storing or using travelers’ photos for their own business purposes and can only view a match/no match result, which relate to the data use limitation principle. Further, CBP has published a Privacy Impact Assessment for TVS that includes information on privacy protections, has a website for the program, and provides onsite signage to notify travelers about facial recognition, which relate to the transparency principle.

While 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, in September 2020 we found that CBP’s privacy notices to inform the public 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, outdated signs at airports, information

[12] The Fair Information Practice Principles adopted by the DHS Chief Privacy Officer are the basis for DHS’s privacy policy and include the following eight principles: transparency, purpose specification, individual participation, data minimization, use limitation, security, data quality and integrity, and accountability and auditing. DHS requires its components—including CBP—to comply with the principles when using personally identifiable information. 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).

on opting out included in privacy notices, and placement of signs at ports of entry. For example:

- CBP online resources and call center had incomplete information. We found that CBP's public website on the Biometric Entry-Exit Program did not accurately reflect the locations where CBP used or tested FRT. Therefore, travelers who checked the website would not see a complete list of locations where they may encounter FRT. In addition, CBP has a call center for travel or customs questions. During five calls we placed to the call center 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.
- 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).The first sign was an outdated notice, as CBP changed the data retention period for photos of 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 they try to update signs when new guidance is issued but said that printing new signs is costly and it is not practical to print and deploy a complete set of new signs immediately after each change or update.
- Notices provided limited information on opting out of facial recognition identity verification. 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, CBP's signs at airport facial recognition locations 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 airport gates, so including this information on a sign could potentially be confusing to a traveler or make it less likely they would request to opt out during air exit.
- Signs were missing. We found that CBP signs at facial recognition locations were not consistently posted or were posted in such a way

that they were not easily seen by travelers. CBP requires that its commercial partners—such as airlines, airports, or cruise lines—post CBP-approved privacy signs at gates where FRT is used to provide travelers with notice that their photos are being taken and for what purposes.[13] However, CBP has not enforced the requirement to post these signs or consistently monitored air exit facial recognition locations to ensure that signs are posted for each flight using FRT. For example, 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.

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 at boarding gates for each flight that uses FRT since they have other duties and responsibilities and are not required by CBP policy or guidelines to do so. Nonetheless, CBP officials acknowledged that CBP is ultimately responsible for informing travelers about FRT across all environments and locations through signs, handouts, and the CBP website, among other methods.

In September 2020, we recommended that CBP 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. CBP implemented this recommendation. Specifically, CBP created a new website that outlines the locations (air, land, and seaports) where CBP uses FRT. CBP also updated its biometrics website to include information on how travelers can opt out of the facial recognition verification process. Furthermore, CBP has begun providing its call center and information center staff with additional training, so staff are prepared to provide the

[13] 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 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 FRT. 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 FRT through emails sent along with reservation information.

public with complete and current information about the facial recognition verification program.

We also recommended that CBP ensure that the Biometric Entry-Exit Program's privacy signage is consistently available at all locations where CBP is using facial recognition. In June 2022, CBP reported that the program office developed a plan to ensure privacy signage for the Biometric Entry-Exit program is consistently available at all locations where FRT is used. As part of that plan, CBP officials said they reviewed the signage language and updated it to be more understandable by, for example, making it clearer that travelers can request alternative screening procedures. CBP also stated that the program office is in the process of upgrading the signs and intends to do so by September 2022. These actions, if fully implemented, should address the intent of our recommendation.

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, in September 2020 we reported that as of May 2020, CBP had audited 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 particular, we found that although CBP's commercial airline partners have used FRT for identity verification since 2017, and cruise lines since 2018, CBP's first audit of a commercial partner occurred in March 2020. 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. At that time, CBP officials said that they expected this initial audit to inform how they design and conduct future audits of commercial partners. However, CBP had not developed a plan with time frames for conducting audits of all of its commercial partners.

