United States Government Accountability Office

Report to Congressional Requesters

August 2021

FACIAL RECOGNITION TECHNOLOGY

Current and Planned Uses by Federal Agencies

GAO-21-526

GAO@100 Highlights

Highlights of GAO-21-526, a report to congressional requesters

August 2021

FACIAL RECOGNITION TECHNOLOGY

Current and Planned Uses by Federal Agencies

Why GAO Did This Study

Facial recognition—a type of biometric technology—mimics how people identify or verify others by examining their faces. Recent advancements have increased the accuracy of automated FRT resulting in increased use across a range of applications. As the use of FRT continues to expand, it has become increasingly important to understand its use across the federal government in a comprehensive way.

GAO was asked to review the extent of FRT use across the federal government. This report identifies and describes (1) how agencies used FRT in fiscal year 2020, including any related research and development and interactions with non-federal entities, and (2) how agencies plan to expand their use of FRT through fiscal year 2023.

GAO surveyed the 24 agencies of the Chief Financial Officers Act of 1990, as amended, regarding their use of facial recognition technology. GAO also interviewed agency officials and reviewed documents, such as system descriptions, and information provided by agencies that reported using the technology.

View GAO-21-526. For more information, contact Candice N. Wright at (202) 512-6888 or wrightc@gao.gov, or Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov.

What GAO Found

In response to GAO's survey about facial recognition technology (FRT) activities in fiscal year 2020, 18 of the 24 surveyed agencies reported using an FRT system, for one or more purposes, including:

- **Digital access or cybersecurity.** Sixteen agencies reported using FRT for digital access or cybersecurity purposes. Of these, 14 agencies authorized personnel to use FRT to unlock their agency-issued smartphones—the most common purpose of FRT reported. Two agencies also reported testing FRT to verify identities of persons accessing government websites.

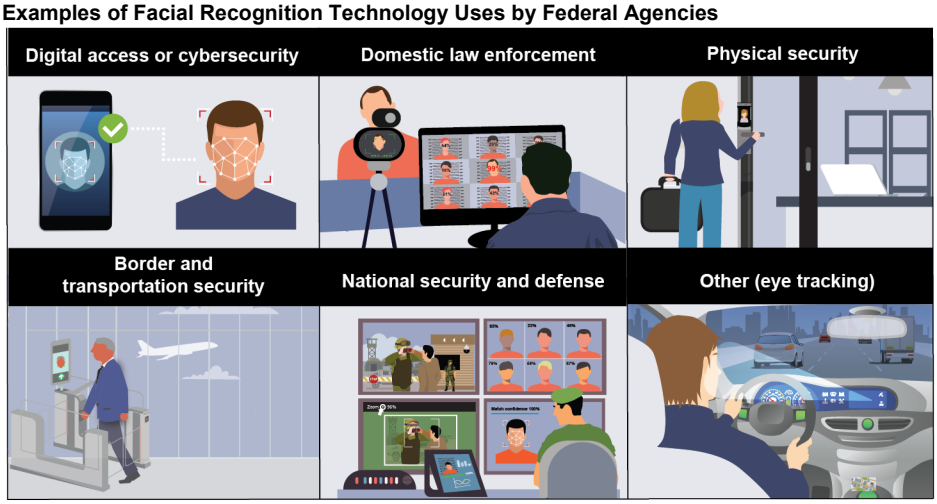
- **Domestic law enforcement**. Six agencies reported using FRT to generate leads in criminal investigations, such as identifying a person of interest, by comparing their image against mugshots. In some cases, agencies identify crime victims, such as exploited children, by using commercial systems that compare against publicly available images, such as from social media.

- **Physical security.** Five agencies reported using FRT to monitor or surveil locations to determine if an individual is present, such as someone on a watchlist, or to control access to a building or facility. For example, an agency used it to monitor live video for persons on watchlists and to alert security personnel to these persons without needing to memorize them.

Ten agencies reported FRT-related research and development. For example, agencies reported researching FRT's ability to identify individuals wearing masks during the COVID-19 pandemic and to detect image manipulation.

