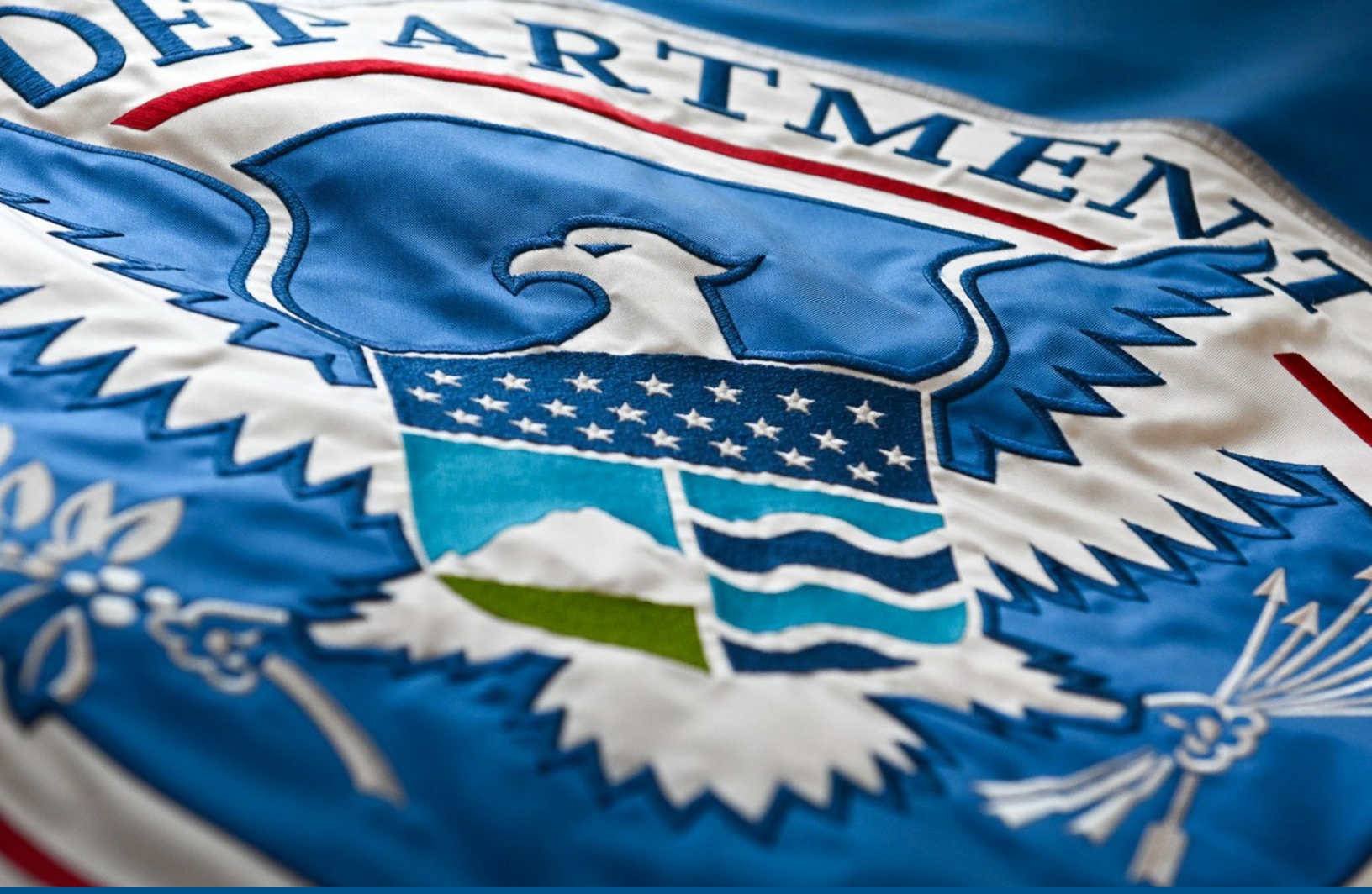


Implementation of DHS Directive 026-11: Use of Face Recognition and Face Capture Technologies

2024 Report on Select Use Cases

January 17, 2025

Homeland Security

Contents

An Update on DHS's Use of Face Recognition and Face Capture Technologies 3

The Difference Between Face Recognition and Face Capture 4

How DHS uses Face Recognition and Face Capture Technologies 4

Testing Face Recognition and Face Capture Technologies 6

U.S. Customs and Border Protection (CBP) 7

CBP Biometric Exit – Air 8

CBP Global Entry - Touchless Portals 11

CBP Global Entry - Mobile application 16

CBP Simplified Arrival - Air Entry 21

CBP Simplified Arrival – Land Pedestrian Entry 24

Homeland Security Investigations (HSI) 27

HSI Face Recognition for Investigations of Child Sexual Exploitation and Abuse 28

Transportation Security Administration (TSA) 33

TSA Credential Authentication Technology with Camera System (CAT-2) 34

TSA PreCheck®: Touchless Identity Solution 39

An Update on DHS's Use of Face Recognition and Face Capture Technologies

Face Recognition and Face Capture (FR/FC) are powerful Artificial Intelligence (AI) technologies that the Department of Homeland Security (DHS) uses to improve how the public interacts with us and to support critical law enforcement investigations, while protecting privacy and individual rights. But when used incorrectly, these technologies, like any advanced technologies, can introduce new risks and challenges.

Recognizing this, in September 2023 DHS instituted the most extensive requirements of any Federal agency to make sure that FR/FC technologies are used properly. DHS Directive 026-11, "Use of Face Recognition and Face Capture Technologies," includes requirements that:

- All uses of FR/FC technologies will be thoroughly tested to ensure there is no unintended bias or disparate impact in accordance with national standards.
- U.S. citizens are afforded the right to opt out of face recognition for non-law enforcement uses unless otherwise authorized or required, and FR/FC cannot be used as the sole basis of any law or civil enforcement related action.
- Department oversight offices including the Privacy Office, the Office for Civil Rights and Civil Liberties (CRCL), and the Office of the Chief Information Officer review all new and existing uses of FR/FC technologies.

FR/FC is a subset of AI technologies, and these requirements complement DHS's implementation of government-wide AI risk management policies. You can find all of DHS's AI use cases, including those involving FR/FC, in our AI Use Case Inventory.

After we issued our FR/FC Directive, teams across DHS worked to review all current uses of the technology and ensure compliance with these requirements. For our most significant FR/FC uses, we conducted extensive testing with hundreds of volunteers through the DHS Science & Technology Directorate's Maryland Test Facility, an internationally recognized lab with experts in biometric research and evaluation. We've also engaged extensively with civil society organizations on how we use and test FR/FC. We will continue to consult with them, as well as with the general public, on an ongoing basis.

This report presents more information than ever previously shared about how we use and govern these technologies. DHS will continue to apply our policies on the responsible use of FR/FC and conduct monitoring, testing, and evaluation to make sure that we are living up to our commitments to use AI in safe, responsible, and trustworthy ways.

The Difference Between Face Recognition and Face Capture

FR/FC technologies are often used together, but they have some important differences.

FR/FC systems use "biometric samples," which are usually a picture of an individual's face. These images can be taken live or come from an identity document like a passport or driver's license. "Biometrics" refers to measuring physical traits, such as facial features, to identify a person.

Face capture means taking a picture of an individual's face so that it can be used in a face recognition system and then applying different automated methods to verify that the photo is actually of a person's face and is of high quality.

Face recognition technology compares an individual's facial features to available images for:

- **Verification:** "One-to-one" matching to confirm a photo matches a different photo of the same person.
- **Identification:** "One-to-many" matching a photo of a person against a selection of photos from a larger group. This can happen against a database of millions of photos, but at DHS this most often involves matching against a limited, pre-built gallery of photos, such as the passport photos of passengers on a flight manifest. This limited gallery matching is more efficient and effective.

Services using FR/FC technologies follow all applicable federal laws, including the Privacy Act of 1974, the Homeland Security Act of 2002, and the E-Government Act of 2002.

How DHS uses Face Recognition and Face Capture Technologies

We identified 14 distinct uses of FR/FC at DHS, which you can see in full in our AI Use Case Inventory. Most of our FR/FC use falls into two categories:

1. Automating identity verification during domestic and international travel, to help travelers get through checkpoints more efficiently and securely.
2. Supporting law enforcement investigations as a part of investigative due process, including identifying victims of crimes and potential leads or suspects.