Similar to CBP's commercial partners, contractors and vendors associated with the Biometric-Entry Exit 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. However, prior to a 2019 data breach involving a CBP subcontractor, CBP had not conducted security or privacy audits of its contractors. In 2019, a CBP subcontractor downloaded photos used in facial matching pilot testing at a land port of entry against CBP protocols.

The subcontractor was later the subject of a data breach.[14] CBP information security officials stated that it is unclear if this particular security vulnerability would have been identified through an audit because protocols were in place that prohibited contractors from downloading and removing data. However, after CBP identified this vulnerability, CBP information security officials began conducting security audits 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. However, in September 2020, we reported that CBP did not have a plan to determine when all contractors and vendors would be audited for compliance with privacy and security requirements.

The Fair Information Practice Principles adopted by DHS 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 such audits but said they have generally not been a priority because CBP's contractors and partners do not have access to internal CBP databases and, therefore, cannot access systems that store personally identifiable information. 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 had not yet audited the majority of its airline business partners to ensure they are adhering to CBP's privacy requirements.

[14] According to CBP, a subcontractor employee involved with the pilot test at the Anzalduas land port of entry removed facial image data from the pilot site and then downloaded them to the company's network for the purpose of performing additional analysis of CBP's data. Data from the subcontractor's network was then 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.

In addition, while CBP had audited one of its airline partners and some locations where it was pilot-testing FRT, we reported that the privacy risks associated with personally identifiable information would continue to grow as the Biometric Entry-Exit Program expands and CBP collaborates with additional airlines, airports, cruise lines, contractors, and others. Thus, we recommended that CBP 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. CBP concurred with our recommendation and, as of July 2022, officials said that CBP has conducted five assessments of its commercial partners in the air environment to ensure that they are adhering to CBP's requirements to protect travelers' privacy. Officials also said that three additional assessments are underway and that CBP has plans to assess about four partners in the air environment each year through 2025. These are positive steps to help ensure travelers' privacy is protected. To fully address the intent of our recommendation, CBP should complete its planned and in-progress assessments in the air environment. In addition, CBP should audit partners in the land and sea environments as well as vendors and contractors who have access to personally identifiable information.

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

During Operational Testing, Air Exit Met Accuracy Requirements but Did Not Meet Photo Capture Performance Requirement

As we reported in September 2020, air exit was the first Biometric Entry-Exit Program capability to progress through the DHS acquisition process and undergo formal operational 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 was to be assessed against program requirements in an operationally realistic environment before it could be fully deployed—referred to as operational testing.[15] From May to June 2019, an independent test agent within CBP performed an operational test and evaluation of air exit facial recognition capabilities.

CBP's operational testing determined that air exit met its defined accuracy requirements but did not meet one of its performance requirements. 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. In August 2019, the test agent found that air exit met or exceeded its two accuracy requirements. Specifically, the test found 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 test also found that air exit incorrectly matched a traveler to a gallery photo less than 0.1 percent of the time.

While air exit met its accuracy requirements during operational testing, it did not meet the program's photo capture performance requirement—that is, the percentage of in-scope travelers whose photos should be captured during the boarding process (also called the biometric compliance rate). Specifically, 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 boarding. The report found that such 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, such as families or individuals using wheelchairs, to speed up the boarding process. 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. The test report noted that testing officials witnessed instances of cameras malfunctioning during boarding at all three of the

[15] 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 by Actions Needed to Enhance Oversight of Schedule Goals,* GAO-20-170SP (Washington, D.C.: Dec. 19, 2019).

airports they visited. During our observations of five flights at three airports in 2019, we identified similar photo capture issues with air exit.

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. Officials suggested that this was one metric of many 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. These factors include 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). Because airline and airport partners participate in air exit voluntarily, they can choose to manually verify travelers' identities (not use FRT) 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. At the time of our 2020 report, CBP did not intend to require airlines to capture photos of all in-scope travelers and did not have a plan to ensure that air exit could meet the 97 percent photo capture requirement defined in its operational requirements document. CBP officials stated that the photo capture rate would naturally improve as air exit expands throughout airports. However, we reported that improved familiarity with facial recognition procedures would 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.