Furthermore, ten agencies reported plans to expand their use of FRT through fiscal year 2023. For example, an agency plans to pilot the use of FRT to automate the identity verification process at airports for travelers.

Examples of Facial Recognition Technology Uses by Federal Agencies



Source: GAO analysis of survey results and GoldenSikora/metamorworks/Cipta/stock.adobe.com. | GAO-21-526

Contents

Letter		1
	Background	3
	Agencies Most Often Reported Using FRT for Digital Access and Domestic Law Enforcement	9
	Ten Agencies Plan to Expand Use of FRT, Mostly through Use of New FRT Systems	25
	Agency Comments	29
Appendix I	Objectives, Scope, and Methodology	31
Appendix II	Summaries of Selected Federal Agencies' Facial Recognition Technology Activities	38
Appendix III	Comments from the U.S. Agency for International Development	81
Appendix IV	Comments from the Social Security Administration	83
Appendix V	GAO Contacts and Staff Acknowledgments	84

Tables

Table 1: Facial Recognition Technology (FRT) Activities Reported by Federal Agencies for Fiscal Year 2020	9
Table 2: Reported Purposes of Facial Recognition Technology Systems Used by Federal Agencies in Fiscal Year 2020	11
Table 3: Federally Owned Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020	16
Table 4: Commercially Owned Facial Recognition Technology (FRT) Systems Accessed by Federal Agencies in Fiscal Year 2020	20
Table 5: Federal Agencies That Reported Plans to Expand Their Use of Facial Recognition Technology (FRT) Systems, through Fiscal Year 2023	25

Table 6: New Facial Recognition Technology (FRT) Systems Federal Agencies Reported they Plan to Use, through Fiscal Year 2023 26

Figures

Figure 1: Process used in Facial Recognition Technology 5
Figure 2: Examples of Federal Agencies' Use of Facial Recognition Technology (FRT) 8
Figure 3: States and Localities that Own Facial Recognition Technology (FRT) Systems Accessed by Federal Agencies in Fiscal Year 2020 18

Abbreviations

CBP	U.S. Customs and Border Protection
CFO Act	Chief Financial Officers Act of 1990
COVID-19	Coronavirus Disease 2019
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
EPA	Environmental Protection Agency
FACE	Facial Analysis, Comparison, and Evaluation
FBI	Federal Bureau of Investigation
FRT	facial recognition technology
GSA	General Services Administration
HHS	Department of Health and Human Services
HSIN	Homeland Security Information Network
IDENT	Automated Biometric Identification System
NASA	National Aeronautics and Space Administration
NCRFRILS	National Capital Region Facial Recognition Investigative Leads System
NSF	National Science Foundation
OPM	Office of Personnel Management
PIN	personal identification number
RAPIDS	Real-time Automated Personnel Identification System
SSA	Social Security Administration
TSA	Transportation Security Administration
USAID	U.S. Agency for International Development
USDA	U.S. Department of Agriculture
VA	Department of Veterans Affairs

441 G St. N.W.
Washington, DC 20548

August 24, 2021

The Honorable Jim Jordan
Ranking Member
Committee on the Judiciary
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
The Honorable James Comer
Ranking Member
Committee on Oversight and Reform
House of Representatives

Of all the biometric technologies—those used to identify people based on their biological and behavioral characteristics—facial recognition most closely mimics how people identify others: by examining their faces. What is an effortless skill in humans has proven difficult to replicate in machines, but computer and technology advancements over the past few decades have increased the overall accuracy of automated facial recognition. As a result, the use of facial recognition technology (FRT) has become increasingly common across business and government sectors. For example, it is used as a tool for identifying or verifying customers, and to verify an employee's identity when logging into a computer. Law enforcement can also use it to search databases, such as driver's license photos and mugshots, for possible leads about an unknown individual's identity as part of a criminal investigation.