For this report, we selected eight use cases based on frequency of use and public interest:

DHS Component	FR/FC use case	Description of FR/FC use case
Customs and Border Protection (CBP)	**1. Biometric Exit by Air**	As passengers board international flights, a quick photo at the gate matches against their travel document photo on record, confirming their departure to improve border security and compliance with immigration laws.
	2. Global Entry: Touchless Portals	Trusted travelers step up to a Portal that captures a photo and matches it against their stored photo, expediting entry into the United States.
	3. Global Entry: Mobile Application	Global Entry members use an app on their phone to take a selfie, which is matched against their stored photo, allowing them to skip the Touchless Portals.
	4. Simplified Arrival: Air Entry	Travelers arriving to the United States on international flights have their photo taken, which is compared with a small gallery of photos of people traveling that day. This streamlines identity checks and reduces manual processing.
	5. Simplified Arrival: Land Pedestrian Entry	Travelers entering the United States at land border crossings have their photo taken, which is matched against their travel documents to streamline identity checks and reduce manual processing.
Homeland Security Investigations (HSI)	**6. Face Recognition for Investigations of Child Sexual Exploitation and Abuse**	Investigators use government databases and commercial tools, including Clearview AI, to help identify victims and offenders within child sexual abuse material. This technology has helped identify victims of child sexual exploitation and resulted in the rescue of children who may not otherwise have been rescued using other investigative means. Clearview AI is not currently used for any other types of investigations or for any other purposes anywhere at DHS.
Transportation Security Administration (TSA)	**7. Credential Authentication Technology**	At TSA checkpoints, travelers hand their ID to an officer or insert it themselves into the kiosk. The system verifies the authenticity of the ID and flight reservation, takes a photo, and matches the traveler's face to their ID.
	8. PreCheck: Touchless Identity Solution	TSA PreCheck members who have opted in approach the checkpoint and have their photo taken. Their photo is matched against photos of travelers with valid flight reservations, and travelers can proceed without presenting an ID. The prototype of the TSA PreCheck: Touchless Identity Solution is being assessed at 10 airports.

For each use case, this report explains how we provide public notice, solicit feedback, and allow opt outs in different travel scenarios.

Testing Face Recognition and Face Capture Technologies

The DHS Science and Technology (S&T) Directorate oversees testing and evaluation for FR/FC technologies. Testing happens both before technologies are put in the field where you might interact with them and at least every three years during operational use.

The Maryland Test Facility conducts robust, independent testing and evaluation of FR/FC technologies. Volunteers who represent a range of demographics sign up to help test biometric technologies in a lab set up to resemble real world conditions. While volunteers represented a wide range of demographics, breakout data is only provided in this report for demographic groups with 90 or more volunteers.

In addition to these performance tests, DHS program teams also work to continuously improve public services so that you have the best possible experience while DHS ensures national security.

DHS completed performance reviews of eight priority uses of FR/FC, based on direct testing, analysis of operational reporting statistics, and reviews of third-party testing results. We analyzed demographic differentials where possible.

Through this testing, we learned that:

- Overall, FR/FC systems performed extremely well for diverse demographic groups. On average, the technology worked more than 99% of the time for systems that are fully operational, like ID checks for travelers at the airport and ports of entry to the United States.
- TSA Credential Authentication Technology, which is used to verify authenticity of IDs and flight reservations at TSA checkpoints, had no performance issues across any demographic group.
- Our testing revealed an important finding for TSA PreCheck's prototype Touchless Identity Solution. While the face matching worked well, we encountered issues with the face detection algorithm used to verify if a photo contains a face before matching. This algorithm was accurate 88% to 97% of the time, with performance varying based on skin tone and self-reported race, gender, and age. To address this, TSA quickly introduced a manual photo capture step, which only adds 2-3 seconds to the process and does not affect the overall screening experience. TSA and DHS S&T are evaluating new algorithms to improve this step and plan to test and implement them later this year.
- We noticed two other minor trends in test results that will be monitored going forward:
    - For some CBP use cases, there were very small differences in measured face matching performance based on skin tone and self-reported race and age, ranging from less than 1% to 2-3%. Face matching still performed well overall, and the lowest success rate for any demographic group was 97%. This round of testing was only designed to reliably detect differences of 5% or greater, so we can't say if smaller measured differences reflect true underlying differences in performance. We will continue to monitor these trends, refine our testing practices, and take action as appropriate.
    - People interacted with systems quickly – in seconds, not minutes. The time to move through the FR/FC process ranged from less than 10 seconds for a Global Entry Touchless Portal to less than 30 seconds to do an ID check at an airport security checkpoint. In general, it took a few seconds longer for those aged 61+ years to complete FR/FC interactions than those 60 years and under. While not a cause for immediate concern, we will work to make sure our systems continue to be usable across all age groups.

You can view detailed test results in each section below.

U.S. Customs and Border Protection (CBP)

U.S. Customs and Border Protection (CBP) uses Face Recognition and Face Capture (FR/FC) technologies to make travel requirements more efficient. This creates a safer, more seamless, and more secure experience for travelers.

The use of biometric technology is required under multiple laws passed by Congress. The **Implementing Recommendations of the 9/11 Commission Act of 2007** authorized the U.S. Government to use an automated system to biometrically record the arrivals and departures of visitors at all air, sea, and land ports of entry.

After years of testing and piloting, CBP operationalized their face recognition technology, called the Traveler Verification Service (TVS). It's used at air, sea, and land ports of entry.

CBP Biometric Exit – Air

AI Use Case Inventory
Use Case Name: 3rd Party Traveler Identity Verification Services
Use Case ID: DHS-2414

The Biometric Exit process uses face recognition to verify your identity when exiting the United States.

Biometric Exit, which first launched in 2016, is used by Customs and Border Protection (CBP) at airports and seaports. This report focuses on implementation by carriers in U.S. airports when you exit the United States.

Biometric Exit gives CBP a biometric confirmation of your departure from the United States. It also provides identity verification before you leave the country.

Biometric Exit can also reduce processing times by allowing you to board international flights without needing to scan a boarding pass.

A camera set up at the departure gate takes your photo.

Before every flight coming to or leaving from the United States, the airlines send CBP information about passengers who will be travelling. This information is called the Advance Passenger Information System (APIS) manifest.

At your departure gate, an airline gate agent takes your photo. The camera can be freestanding or an "e-gate."

Your photo is sent to CBP's Traveler Verification Service (TVS), which compares the live photo against a small gallery of high-quality images of documents already provided to the government, like passport or visa photos. The image gallery is built from the APIS manifests that the airlines already sent to CBP.

This process biometrically verifies your identity. Once your image is matched, you can proceed.

Depending on the carrier's systems, you might not need to scan your boarding pass. If the TVS response is integrated into the airline's Departure Control System (DCS), you can board without scanning. Otherwise, you'll scan your boarding pass to board.

If the system doesn't produce a match, the gate agent will do a manual identity document check. The manual identity check is efficient and doesn't create undue delays. The gate agent will then scan your boarding pass.

You can opt out before going through the departure gate.

If you don't want your picture taken, you can request manual identity verification when you approach the departure gate. At present, both U.S. citizens and noncitizens can opt out when the airlines conduct this process.

You won't lose your place in line or have any negative consequences based on opting out. The gate agent will use your ID documents and boarding pass to verify your identity.

Read the regulation about when biometrics are needed for U.S. entry.

Encounter photos of U.S. citizens are deleted from CBP databases after use. Retention periods vary based on citizenship.

CBP uses TVS for all border crossing processes that use face recognition.

- All travelers are processed through TVS unless they opt out.
- No photos are permanently stored in the TVS cloud matching service.
  - **Photos of U.S citizens are deleted from CBP databases within 12 hours.** CBP only retains confirmation of the crossing and the associated biographic information.
  - **Photos of noncitizens are deleted from CBP databases within 14 days but kept in a DHS-wide system.** Photos of noncitizens aged 14-79 years who are required to provide biometrics are submitted to the appropriate system of record. CBP transmits these photos to a DHS-wide system called the Automated Biometric Identification System (IDENT), where they are kept for up to 75 years.

Redress

If you have feedback, questions, or a complaint about your experience with CBP's use of FR/FC technologies, get in touch.

- You can contact the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) if you've had difficulty with travel screenings, such as denied or delayed entry into the U.S., or repeated additional screening.
- If you believe DHS has violated your rights or someone else's rights, you can file a complaint with the DHS Office for Civil Rights and Civil Liberties.

These options are available to all travelers, regardless of citizenship status.

Testing

Face capture testing

Airport and airline partners own and operate the cameras used in the Biometric Exit process, not CBP.

CBP collaborates with carriers and airlines to ensure adherence to the latest system guidelines and is committed to providing guidance on use and best practices. Airports and airlines are responsible for testing their own cameras and face capture systems to make sure they follow these guidelines.

Image 1: Example of a Biometric Exit – Air setup at an airport departure gate.

Face recognition testing

CBP evaluated the technology before deployment and analyzed face recognition performance when the algorithm was updated in 2021. DHS did not conduct specific new testing for this report, but Biometric Exit uses the same underlying face matching system as other CBP FR/FC systems, including the two newly tested Global Entry use cases discussed in the following sections. The face matching system was tested as part of Global Entry, and we expect that performance in Biometric Exit is likely to be similar.

In the face recognition testing, we saw an overall face matching success rate of over 99% with a few cases of very small differences in measured face matching performance based on self-reported race, skin tone, and age, ranging from less than 1% to 2-3%. Face matching still performed well overall, and the lowest success rate for any demographic group was 97%. This round of testing was only designed to reliably detect differences of 5% or greater, so we can't say if smaller measured differences reflect true underlying differences in performance. We will continue to monitor these trends, refine our testing practices, and take action as appropriate.

We regularly review and update requirements as appropriate.

To mitigate the potential for demographic differences in either face capture or face recognition, CBP will regularly review and update their Biometric Exit business requirements for airline partners as appropriate. This may include camera hardware and face capture performance standards and requirements, which will be based on operational and scenario testing of similar systems.