In September 2020, we recommended that CBP develop and implement a plan to ensure that the biometric air exit capability meets its established photo capture requirement. CBP agreed with the recommendation. In June 2022, CBP officials noted that the photo capture rate requirement was included in the 2017 Operational Requirements Document when there was the possibility of CBP owning, operating, and maintaining cameras at airport departure gates. As the photo capture process was implemented, CBP determined that it does not have the staff to be present at every departure gate to oversee the process. Further, CBP does not require airlines to take a photo of every traveler. According to CBP officials, the photo capture requirement was removed from the latest draft of the Operational Requirements Document and CBP is waiting for the revised requirements to be fully approved by DHS, which it expected in August 2022. We will continue to follow up on the status of these revised requirements and the extent to which they may address our recommendation once approved by the department.

Effort to Assess the Accuracy of CBP's Facial Matching Across Demographic Variables

In addition to CBP's accuracy assessment conducted during the operational test of air exit capabilities, in December 2018, the National Institute of Standards and Technology (NIST)—a government laboratory that has studied commercially available FRT—entered into an agreement with CBP to further assess the accuracy of TVS.[16] According to the terms of the agreement, NIST was 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 intended to assess the accuracy of TVS by testing an algorithm similar to that used in TVS and analyzing the impacts of gender, ethnicity, and age on matching accuracy.[17] In September 2020, we reported that CBP planned to use the same matching algorithm for all travel environments, and NIST's findings on the demographic effects on matching accuracy planned to take into account

[16] 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. A NIST evaluation in December 2019 focused on testing the effects of demographics on matching accuracy of over 100 commercially available facial recognition algorithms. 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. National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (Dec. 2019).

[17] According to CBP officials, NIST was 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.

all travel environments. Per the agreement, NIST was to provide technical information to CBP related to the algorithm, optimal thresholds, and gallery creation strategies.[18] NIST completed this report in July 2021.[19]

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

In September 2020, we reported that CBP officials conduct monitoring of the accuracy and performance of air exit through random sampling, but the monitoring process did not alert them when performance fell below minimum requirements (such as the 97 percent photo capture rate described above). CBP officials said they randomly sampled two flights per airport per week and reviewed 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 or photo capture rates, and they would investigate any identified problems by contacting the airline or airport where they occurred. In addition to random sampling, airline or airport officials can report problems with air exit facial recognition to CBP officials. 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, we reported that CBP's monitoring process did not immediately alert officials to problems that affect the performance of air exit. For example, randomly 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 or airport. 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 had a small team of five analysts dedicated to monitoring air exit's performance, and they did 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.

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

[19] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration,* NISTIR 8381 (July 2021).

However, 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. We recommended 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 agreed with our recommendation. In April 2021, CBP reported that it had developed various monitoring systems for the air exit facial recognition program. For example, CBP produces reports that provide program stakeholders with operational performance data by flight number, passenger counts, and biometric match rates. According to CBP, the program team monitors these reports for performance issues and addresses any anomalies with stakeholders as they arise. The program team also conducts random sampling to determine the technical match rates and to identify any system or equipment issues. Finally, the program team receives notifications if the system experiences an outage and has a gallery assembly system monitor that provides notifications when a flight gallery is not created. These actions addressed the intent of our recommendation.

Chairwoman Barragán, Ranking Member Higgins, and Members of the Subcommittee, this completes my prepared statement. I would be happy to respond to any questions you or the members of the subcommittee may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this statement, please contact Rebecca Gambler 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 statement.

GAO staff who made key contributions to this testimony are Adam Hoffman (Assistant Director), Kelsey Burdick, Jason Jackson, Sasan J. "Jon" Najmi, and Mary Pitts.

(106154)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548