As the use of FRT continues to expand, Members of Congress, academics, and advocacy organizations have highlighted the importance of developing a comprehensive understanding of how it is used by federal agencies. This report is the latest in a series of recent reports we have issued on FRT. In June 2021, we reported on federal law enforcement's use of FRT, including the extent of its use and how the agencies monitor such use.[1] In September 2020, we reported on the U.S. Customs and

[1]GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Washington, D.C., June 3, 2021). In this report, we made 26 recommendations related to using nonfederal systems with facial recognition technology to eight agencies, including the Departments of Health and Human Services, Homeland Security, the Interior, Justice, State, and the Treasury.

Border Protection's (CBP) and Transportation Security Administration's (TSA) use of FRT at U.S. ports of entry and made recommendations to CBP to improve its privacy practices and system performance.[2] In 2016, we reported on the Federal Bureau of Investigation's (FBI) use of FRT and made recommendations to improve the Bureau's understanding of the accuracy of and privacy protection processes for its FRT capabilities.[3] We have also recently reported on the ways FRT can be used in commercial settings, including to provide secure access to online customer accounts and information on customer flows during peak times, among others.[4]

You asked us to review the extent of FRT use across the federal government. This report identifies and describes (1) how agencies used FRT in fiscal year 2020, including any FRT-related research and development activities and interactions with nonfederal entities, and (2) how agencies plan to expand their use of FRT through fiscal year 2023.

To address these objectives, we administered a survey to the 24 Chief Financial Officers (CFO) Act agencies[5] to collect information related to: (1) FRT systems used (owned or accessed, including those tested) by

[2]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). In this report, we made five recommendations to CBP related to its use of facial recognition technology, and DHS concurred with the recommendations. In March and April 2021, CBP provided a status update on progress towards each of these recommendations. Based on the documentation provided by CBP, GAO closed two recommendations as implemented.

[3]GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016). In this report, we made six recommendations related to accuracy and privacy. The FBI has addressed all six recommendations.

[4]GAO, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522 (Washington, D.C.: July 13, 2020) and GAO, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015).

[5]The 24 agencies are those identified in the Chief Financial Officers Act of 1990, as amended (31 U.S.C. § 901(b)). They are the U.S. Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, Veterans Affairs, Environmental Protection Agency, National Aeronautics and Space Administration, U.S. Agency for International Development, General Services Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration.

agencies during fiscal year 2020; (2) FRT systems agencies planned to use through fiscal year 2023; (3) agencies' FRT-related research and development activities; (4) transactions (financial or otherwise) that agencies entered into for nonfederal entities' use of FRT; and (5) the extent to which agencies regulated nonfederal entities' use of FRT.[6] The questionnaire also asked detailed questions about the individual FRT systems that agencies reported, which included the purpose(s), a brief description of its use, and obligations related to its use. We asked agencies to include the activities of all their components, bureaus, and offices in their responses. We emailed questionnaires to the agencies in October 2020, and closed the survey in January 2021 after receiving responses from all 24 agencies. We reviewed the responses we collected and took quality control steps by performing checks for completeness, logical errors, and inconsistencies. We followed up with agencies in writing or through interviews, as appropriate. See appendix I for additional information on our scope and methodology.

We conducted this performance audit from April 2020 through August 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

Background

How Facial Recognition Technology Works

Facial recognition can verify or identify individuals by their faces. It is one of several biometric technologies that identify individuals by measuring and analyzing physical and behavioral characteristics.[7] As seen in figure 1, facial recognition technology uses a photo or still from a video feed of a person—often called a probe or live photo—and converts it into a template, or a mathematical representation of the photo. A matching