CBP Global Entry - Touchless Portals

AI Use Case Inventory
Use Case Name: Semi-Supervised Traveler Identity Verification Services (Traveler Initiated)
Use Case ID: DHS-2413

Global Entry Touchless Portals enhance the Global Entry process.

Global Entry Touchless Portals are used by U.S. Customs and Border Protection (CBP) at airports of entry to verify identity and confirm membership. The Trusted Traveler Program (TTP) office began transitioning from Global Entry kiosks to portals in June 2023 and finished portal deployments to all major U.S. airports by the end of 2023.

Global Entry allows qualified, pre-approved travelers, who have been determined to be of low risk, to have facilitated clearance into the United States from abroad. Touchless Portals have face recognition functionality embedded, eliminate paper receipts, and provide a streamlined experience for the traveler.

You must apply, pay a non-refundable application fee, and be pre-approved for Global Entry membership. Applicants undergo a background check and an in-person interview as part of the enrollment process. Learn how to enroll in Global Entry.

Image 2: Example of a Biometric Entry – Air set up at an airport departure gate.

The Touchless Portal has two automated, self-adjusting cameras that capture your photograph.

When you walk up to the Global Entry Portal, the process begins automatically.

Once an acceptable photo is captured, the portal will begin the verification process. Your picture is compared to a photo gallery to verify your identity.

- If you receive the **"Processing Completed, Please Proceed"** message, you have completed the portal process and may continue to the exit.
- If you receive the **"Insert Travel Document"** message, scan your travel document to continue the process.
- After scanning your document, if you receive the **"Processing Completed, Please Proceed"** message, you have completed the process and can continue to the exit.
- If you receive the **"Processing Completed. See Officer for Assistance" message**, you have completed the process. An officer will assist you further when you proceed to the exit.

Global Entry is a voluntary, opt-in service.

Global Entry is a voluntary, opt-in service that requires biometrics. Global Entry members can always opt out of using Global Entry and go through standard CBP processing.

Encounter photos are deleted from CBP databases after use but kept in a DHS-wide system.

CBP uses an application called the Traveler Verification Service (TVS) for all border crossing processes that use face comparison.

No photos are permanently stored in the TVS cloud matching service.

- Photos of U.S citizens are deleted from CBP databases within 12 hours. CBP only retains confirmation of the crossing and the associated biographic information.
- CBP transmits encounter photos to a DHS-wide system called the Automated Biometric Identification System (IDENT), where they are kept for up to 75 years.

Redress

If you have feedback, questions, or a complaint about your experience with CBP's use of FR/FC technologies, get in touch.

If it's in the moment, ask to speak to the supervisory agent or officer on hand.

If it's after the fact, you can:

- Contact the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) if you've had difficulty with travel screenings, such as denied or delayed entry into the U.S., or repeated additional screening.
- If you believe DHS has violated your rights or someone else's rights, you can file a complaint with the DHS Office for Civil Rights and Civil Liberties.

These options are available to all travelers, regardless of citizenship status.

Testing

DHS Science and Technology (S&T) and CBP most recently tested the Global Entry Touchless Portals system in the summer of 2024. The evaluation process used both scenario testing and operational data. Scenario testing looks at how technology works in a simulated real-world environment. Operational data come from airports where the system is being used.

This technology is fully operational.

Two elements of the Global Entry Touchless Portals system were tested: face capture and face recognition.

Face capture testing results

- **On average, face capture technology for Global Entry Touchless Portals worked more than 99% of the time. There were no differences based on demographics.**

Face recognition testing results

- **In this test, face matching for Global Entry Touchless Portals worked 99% of the time.**
  - **There were small variations in performance based on skin tone and age that will be monitored going forward.**
    - In testing, face matching worked 98% of the time for those with darker skin tones. It worked >99% of the time for those with lighter skin tones. This shows a very small (1%) difference in performance based on skin tone.
    - In testing, face matching worked 97% of the time for those aged 18-30 years, compared to 99% or better for those over 31 years, showing a small difference in performance based on age.
    - This round of testing was only designed to reliably detect differences of 5% or greater, so we can't say if smaller measured differences reflect true underlying differences in performance. We will continue to monitor these trends, refine our testing practices, and take action as appropriate.
  - **There were no differences in performance based on gender.**

Transaction time

DHS also measures the transaction time, or "efficiency." This is a measure of how long it takes to move through the process and is important for operational planning. The transaction time was quick for all participants, at less than 10 seconds.

Table 1 – Summary performance metrics for CBP Global Entry: Touchless Portals

Metric	Measured
Face Capture Success Rate Percentage of interactions where system successfully captured face on first try	>99%
Face Matching Success Rate Percentage of interactions where the probe (encounter) photo successfully matched the gallery photo	99%
Transaction time Average time for volunteer to interact with system through entire interaction (includes system and volunteer errors)	9.1 seconds

Volunteer demographics

634 volunteers took part in testing. They provided demographic information, including:

- Self-reported age, gender, and race/ethnicity
- A measure of skin tone, which is taken by a calibrated instrument called a colorimeter. S&T uses the DSM III colorimeter from Cortex Technology.

Table 2 – Performance metrics by demographic group for CBP Global Entry Touchless Portals

Demographic Group Results are shown for demographic groups with over 90 samples.	**Face Capture Success Rate** *Measured*	**Face Matching Success Rate** *Measured*	**Transaction Time** *Measured*
Gender *Volunteers self-identified*			
Male	>99%	99%	8.9 seconds
Female	>99%	99%	9.3 seconds
Race *Volunteers self-identified*			
Black or African American	100%	99%	9.6 seconds
White	>99%	100%	8.5 seconds
Age Group (years) *Volunteers self-identified*			
18-30	100%	97%	9.1 seconds
31-45	100%	99%	8.5 seconds
46-60	>99%	99%	9.0 seconds
61+	99%	100%	9.8 seconds
Skin Tone *Measured by a calibrated instrument called a colorimeter. S&T uses the DSM III colorimeter from Cortex Technology.*			
T1 (Darker)	>99%	98%	9.5 seconds
T2	>99%	>99%	9.4 seconds
T3 (Lighter)	100%	>99%	8.4 seconds

Testing Process

Scenario Testing

We tested the Global Entry Touchless Portals system at the Maryland Test Facility (MdTF). The lab was set up to resemble a Touchless Portal at an airport.

Volunteers went through the Global Entry Touchless Portals system. They had their face detected and a photo taken. The photo was then matched to a gallery of images using the CBP TVS system.

Table 3 – Scenario testing process for Global Entry Touchless Portals

Test process
1. The volunteer approaches the Global Entry Touchless Portal.
2. The volunteer follows on-screen instructions.
3. The system takes a photo of the volunteer and issues a result.

Table 4 – Technology summary for Global Entry Touchless Portals

Technology title	Technology name/type
System Build (Face Capture Software)	As delivered to S&T in September 2024
System Type	Auto Facial Capture with 1:N (Gallery) Face Matching
Face Capture Device	IDS uEye Camera
Face Detection Algorithm	Idemia mFace
Face Recognition Algorithm	NEO NeoFaceV Version 3.3.0.0200 64bit Traveler Verification Service (TVS) Identify (Air Arrival Port Galleries) from Customs and Border Protection

Image 3: A row of Global Entry Touchless Portals set up at an airport.

CBP Global Entry - Mobile application

AI Use Case Inventory
Use Case Name: Semi-Supervised Traveler Identity Verification Services (Traveler Initiated)
Use Case ID: DHS-2413

The Global Entry Mobile Application gives Global Entry members an alternative processing option using an application.

The Global Entry Mobile Application (app) streamlines the entry process into the United States by reducing passport inspection and overall waiting time.

This free app was launched by U.S. Customs and Border Protection (CBP) in 2023. It can be downloaded from the Google Play store and the Apple App store. It can only be used by members of the Global Entry program.

You must apply, pay a non-refundable application fee, and be pre-approved for Global Entry membership. Applicants undergo a background check and an in-person interview as part of the enrollment process. Learn how to enroll in Global Entry.

You can use the Global Entry Mobile App at international airports.

To participate, download the app on your smartphone or other mobile device and open it when you land. Enter your airport and terminal information. You'll be asked to capture a picture of your face using the app. This is called an "encounter photo."

Your picture is compared to a photo gallery to verify your identity.

This allows CBP to confirm your identity and your membership status. If your membership is confirmed, you can proceed without using a Global Entry Portal.

You will need to present your digital receipt to a CBP officer to proceed.

Global Entry members aren't required to use the app.

If you have Global Entry, you can still use a Global Entry Portal instead of the mobile app.

Global Entry is a voluntary, opt-in service that requires biometrics.

Encounter photos are deleted from CBP databases after use but kept in a DHS-wide system.

CBP uses an application called the Traveler Verification Service (TVS) for all border crossing processes that use face comparison.

No photos are permanently stored in the TVS cloud matching service.

- Photos of U.S citizens are deleted from CBP databases within 12 hours. CBP only retains confirmation of the crossing and the associated biographic information.
- CBP transmits encounter photos to a DHS-wide system called the Automated Biometric Identification System (IDENT), where they are kept for up to 75 years.

Redress

If you have feedback, questions, or a complaint about your experience with CBP's use of FR/FC technologies, get in touch.

If it's in the moment, ask to speak to the supervisory agent or officer on hand.

If it's after the fact, you can.

- Contact the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) if you've had difficulty with travel screenings, such as denied or delayed entry into the U.S., or repeated additional screening.
- If you believe DHS has violated your rights or someone else's rights, you can file a complaint with the DHS Office for Civil Rights and Civil Liberties.

These options are available to all travelers, regardless of citizenship status.

Testing Results

DHS Science and Technology (S&T) and CBP most recently tested the Global Entry Mobile App system in the summer of 2024. The evaluation process used both scenario testing and operational data. Scenario testing looks at how technology works in a simulated real-world environment. Operational data are real figures that come from airports where the system is being used.

This technology is fully operational.

Two elements of the Global Entry Mobile App system were tested: face capture and face recognition.

Face capture testing results

- **The face capture technology for the Global Entry Mobile App system worked more than 99% of the time across demographics.**

Face recognition testing results

- **On average, face matching for the Global Entry Mobile App worked 99% of the time.**
    - **There were small variations in performance based on some demographic factors that will be monitored going forward.**
        - In testing, face matching worked 98% of the time for those who identify as Black or African American and for those with darker skin tones. It worked >99% of the time for those who identify as White and those who have lighter skin tones. This shows a very small (1%) difference in performance based on race and skin tone.
        - In testing, face matching worked 98% of the time for those aged 18-30 years, compared to about 99% for those over 31 years, showing a very small (1%) difference in performance based on age.

- This round of testing was only designed to reliably detect differences of 5% or greater, so we can't say if smaller measured differences reflect true underlying differences in performance. We will continue to monitor these trends, refine our testing practices, and take action as appropriate.

- **There were no differences in performance based on gender.**

Transaction time

DHS also measures the transaction time, or "efficiency." This is a measure of how long it takes to complete the process and is helpful for operational planning. The transaction time for the Global Entry Mobile App was about 21 seconds on average. There was no difference in the transaction time based on race or skin tone. It took a few seconds longer than average, about 25 seconds, for people aged 61 years and over.

Table 5 – Summary performance metrics for the Global Entry Mobile App

Metric	Measured
Face Capture Success Rate Percentage of interactions where system successfully captured face on first try	>99%
Face Matching Success Rate Percentage of interactions where the probe (encounter) photo successfully matched the gallery photo	99%
Transaction time Average time for volunteer to interact with system through entire interaction (includes system and volunteer errors)	20.5 seconds

Volunteer demographics

634 volunteers took part in testing. They provided demographic information, including:

- Self-reported age, gender, and race/ethnicity
- A measure of skin tone, which is taken by a calibrated instrument called a colorimeter. S&T uses the DSM III colorimeter from Cortex Technology.

Table 6 – Performance metrics by demographic group for the Global Entry Mobile App

Demographic Group Results are shown for demographic groups with over 90 samples.	**Face Capture Success Rate** *Measured*	**Face Matching Success Rate** *Measured*	**Transaction Time** *Measured*
Gender *Volunteers self-identified*			
Male	99%	>99%	20.1 seconds
Female	>99%	99%	20.8 seconds
Race *Volunteers self-identified*			
Black or African American	>99%	98%	20.6 seconds
White	>99%	>99%	21.2 seconds
Age Group (years) *Volunteers self-identified*			
18-30	100%	98%	17.6 seconds
31-45	>99%	99%	17.9 seconds
46-60	>99%	>99%	20.7 seconds
61+	99%	99%	24.9 seconds
Skin Tone *Measured by a calibrated instrument called a colorimeter. S&T uses the DSM III colorimeter from Cortex Technology.*			
T1 (Darker)	99%	98%	20.5 seconds
T2	>99%	99%	20.1 seconds
T3 (Lighter)	>99%	>99%	21.1 seconds

Testing Process

Scenario testing

We tested the Global Entry Mobile App at the Maryland Test Facility (MdTF). The lab was set up to resemble a CBP Port of Entry.

With minimal assistance from staff, volunteers operated the Global Entry Mobile App on a smartphone provided by DHS S&T. Using the app, they took a photo of their face, which was then matched to a gallery of images using the TVS.

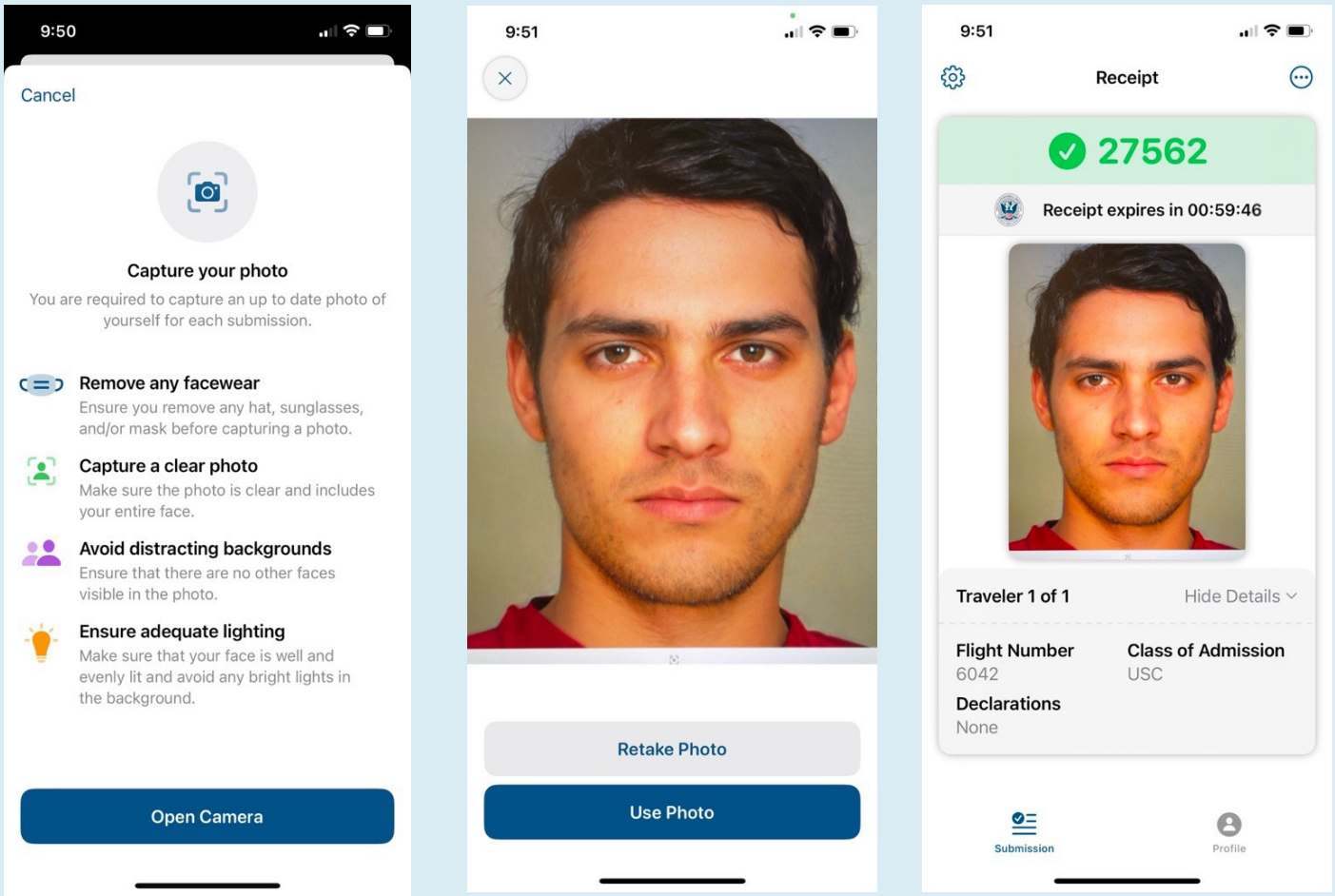
Table 7 – Scenario testing process for the Global Entry Mobile App

Test process
1. The volunteer is provided a smartphone running the Global Entry Mobile App.
2. The volunteer follows on-screen instructions.
3. The volunteer self-captures their photo using the app.

Table 8 – Technology summary for the Global Entry Mobile App

Technology title	Technology name/type
System Build (Face Capture Software)	As delivered to S&T in September 2024, Global Entry Mobile Application Version 1.4.0
System Type	Manual Facial Capture with 1:N (Gallery) Face Matching
Face Capture Device	Global Entry Mobile App on: Apple iPhone 14; Samsung Galaxy S22; Google Pixel 7
Face Recognition Algorithm	NEC NeoFaceV Version 3.3.0.0200 64bit Traveler Verification Service (TVS) Identify (Air Arrival Port Galleries) from Customs and Border Protection

Image 4-6: Screenshots from the Global Entry Mobile App



CBP Simplified Arrival - Air Entry

AI Use Case Inventory
Use Case Name: Supervised Traveler Identity Verification Services (Officer Initiated)
Use Case ID: DHS-2412

Simplified Arrival makes the process to enter the U.S. more secure and efficient.

Customs and Border Protection (CBP) uses face recognition technology at all international airports in the United States. The face recognition process takes only a few seconds to complete.

Simplified Arrival uses a picture of your face to verify your identity.

A CBP officer manually takes the photo.

The photo is compared to a gallery of high-quality images that you and other travelers that day have already provided to the government, such as passport or visa photos.