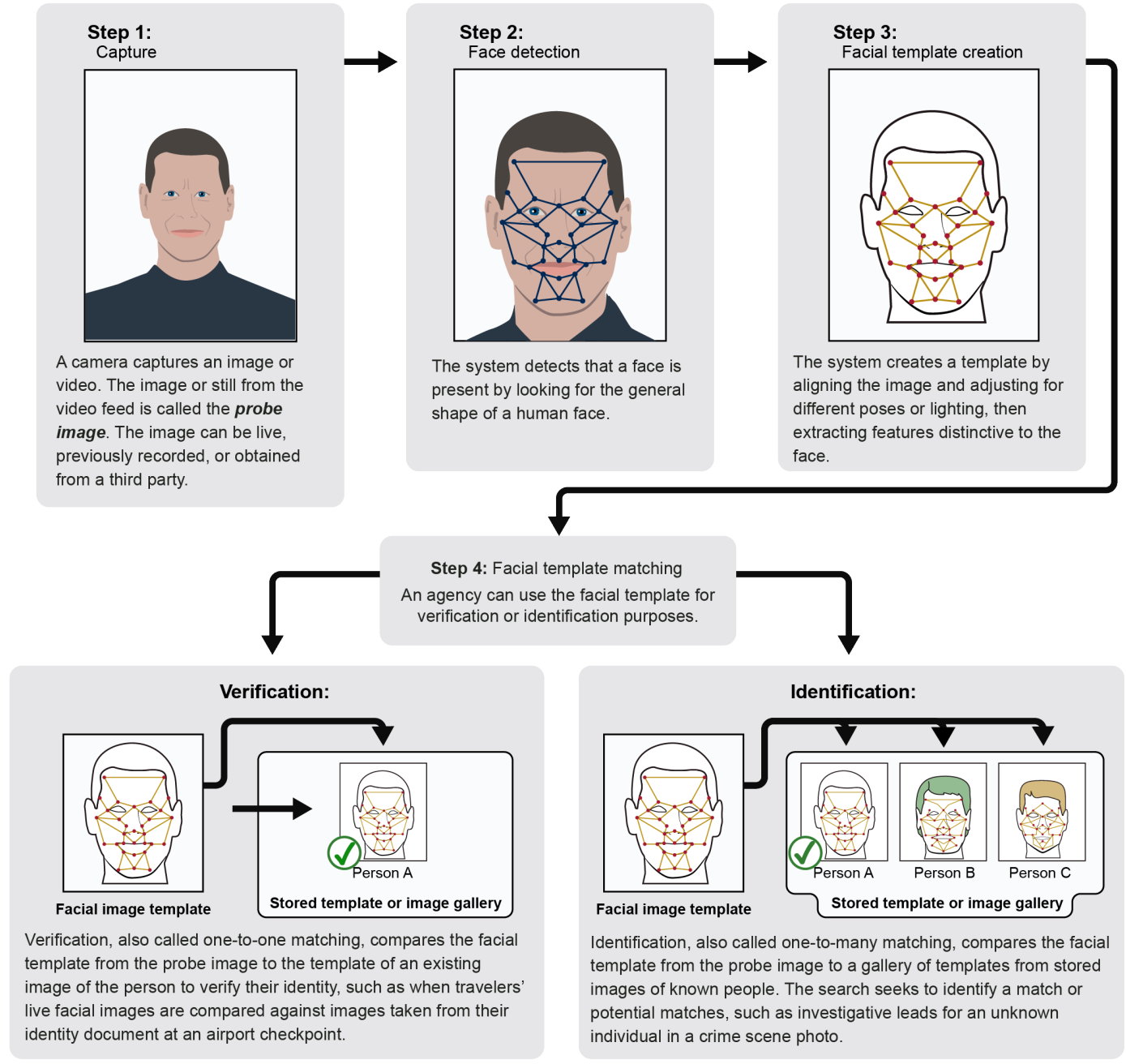
[6]Regulated refers to using regulatory authority over a nonfederal entity to regulate that entity's use of its own FRT. For the purposes of our questionnaire, we defined "regulated" as regulatory functions in which the agency engaged, including, but not limited to, investigatory and inspections activities, taking enforcement actions, prescribing requirements or guidance, conducting oversight, and maintaining performance standards.

[7]Other biometric technologies can identify individuals by measuring and analyzing physical and behavioral characteristics, which include fingerprints, eye irises, voice, and gait.

algorithm can then compare the template to one from another photo and calculate their similarity.