If you are matched, your associated biographic information is run through CBP systems. The systems search for lookouts, warrants and other required actions. Once any records or lookouts are addressed, the CBP officer will either authorize you to exit the primary inspection point or refer you for further inspection.

If you aren't matched, the officer will scan your passport or other document and the system will try to match your photo against the photo on identity document. If this still doesn't match, CBP will take other steps to verify your identity before admitting you into the country.

U.S. citizens and some noncitizens can opt out of having a photo taken.

If you are a U.S. citizen and don't want to have your photo taken, you may tell the CBP officer as you approach the primary inspection point. There are no negative consequences based on opting out.

You will need to present valid travel documents for inspection.

Most noncitizens must provide biometrics, such as fingerprints, when entering the U.S. Some noncitizens are exempt. Read the regulation about when biometrics are needed for U.S. entry.

Photo retention periods vary based on citizenship.

CBP uses an application called the Traveler Verification Service (TVS) for all border crossing processes that use face recognition.

- U.S. citizens and individuals not required to provide biometrics may opt out.

- Your photo will be taken unless you opt out.
- No photos are permanently stored in the TVS cloud matching service.
  - **Photos of U.S citizens are deleted from CBP databases within 12 hours.** CBP only retains confirmation of the crossing and the associated biographic information.
  - **Photos of noncitizens are deleted from CBP databases within 14 days but kept in a DHS-wide system.** Photos of noncitizens aged 14-79 years who must provide biometrics are submitted to the appropriate system of record. CBP transmits these photos to a DHS-wide system called the Automated Biometric Identification System (IDENT), where they are kept for up to 75 years.

Redress

If you have feedback, questions, or a complaint about your experience with CBP's use of FR/FC technologies, get in touch.

If it's in the moment, ask to speak to the supervisory agent or officer on hand.

If it's after the fact, you can:

- Contact the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) if you've had difficulty with travel screenings, such as denied or delayed entry into the U.S., or repeated additional screening.
- If you believe DHS has violated your rights or someone else's rights, you can file a complaint with the DHS Office for Civil Rights and Civil Liberties.

These options are available to all travelers, regardless of citizenship status.

Analysis Results

The CBP Simplified Arrival – Air Entry system involves face capture, face recognition, and CBP system queries. In 2024, DHS Science and Technology (S&T) evaluated aspects of the face recognition part of the Simplified Arrival – Air Entry system. Other aspects of system performance were examined by DHS S&T using CBP provided operational reporting statistics.

Face capture data analysis

The standard web camera used by CBP officers during the Simplified Arrival process doesn't use an automated system to capture photos. TThe officer manually adjusts the camera based on operational conditions to take a photo. The picture is sent to the face recognition service to be compared with known document photos.

Simplified Arrival doesn't use automated software to detect and take a face photo, so no automated software is available to test or examine demographic differentials.

Face recognition performance analysis

Due to limited resources and the manual face capture process, we didn't conduct a full scenario test for the Simplified Arrival – Air Entry system.

However, we reviewed operational reporting statistics from CBP spanning 15 days of active usage. These data show an overall face matching success rate over 99%, which includes both steps of the face recognition process.

These operational reporting statistics didn't include demographic information. However, the underlying face recognition system is the same one used for Global Entry, and face recognition performance in this use case is likely similar. In that testing, we saw a few cases of very small differences in measured face matching performance based on self-reported race, skin tone, and age, ranging from less than 1% to 2-3%. Face matching still performed well overall, and the lowest success rate for any demographic group was 97%. This round of testing was only designed to reliably detect differences of 5% or greater, so we can't say if smaller measured differences reflect true underlying differences in performance. We will continue to monitor these trends, refine our testing practices, and take action as appropriate.

CBP and S&T will continue to work together to analyze reporting from this use case and conduct additional testing as necessary to provide additional validation.

Table 9 – Technology summary for Simplified Arrival: Air Entry

Technology title	Technology name/type
System Type	Manual Facial Capture with 1:N (Gallery) Face Matching
Face Capture Device	Logitech C920 Webcam, Android, iPhone, iPad cameras
Face Recognition Algorithm	NEC NeoFaceV Version 3.3.0.0200 64bit Traveler Verification Service (TVS) Identify (Air Arrival Port Galleries) from Customs and Border Protection

Image 7: An example of Simplified Arrival - Air Entry process

CBP Simplified Arrival – Land Pedestrian Entry

AI Use Case Inventory
Use Case Name: Supervised Traveler Identity Verification Services (Officer Initiated)
Use Case ID: DHS-2412

Simplified Arrival makes the process to enter the U.S. more efficient.

Customs and Border Protection (CBP) uses face recognition technology at all pedestrian lanes at Southwest Border and Northern Border ports of entry. The face recognition process takes only a few seconds to complete.

Simplified Arrival uses a picture of your face to verify your identity, instead of requiring a physical document check.

When you arrive at a U.S. land border port as a pedestrian, a CBP officer will take a photo at an inspection point for identity verification and scan the document you provide, such as your passport.

If your identity document has an electronic photo associated with it, your photo will be compared to the photo on the document presented. CBP uses the Traveler Verification Service (TVS) for face recognition. If you are matched, your associated biographic information is run through CBP systems. The systems search for lookouts, warrants, and other required actions. Once any records or lookouts are addressed, the CBP officer will either authorize you to exit the primary inspection point or refer you for further inspection.

If you are not matched, the officer will do a manual identity check and CBP will take other steps to verify your identity before admitting you into the country.

U.S. citizens and some noncitizens can opt out.

If you are a U.S. citizen and do not want to have your photo taken, you may tell the CBP officer as you approach. You will not lose your place in line or have any negative consequences.

You will need to present a valid travel document for inspection. Most noncitizens must provide biometrics, like a picture, when entering the U.S. Some noncitizens are exempt. Read the regulation about when biometrics are needed for U.S. entry.

Photo retention periods vary based on citizenship.

CBP uses the Traveler Verification Service (TVS) for all border crossing processes that use face recognition.

- U.S. citizens and those not required to provide biometrics may opt out.
- Your photo will be taken unless you opt out.

- No photos are permanently stored in the TVS cloud matching service.
  - **Photos of U.S citizens are deleted from CBP databases within 12 hours.** CBP only retains confirmation of the crossing and the associated biographic information.
  - **Photos of noncitizens are deleted from CBP databases within 14 days but kept in a DHS-wide system.** Photos of noncitizens aged 14-79 years who must provide biometrics are submitted to the appropriate system of record. CBP transmits these photos to a DHS-wide system called the Automated Biometric Identification System (IDENT), where they are kept for up to 75 years.

Redress

If you have feedback, questions, or a complaint about your experience with CBP's use of FR/FC technologies, get in touch.

If it's in the moment, ask to speak to the supervisory agent or officer on hand.

If it's after the fact, you can:

- Contact the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) if you've had difficulty with travel screenings, such as denied or delayed entry into the U.S., or repeated additional screening.

Image 8: Traveler using the Simplified Arrival process at land port of entry.

- If you believe DHS has violated your rights or someone else's rights, you can file a complaint with the DHS Office for Civil Rights and Civil Liberties.

These options are available to all travelers, regardless of citizenship status.

Analysis Results

There are two elements to the Biometric Exit system: face capture and face recognition. In 2024, DHS S&T evaluated aspects of the face recognition part of the Simplified Arrival – Land Pedestrian Entry system. Other aspects of system performance were examined by DHS using CBP provided operational reporting statistics.

Face capture testing

The standard web camera used by CBP officers during the Simplified Arrival process doesn't use an automated system to capture photos. The officer manually operates the camera based on operational conditions to take a photo. The picture is sent to the face recognition system to be compared with known document photos.

Simplified Arrival doesn't use automated software to detect and take a face photo, so no automated software is available to test or examine demographic differentials.

Face recognition testing

Due to limited resources and the manual face capture process, we didn't conduct a full scenario test for the Simplified Arrival – Air Entry system.

However, we reviewed operational reporting statistics from CBP spanning 15 days of active usage. These data show an overall face matching success rate over 98%, which includes both steps of the face recognition process.

Image 9: Traveler using the Simplified Arrival process at land port of entry.

These operational reporting statistics didn't include demographic information. However, the underlying face recognition system is the same one used for Global Entry, and face recognition performance in this use case is likely similar. In that testing, we saw a few cases of very small differences in measured face matching performance based on self-reported race, skin tone, and age, ranging from less than 1% to 2-3%. Face matching still performed well overall, and the lowest success rate for any demographic group was 97%. This round of testing was only designed to reliably detect differences of 5% or greater, so we can't say if smaller measured differences reflect true underlying differences in performance. We will continue to monitor these trends, refine our testing practices, and take action as appropriate.

CBP and S&T will continue to work together to analyze reporting from this use case and conduct additional testing as necessary to provide additional validation.

Table 10 – Technology summary for Simplified Arrival – Land Pedestrian Entry

Technology title	Technology name/type
System Type	Manual Facial Capture with 1:1 Face Matching
Face Capture Device	Logitech C920 Webcam, Android, iPhone, iPad cameras
Face Recognition Algorithm	NEC NeoFaceV Version 3.3.0.0200 64bit Traveler Verification Service (TVS) Verify 1:1

Homeland Security Investigations (HSI)

Homeland Security Investigations (HSI) uses AI for facial recognition in certain investigations. Facial recognition helps HSI identify and rescue victims of child sexual exploitation (CSE). The use of facial recognition at HSI has led to arrests of suspected CSE perpetrators and the rescue of victims in previously cold cases.