Facial recognition searches or comparisons generally fall into two categories: verification and identification. Verification (or one-to-one searches) compares a stored photo of an individual to another photo purportedly of the same individual to determine whether they are the same person. For example, this type of comparison can help verify the identity of an individual attempting to unlock a smartphone. Identification (or one-to-many searches) compares a photo from a single individual against a gallery of stored photos from a number of individuals to determine if there is a potential match. For example, this type of comparison can be used to identify investigative leads for an unknown individual in a crime scene photo.

Figure 1: Process used in Facial Recognition Technology



Source: GAO analysis. | GAO-21-526

Two technologies, facial detection and facial analysis, are related to, but distinct from, facial recognition. Whereas facial recognition matches a face to a specific identity:

- *Facial detection* determines if a photo or video contains a face in the image. It is commonly used to count the number of people that move through a particular area without determining their identities, such as counting people in stores or amusement park lines.
- *Facial analysis*, sometimes referred to as facial classification or characterization, uses a facial image to estimate or classify personal characteristics such as age, race, or sex, or tracks facial features or movement to recognize expressions or gaze, among other analyses. For example, facial analysis can be part of an eye tracking system, which can allow researchers to analyze how well pilots use their eyes or gaze to scan their cockpit instruments.

For the purposes of this report, we use the term "facial recognition technology" to include facial recognition, facial detection, or facial analysis technologies.

Federal Use of Facial Recognition Technology Systems

A facial recognition technology system may include components or modules of systems, software applications, or devices with automated facial recognition capabilities, such as a face recognition algorithm, hardware, or software. Federal agencies can own their FRT systems or access the FRT systems of other government entities, including federal, state, local, tribal, and territorial governments, and commercial facial recognition service providers.[8] Agencies can have direct access to an FRT system, such as by logging into the system, or indirect access, such as by requesting a state government (i.e., a third party) run a facial recognition search on behalf of the federal agency.

FRT systems are used for a variety of purposes across the federal government. These purposes and examples of how FRT can be used are grouped into seven different categories, as follows:[9]

[8]We use the term "federally owned" when an agency developed or acquired the FRT and performs its own searches. We use the term "commercially owned" when an agency contracts for an FRT service, such as a search performed against the commercial entity's database of images or performed by the commercial entity itself and the results are provided back to the agency.

[9]For the purposes of this report, we determined these categories to describe the different ways agencies could use FRT.

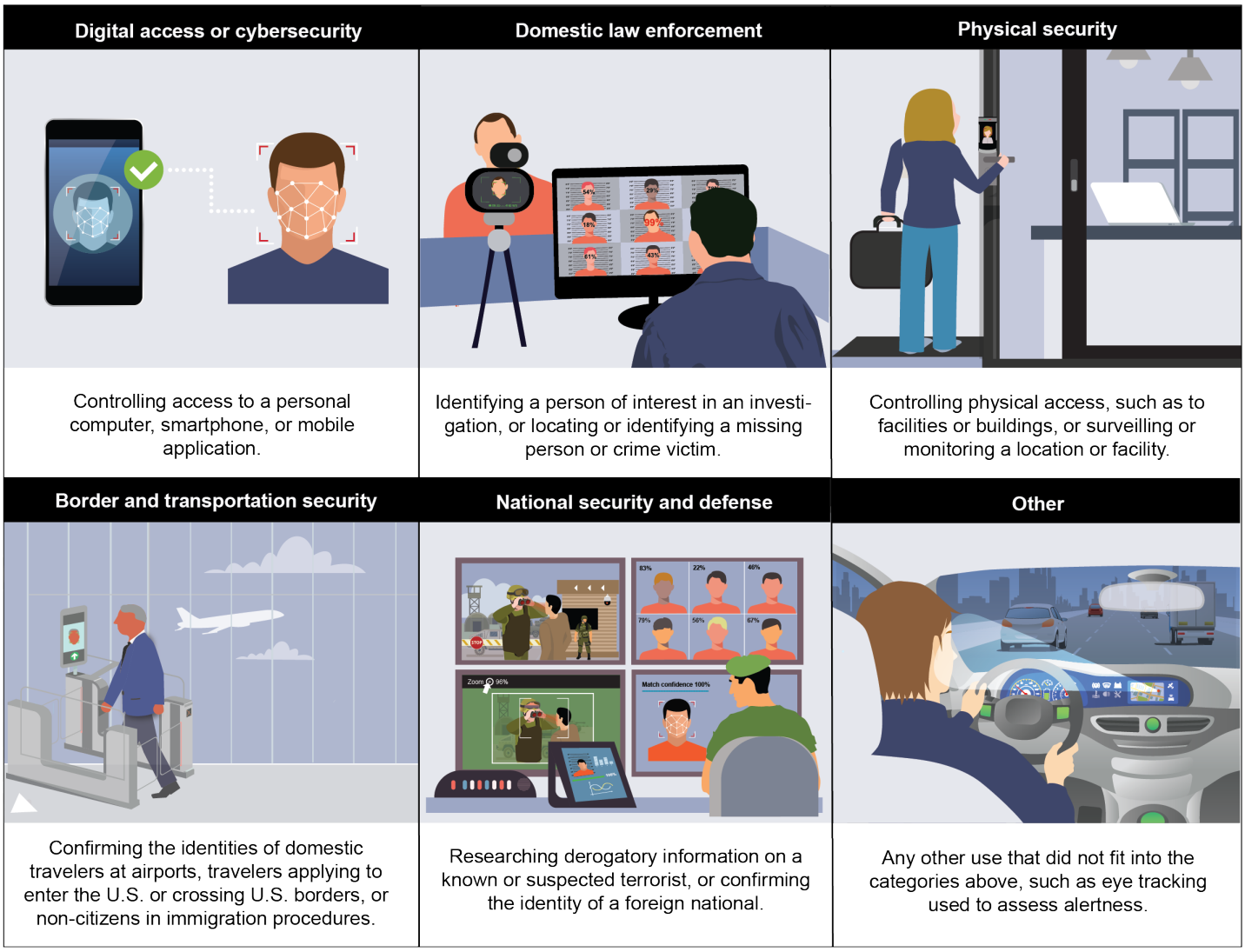
- **Digital access or cybersecurity.** This purpose includes FRT that can be used to control access to a personal computer, smartphone, or mobile application.
- **Domestic law enforcement.** This purpose includes FRT that can be used to identify a lead or person of interest in an investigation, or to locate or identify a missing person or crime victim.
- **Physical security.** This purpose includes FRT that can be used to control physical access, such as to facilities or buildings, or to surveil or monitor a location or facility, including notification that an individual is present in real-time.
- **Border and transportation security.** This purpose includes FRT that can be used to confirm the identities of domestic travelers at airports, travelers applying to enter the United States or crossing U.S. borders, or non-citizens in immigration proceedings.
- **National security and defense.** This purpose includes FRT that can be used to research derogatory information on a known or suspected terrorist, or confirm the identity of a foreign national for national security reasons.[10]
- **Medical assessment.** This purpose includes FRT that can be used to confirm a patient's identity in a medical setting, such as when dispensing controlled substance prescriptions, or to assist with contact tracing (e.g., related to Coronavirus Disease 2019 or COVID-19).[11]
- **Other.** These FRT purposes include analysis of the face itself, such as analysis of attention or alertness based on eye tracking, or inferring characteristics of a person, including age or sex. It also includes any other agency use that does not fit into the categories above.

Illustrative examples of these purposes are shown in figure 2.

[10]For example, to confirm the identity of a foreign national seeking access to a military installation.

[11]For information on how contact tracing can occur, see GAO, *Science & Tech Spotlight: Contact Tracing Apps*, GAO-20-666SP (Washington, D.C., Jul. 28, 2020).