Homeland Security Investigations (HSI)

AI Use Case Inventory
Use Case Name: Face Recognition for Investigations of Child Sexual Exploitation and Abuse
Use Case ID: DHS-362

Face Recognition for Investigations of Child Sexual Exploitation and Abuse

The Homeland Security Investigations (HSI) Child Exploitation Investigations Unit (CEIU) uses government databases and commercial tools, including Clearview AI, to help identify victims and offenders with child sexual abuse material.

HSI's use of face recognition technology has helped identify victims of child sexual exploitation and resulted in the rescue of children who may not otherwise have been rescued using other investigative means. It has likely prevented other children from being victimized through the arrests of offenders who could otherwise go undetected by law enforcement.

Clearview AI is not currently used for any other types of investigations or for any other purposes anywhere at DHS. Expansion of this use case into other types of investigations would require additional review and disclosure per policy.

No law enforcement action is taken based on a lead alone.

Trained, licensed HSI personnel use face recognition to generate leads to identify victims and offenders. Every lead is investigated before law enforcement action is taken.

HSI personnel exhaust all other investigative techniques before using face recognition.

HSI personnel conduct investigations of newly discovered child sexual abuse material. In this material, the subject and victim's identities are not known to law enforcement.

When HSI personnel begin their investigation into any child sexual abuse material, they must try to identify the people through other investigative techniques and methods before using face recognition technology. They first research any biographical and non-biometric information from the material and document their work. It's only after exhausting all these investigative techniques that the HSI personnel may use face recognition for investigations of child sexual exploitation and abuse.

HSI personnel choose an image that increases accuracy.

When they've exhausted all other investigative techniques, HSI personnel will select an image, called the "probe image," to upload to face recognition tools used for investigations of child sexual exploitation and abuse.

They look for an image that has:

- The highest image quality possible;
- The fewest obstructions to the subject's face; and
- The most similarity to a standard ID picture in terms of angle, lighting, distance, and expression

All of this increases the chances of the algorithm returning other images depicting the same individual.

HSI personnel are provided a list of potential matches.

After the search, the technology returns images from publicly available websites that the algorithm finds similar to the probe image. It can return images from news articles, social media, online mugshots, and other websites. This type of face recognition technology performs a type of identification, or "one-to-many" matching, to return face images that are the most similar in appearance. This increases the chance of returning a picture of the same individual who appears in the probe image. It also means that there are likely to be pictures returned regardless of whether the person shown in the probe image is present among the publicly available photos.

HSI personnel vet the list of returned images.

Once they have the candidate list of potential matches, HSI personnel must investigate the leads and document their use of the face recognition technology. HSI personnel use a process called "vetting." They compare the information they were provided from the face recognition tool to other information obtained using investigative techniques to see if any of the potential matches are supported by corroborating evidence.

Other evidence that helps to validate or eliminate a candidate include things like biographic information, telephone numbers, current and previous addresses, vehicles, telephone numbers, criminal history, skin markings like tattoos, and body coverings like jewelry and clothing.

If a lead from the face recognition tool is successfully "vetted," HSI personnel work on the lead for further investigation.

Any information that isn't vetted is not used for leads or entered into a Report of Investigation. It also doesn't get recorded in HSI's Investigative Case Management system.

If a lead is created from a vetted image and then combined with other evidence to create probable cause, HSI personnel may have to testify to their use of face recognition in court. They would also explain how they initially identified the subject in affidavits for warrants. The court reviews the affidavit before issuing a warrant. If a case goes to trial, information about HSI's use of face recognition is discoverable pursuant to normal judicial procedures.

There are safeguards in place to protect privacy, civil rights, and civil liberties.

Face recognition is only used by trained staff.

HSI personnel who investigate child sexual exploitation and abuse are trained on how to use face recognition technology. They learn how to examine newly discovered child sexual abuse material in which law enforcement is unaware of the subject's and victim's identities.

The CEIU manages the distribution of software licenses within HSI. They make sure HSI personnel who use face recognition tools follow all policy standards and fair information practice principles in the Privacy Impact Assessment.

Supervisors at HSI regularly review case files and agent submissions to face recognition tools to verify that all privacy-related data handling safeguards are being followed and that searches are conducted in accordance with policy.

HSI only supplies the minimum information required to run the search.

The minimum information required is usually the HSI personnel's information, and the "probe image" they selected for the search. The image uploaded by the agent stays private. That image doesn't enter the service providers' galleries of images.

DHS Science and Technology Directorate analyzed results from NIST and found that the system is likely to provide value to HSI investigators as configured.

On an ongoing basis, HSI's Operational Systems Development and Management Unit (OSDM) uses resources like the National Institute for Standards and Technology's (NIST) Face Recognition Technology Evaluation to evaluate performance of face recognition tools used for investigations of child sexual exploitation and abuse.

OSDM also conducts regular self-audits as non-scientific tests to check how accurate each service is.

In 2024, the DHS Science and Technology Directorate (S&T) used independent testing results from NIST to estimate and model Clearview AI's performance based on international standards.. The current algorithm in use was submitted to the NIST Face Recognition Technology Evaluation under the moniker "clearviewai_002."

S&T analysis concluded that the system is likely providing value as configured.

S&T analysis and modeling focused on two key measures to conclude that one face recognition tool used by HSI for investigations of child sexual exploitation and abuse is likely providing value.

Table 11: Performance metrics for HSI Face recognition for Investigations of Child Sexual Exploitation and Abuse

Performance Metric	Result
False Negative Rate (FNIR) FNIR is how often an individual in the gallery is searched but the system doesn't return them in the candidate list. False negatives are the error of primary concern in the context of HSI use of face recognition technology for child sexual exploitation and abuse investigations. When this error occurs, HSI personnel are unable to use the software to develop a lead on a missing person or person of interest, even though that person was in the tool's holdings. The low false negative rate found in testing leads us to conclude that using face recognition software has operational utility for HSI and is likely providing worthwhile results to HSI investigators as configured.	NIST's Face Recognition Technology Evaluation (FRTE) Part 2 evaluation found low false negative rates ranging from 0.37% to 6.6% for representative galleries. A low false negative rate means that the software is unlikely to miss a match between the probe photo and an image of the same individual in the gallery.
False Positive Identification Rate (FPIR) FPIR is how often an individual not in the gallery is searched, but the system still returns a list of potential matches. When HSI personnel use Face recognition software, every lead is investigated and vetted, and no law enforcement action is ever taken based on the matches alone. HSI personnel are trained to know that the lists returned by the software don't mean that the subject of the search probe image is actually one of the candidates in the list. HSI personnel are also trained to use extensive investigative techniques outside of facial similarity in the vetting process. This is very important because academic literature shows that untrained people don't perform well at picking candidates from algorithm-generated lists based on facial features.	Using data provided by NIST for the performance of the clearview_002 algorithm, S&T estimated the FPIR of the system to be between 2.8% and 16.8%, depending on the threshold, when searching the largest gallery size tested by NIST (12 million enrolled individuals.) However, FPIR scales with gallery size. When searching galleries of 50 billion samples, S&T models show the false positive rate at either threshold is likely 100%. Reducing this error rate against a gallery of 50B samples would require the use of extraordinarily high matching thresholds that would likely diminish the utility of the HSI system. A face identification system with a 100% false positive identification rate means that any search, of any individual, will return a list of potential matches. The list of potential matches will be very similar in facial structure and demographics to the image that was searched, even though it's a different person.

This face recognition tool used by HSI for investigations of child sexual exploitation and abuse can't be evaluated using traditional scenario testing or operational testing approaches.

There are several reasons for this:

1. This face recognition tool for investigations of child sexual exploitation and abuse uses a gallery of more than 50 billion images. One of the factors that affects the performance of face recognition systems is the number of individuals and images in the gallery. To test it using operational or scenario testing, researchers would need to access 50 billion images approved for testing, which isn't feasible. The NIST FRTE evaluation is based on an evaluation using a gallery of 12 million mug shot images.
2. In operations, this face recognition tool used for investigations of child sexual exploitation and abuse uses indexing to efficiently search the 50 billion image gallery, however the software evaluated by NIST did not use indexing. The software evaluated by NIST did not use indexing, which means it compared each probe photo to each photo in the NIST gallery. This is time and resource intensive in an operational system with 50 billion face photos, so the software uses indexing to search the gallery more efficiently. This may affect estimates of error rates.
3. HSI personnel's skill level affects how the system performs. Trained staff review every candidate list that the face recognition tool produces. Their investigative ability affects how well the overall system works.
4. The demographics (especially age), sources, and quality of probe images used by HSI vary dramatically from traditional datasets used for biometric evaluation protocols. These variations impact error rates.

This is why S&T relied on NIST testing and modeling to analyze this face recognition tool used by HSI for investigations of child sexual exploitation and abuse.

Transportation Security Administration (TSA)

Identity verification is a key enabler of TSA's risk-based aviation security model. To securely facilitate commercial air travel, TSA must quickly and accurately verify the identity of almost 3 million travelers per day at over 400 airports nationwide.

Identity verification makes sure that each traveler entering a security checkpoint is the same ticketed passenger who was vetted by Secure Flight. Secure Flight pre-screens passengers' information provided by airlines against U.S. Government lists of high- and low-risk passengers and determines the appropriate amount of physical screening needed for each passenger.

The challenges of evolving security threats, including high-quality fraudulent IDs and imposter attacks, combined with rising air travel volumes, resource constraints, and recent advances in face recognition technology led TSA to begin automating the identity verification process to enhance security effectiveness and operational efficiency.

Before any automation, identity verification was a manual process. Transportation Security Officers (TSOs) would inspect the traveler's identity document (ID) and then scan their boarding pass. Now, some elements are automated using FR/FC technology.

Overall, biometrics testing shows that FR/FC technology produces better identification results than the manual process. Compared with human-based recognition, face recognition technology is less likely to result in mistakes, reducing the potential for bad actors to gain access to the secure areas of airports.

TSA Credential Authentication Technology with Camera System (CAT-2)

AI Use Case Inventory
Use Case Name: Credential Authentication Technology with Camera System (CAT-2) and AutoCAT (CAT-2 in an E-Gate Form Factor)
Use Case ID: DHS-327

TSA's CAT-2 system can verify your identity without you having to show your physical or digital ID.

Identity verification is a key enabler of TSA's risk-based aviation security model.

One type of technology used to verify identity is called Credential Authentication Technology (CAT). Since June 2023, TSA has been deploying the second-generation CAT system (CAT-2), which helps Transportation Security Officers (TSOs) to confirm your identity and boarding pass information.

The CAT-2 system has a passenger-facing camera and digital ID reader. It takes your photo at the security checkpoint and compares it to your physical or digital ID photo. CAT-2 displays your prescreening status from Secure Flight to the TSO. They verify that you have been properly vetted and can move through the appropriate level of checkpoint security screening.

The CAT-2 system uses a type of face matching called "one-to-one," which is used in identity verification to confirm a photo matches a different photo of the same person.

Participation is voluntary.

You can opt out of having your photo taken by telling the TSA officer.

Interacting with TSA's face recognition technology (FRT) is voluntary. You still have to submit and scan your credentials to be authenticated, but you don't have to have your picture taken.

If you do not want your photo to be taken, tell the TSO before scanning your credentials. You won't lose your place in line, and you won't have to go through additional screening procedures or experience other negative consequences. The TSO will turn off the CAT-2 camera. Your ID will be scanned to confirm its authenticity, and the TSO will manually match your face with your ID photo. Travelers under age 18 are not photographed. Minors don't have to provide identity documents for verification.

If you choose to participate, the CAT-2 takes your picture and compares it to the picture on your photo ID.

When you get to the airport security checkpoint, you'll see signage reminding you that you can opt out of having your picture taken. TSA displays opt-out language on signage near all CAT-2 systems, on the CAT-2's passenger-facing screen, and on kiosk stickers.

If you choose to participate, you will step up to the CAT-2 system and insert your ID into the CAT-2's ID scanner to authenticate your ID (or place your passport on top of the scanner). At some airports, the TSO will ask for your ID to scan it themselves. Inserting your ID also turns on the CAT-2 camera, which takes your photo, and compares it to your photo on the ID. The camera immediately turns off until the next ID is inserted.

Your photo is deleted after use.

Your live photo and the image captured from your photo ID are never stored or transmitted to any other system except as described in the Testing section below. Everything stays local to the specific CAT-2 machine that you interacted with. Further, both the live photo and ID photo are transformed into irreversible templates when being compared to each other.[1]

Both images are overwritten when the next passenger's photo is taken, or when the TSO logs off the machine, whichever comes first.

There is only one exception to the immediate deletion of the photo, as described in the Testing Section below. TSA periodically collects biometric data for testing and evaluation. This ensures that TSA's algorithms provide accurate and reliable results.

If there are matching or technical issues, the "human in the loop" is there to adjudicate.

If the live photo taken at the check point doesn't match the image from your photo ID, the TSO will use the standard, manual passenger identity verification procedures or escalate to their supervisor based on Standard Operating Procedures (SOP).

Redress

If you have feedback, questions, or a complaint about your experience with TSA's use of FR/FC technologies, get in touch.

If it's in the moment, ask to speak to the supervisory agent or officer on hand.

If it's after the fact, you can:

- Contact Customer Service | Transportation Security Administration (tsa.gov) to request information, submit complaints or compliments, and let TSA know about security issues or civil rights violations.
- File a complaint with the DHS Office for Civil Rights and Civil Liberties if you believe DHS has violated your rights or someone else's rights.

These options are available to all travelers, regardless of citizenship status.

Testing Results

DHS Science and Technology (S&T) and TSA most recently tested the TSA CAT-2 system in 2023 and 2024. The evaluation process used a very large scenario test with more than 1,600 volunteers.

This technology is fully operational.

There are two elements to the CAT-2 system that were tested: face capture and face recognition.

Face capture

- The face capture technology for TSA CAT-2 worked >99% of the time. For CAT-2, this didn't vary based on age, gender, race, or skin tone.

Face recognition

- The face recognition technology for TSA CAT-2 worked >99% of the time. For CAT-2, this didn't vary based on age, gender, race, or skin tone.

Transaction time

DHS also measures the transaction time, or "efficiency." This is how long it takes to move through the whole process and is important for operational planning. On average, the TSA CAT-2 identity verification process took 23 seconds per person. It took well under 30 seconds for all demographic groups, and all demographic groups were within a few seconds of the average.

Table 12 – Performance metrics for CAT-2

Metric	Measured
Face Capture Success Rate Percentage of interactions where system successfully captured face on first try	>99%
Face Matching Success Rate Percentage of interactions where probe photo successfully matched ID photo	>99%
Transaction time Average time for volunteer to interact with system through entire interaction (includes system and volunteer errors)	22.8 seconds

[1] A biometric template is a digital representation of a biometric trait of a person, generated from a biometric image (picture) and processed by an algorithm. The template is usually represented as a sequence of characters and numbers. For CAT-2, templates cannot be reverse-engineered to recreate a biometric image. This means that once the picture is processed and made into a template, you can't turn it back into a picture. The templates generated for CAT-2 are proprietary to a specific vendor's algorithm and cannot be used with other vendor's algorithms.

Volunteer demographics

1653 volunteers participated in the test. The volunteers provided demographic information, including:

1. Self-identified age, gender, and race/ethnicity
2. A measure of skin tone, which is taken by a calibrated instrument called a colorimeter. S&T uses the DSM III colorimeter from Cortex Technology.

Table 13 – Performance metrics by demographic group for CAT-2

Demographic Group *Results are shown for demographic groups with over 90 samples.*	**Face Capture Success Rate** *Measured*	**Face Matching Success Rate** *Measured*	**Transaction Time** *Measured*
Gender *Volunteers self-identified*			
Male	>99%	100%	22.8 seconds
Female	>99%	>99%	22.8 seconds
Race *Volunteers self-identified*			
Black or African American	>99%	98%	20.6 seconds
White	>99%	>99%	21.2 seconds
Asian	>99%	>99%	22.3 seconds
Hispanic or Latino	>99%	100%	23.2 seconds
Age Group (years) *Volunteers self-identified*			
18-30	>99%	100%	19.5 seconds
31-45	100%	>99%	20.8 seconds
46-60	>99%	100%	23.0 seconds
61+	99%	100%	27.8 seconds
Skin Tone *Measured by a calibrated instrument called a colorimeter.* *S&T uses the DSM III colorimeter from Cortex Technology.*			
T1 (Darker)	>99%	>99%	22.9 seconds
T2	100%	>99%	22.7 seconds
T3 (Lighter)	>99%	>99%	22.7 seconds

Scenario testing

We tested the TSA CAT-2 at the Maryland Test Facility (MdTF) and in San Diego, California. The lab was set up to resemble a real TSA security checkpoint. An operator played the part of the Transportation Security Officer (TSO) who would staff the checkpoint at an airport.

Table 14 – Scenario testing process for CAT-2

Test process
1. The volunteer approaches the CAT-2 system and inserts their physical driver's license into the document scanner.
2. The CAT-2 system camera takes a live photo (called the "probe face image") of the volunteer.
3. The CAT-2 system scans the image from the driver's license. This is called the "reference face image."
4. The system compares the live photo ("probe face image") to the driver's license photo ("reference face image") and looks for a match.

Image 8: TSA CAT-2 kiosk at an airport

Table 15 – Technology summary for CAT-2

Technology title	Technology name/type
System Build (Face Capture Software)	As delivered to S&T in 2024
System Type	Auto and Manual Facial Capture with 1:1 Face Matching
Face Capture Device	Idemia CAT-2 Camera (3.2 MP)
Document Scanner	E-Seek M500
Face Recognition Algorithm	Idemia MorphoLite V3.1.1

TSA PreCheck®: Touchless Identity Solution

AI Use Case Inventory
Use Case Name: PreCheck Touchless Identity Solution (TIS)
Use Case ID: DHS-345

When you use TSA PreCheck: Touchless Identity Solution, you verify your identity without having to show your physical or digital ID.

The Transportation Security Administration's (TSA) PreCheck®: Touchless Identity Solution (TIS) lets DHS Trusted Travelers verify their identity without having to present their ID at certain security checkpoint locations.

The TSA PreCheck: TIS is a "proof of concept" that is being assessed at specific airports with select airline partners.

The program is available to any DHS Trusted Traveler with a Known Traveler Number (KTN) and passport who is flying with a partner airline. This includes members of TSA PreCheck and U.S. Customs and Border Protection's (CBP) Global Entry program.

Opt in through your airline's mobile app.

Participating airlines at select airports notify you of the TSA PreCheck: TIS option when you check in using your airline's mobile app. Opting in means volunteering to participate in the use of face recognition technology. Your mobile boarding pass will be marked with a "consent indicator" to show that you have chosen to participate.

If you don't choose to opt in, your mobile boarding pass will not be marked, and you will not be eligible to participate in TSA PreCheck: TIS.

Participation in TSA PreCheck: TIS is voluntary.

Even if you've opted in with your airline, you can still change your mind and opt out of having your photo taken at the TSA checkpoint. If you don't want to have your photo taken, you will go through TSA's standard identity verification and screening procedures. You won't lose your place in line, and you won't have to go through additional screening procedures or have other negative consequences.

Minors don't participate in TSA PreCheck: TIS since they don't have to provide identity documents for verification.

The system compares your live photo template with a template of your pre-staged ID photo.

When you get to the airport security checkpoint, you'll see signage directing TSA PreCheck: TIS passengers to the appropriate lane.

When you go through the TSA PreCheck: TIS lane, you'll have your live photo taken.

TSA PreCheck: TIS uses CBP's facial identification technology, the Traveler Verification Service (TVS). CBP developed the TVS for its Congressionally-mandated biometric entry and exit program.

If you opted in, the TVS will retrieve your passport and/or other government-held photographs using your passport number or Known Traveler Number. These are pictures that you previously supplied to the government. TVS will stage a biometric template of the photo for matching in a temporary gallery. The gallery is airport-specific and includes pictures of travelers for that day only.

These photos are encrypted while in DHS holdings, as well as during transit. The photos are templatized when staged in the temporary gallery. This means that the images are transformed into proprietary mathematical representations that can't be reverse engineered to reproduce the original image. At the checkpoint, TVS compares a template of your live photo to templates of the pre-staged photos.

Your live photo is deleted within 24 hours.

- The staged images are deleted from TVS within 24 hours after your scheduled departure.
- The live photos are deleted within 24 hours after your scheduled departure, with one exception. On rare occasions, DHS Science and Technology (S&T) uses photos for testing and evaluation under tightly constrained terms and limits to examine performance and recommend improvements. The photos selected for testing vary depending on the technology being evaluated. TSA posts signage to provide notice that data is used for limited testing purposes. TSA does not have access to the data after it is transferred to DHS S&T.

With TSA PreCheck: TIS, only biometric templates of facial images of passengers who have opted in through the airline and are traveling that day from that airport are staged in the CBP TVS gallery.

Redress

If you have feedback, questions, or a complaint about your experience with TSA's use of FR/FC technologies, get in touch.

If it's in the moment, ask to speak to the supervisory agent or officer on hand.

If it's after the fact, you can:

- Contact Customer Service | Transportation Security Administration (tsa.gov) to request information, submit complaints or compliments, and let TSA know about security issues or civil rights violations.
- File a complaint with the DHS Office for Civil Rights and Civil Liberties if you believe DHS has violated your rights or someone else's rights.

These options are available to all travelers, regardless of citizenship status.

Testing Results

DHS S&T and TSA most recently tested the TSA PreCheck: Touchless Identity system in the fall of 2024. The evaluation process used both scenario testing and operational data. Scenario testing looks at how technology works in a simulated real-world environment. Operational data were provided with informed consent by TSA PreCheck members from airports where the system is being used.

This technology is still in a field assessment phase. This means that it isn't fully operational.

Two elements of TSA PreCheck: Touchless Identity Solution (TIS) system were tested: face capture and face recognition.

Face capture testing results:

- **On average, the face capture technology for TSA PreCheck: Touchless Identity Solution worked 93% of the time.** This was caused by an issue with the face detection algorithm, which automatically confirms if a photo actually contains a face the photo is processed for face recognition.
- **This led to variations in face capture performance based on age, gender, race, and skin tone.**
  - In testing, face capture worked 89% of the time for those aged 61+ years. It worked 94-96% of the time for those under age 61 years, showing a difference in performance based on age.
  - Face capture worked 91% of the time for male volunteers, compared to 95% for female volunteers, showing a difference in performance based on gender.
  - Face capture worked 88% of the time for those with darker skin tones, compared to 94-97% of the time for those with lighter skin tones. This shows a difference in performance based on skin tone. Additionally, it worked 91% for participants who identified as Black or African American, compared to 96% for those who identified as white.
- **A new manual override feature allows for a 100% face capture success rate.**
  In response to these findings, TSA immediately introduced a feature to allow the Transportation Security Officer (TSO) to manually override the face detection algorithm when it doesn't work. Based on testing in December 2024, this only adds 2-3 seconds to the process and does not affect the overall screening experience. TSA and DHS S&T are evaluating new algorithms to improve this step and plan to test and implement them later this year.

Face recognition testing results

- The face recognition technology for TSA PreCheck: Touchless Identity Solution worked more than 99% of the time. This number was above 99% for all demographic groups.

Transaction time

DHS also measures the transaction time, or "efficiency." This is how long it takes to move through the whole process and is important for operational planning. The efficiency, or transaction time, was 8 seconds on average. All demographic groups were within 1 second of the average, and it took less than 9 seconds for all demographic groups.

Next Steps

TSA continues working with DHS S&T and the Maryland Test Facility (MdTF) to conduct additional testing on commercial face capture algorithms integrated in the TSA PreCheck: TIS unit. Early in summer 2025, DHS S&T and the Maryland Test Facility (MdTF) will conduct a small-scale experiment with participants to interact with the TSA PreCheck: TIS unit to test each face capture algorithm. They will use the results to determine the best face capture algorithm for TSA's use case and then conduct a larger, lab-based test to ensure that TSA meets the DHS FR/FC Directive requirements for a demographically diverse population.

Table 16 – Summary performance metrics for TSA PreCheck: Touchless Identity Solution

Metric	Measured
Face Capture Success Rate Percentage of interactions where system successfully captured face on first try	93%
Face Matching Success Rate Percentage of interactions where probe photo successfully matched ID photo	>99%
Transaction time Average time for volunteer to interact with system through entire interaction (includes system and volunteer errors)	8.0 seconds

Volunteer demographics

634 volunteers took part in the test. The volunteers provided demographic information, including:

- Self-identified age, gender, and race/ethnicity
- A measure of skin tone, which is taken by a calibrated instrument called a colorimeter. S&T uses the DSM III colorimeter from Cortex Technology.

Table 17 – Performance metrics by demographic group for TSA PreCheck: Touchless Identity Solution

Demographic Group Results are shown for demographic groups with over 90 samples.	**Face Capture Success Rate** *Measured*	**Face Matching Success Rate** *Measured*	**Transaction Time** *Measured*
Gender *Volunteers self-identified*			
Male	91%	>99%	8.1 seconds
Female	95%	100%	7.9 seconds
Race *Volunteers self-identified*			
Black or African American	91%	>99%	8.3 seconds
White	96%	100%	7.8 seconds
Age Group (years) *Volunteers self-identified*			
18-30	94%	100%	7.7 seconds
31-45	96%	100%	7.6 seconds
46-60	94%	100%	7.9 seconds
61+	89%	>99%	8.7 seconds
Skin Tone *Measured by a calibrated instrument called a colorimeter.* *S&T uses the DSM III colorimeter from Cortex Technology.*			
T1 (Darker)	88%	>99%	8.5 seconds
T2	94%	100%	7.8 seconds
T3 (Lighter)	97%	100%	7.8 seconds

Scenario testing

We tested the TSA PreCheck: Touchless Identity Solution (TIS) at the Maryland Test Facility. The testing lab was set up to resemble a TSA PreCheck security checkpoint. An operator played the part of the Transportation Security Officer (TSO) who would staff the checkpoint at an airport.

Table 18 – Scenario testing process

Test process
1. The volunteer approaches the TIS and operator.
2. The TIS performs face detection and takes a picture (a "probe face image") of the volunteer.
3. The operator sees the picture onscreen and approves it.
4. The live photo ("probe face image") is matched to a gallery of previously acquired face images.

Table 19 – Technology summary

Technology title	Technology name/type
System Build (Face Capture Software)	TIS V1.0 Fall 2024
System Type	Auto and Manual Facial Capture with 1:N (Gallery) Face Matching
Face Capture Device	3.2 MP Digital Camera
Face Capture Algorithm	OpenCV Haar Cascade Frontal Classifier combined with the Haar Cascade Eye Classifier
Face Recognition Algorithm	NEC NeoFaceV Version 3.3.0 0200 64-bit TVS Identify (Trusted Traveler Galleries)

Image 10: A TSA PreCheck: Touchless Identity Solution kiosk at an airport.

Homeland Security

IMPLEMENTATION OF DHS DIRECTIVE 026-11: USE OF FACE RECOGNITION AND FACE CAPTURE TECHNOLOGIES

2024 Report on Select Use Cases