Figure 2: Examples of Federal Agencies' Use of Facial Recognition Technology (FRT)



Source: GAO analysis of survey results and GoldenSikora/metamorworks/Cipta/stock.adobe.com. | GAO-21-526

Agencies Most Often Reported Using FRT for Digital Access and Domestic Law Enforcement

Most of the federal agencies we surveyed—19 of 24—reported one or more FRT-related activities in fiscal year 2020, with digital access and domestic law enforcement as the most common. For the purposes of our survey, we identified four types of FRT activities an agency can engage in: (1) using an FRT system, which includes owning, accessing, or testing the system; (2) conducting or supporting FRT-related research and development; (3) entering into transactions with nonfederal entities, such as awarding grants to enable entities to obtain FRT systems for their own uses; and (4) regulating the use of FRT by nonfederal entities. Table 1 shows the four types of FRT activities reported in fiscal year 2020 by the 24 federal agencies we surveyed. Five agencies reported they did not conduct any of these FRT activities in fiscal year 2020: the Department of Education, Department of Housing and Urban Development, Department of Labor, the Nuclear Regulatory Commission, and the Small Business Administration.

Table 1: Facial Recognition Technology (FRT) Activities Reported by Federal Agencies for Fiscal Year 2020

Federal Agency	Used FRT systems[a]	Conducted FRT-related research and development[b]	Entered into transactions with nonfederal entities for FRT[c]	Regulated nonfederal entities' use of FRT[d]
Department of Agriculture	●	⊗	⊗	⊗
Department of Commerce	●	●	⊗	⊗
Department of Defense	●	●	⊗	⊗
Department of Education	⊗	⊗	⊗	⊗
Department of Energy	●	⊗	⊗	⊗
Department of Health and Human Services	●	●	⊗	⊗
Department of Homeland Security	●	●	●	●[e]
Department of Housing and Urban Development	⊗	⊗	⊗	⊗
Department of the Interior	●	⊗	⊗	⊗
Department of Justice	●	●	●	⊗
Department of Labor	⊗	⊗	⊗	⊗
Department of State	●	●	●	⊗
Department of Transportation	⊗	●	⊗	⊗
Department of the Treasury	●	⊗	⊗	⊗
Department of Veterans Affairs	●	●	●	⊗
U.S. Agency for International Development	●	⊗	⊗	⊗
Environmental Protection Agency	●	⊗	⊗	⊗
General Services Administration	●	⊗	⊗	⊗
National Aeronautics and Space Administration	●	●	⊗	⊗

Federal Agency	Used FRT systems[a]	Conducted FRT-related research and development[b]	Entered into transactions with nonfederal entities for FRT[c]	Regulated nonfederal entities' use of FRT[d]
National Science Foundation	●	●	⊗	⊗
Nuclear Regulatory Commission	⊗	⊗	⊗	⊗
Office of Personnel Management	●	⊗	⊗	⊗
Small Business Administration	⊗	⊗	⊗	⊗
Social Security Administration	●	⊗	⊗	⊗

● Yes

⊗ No

Source: GAO analysis of survey results. | GAO-21-526

[a]The agency owned or accessed FRT in fiscal year 2020.

[b]Research and development also includes agencies that obligated funds for FRT-related research conducted by other entities.

[c]Refers to agencies that entered into transactions, such as awarding grants to nonfederal entities to purchase FRT equipment.

[d]Refers to using regulatory authority over a nonfederal entity to regulate that entity's use of its own FRT. For the purposes of our questionnaire, we defined "regulated" as regulatory functions in which the agency engaged, including, but not limited to, investigatory and inspections activities, taking enforcement actions, prescribing requirements or guidance, conducting oversight, and maintaining performance standards.

[e]The Transportation Security Administration within the Department of Homeland Security used its authority to regulate entities under its jurisdiction.

Eighteen Agencies Reported Using FRT for a Variety of Purposes

Eighteen of the 24 agencies we surveyed responded that they used facial recognition technology in fiscal year 2020, as shown in the first column of table 1 above.[12] These agencies reported using FRT for one or more purposes, with digital access and domestic law enforcement as the most common (see table 2).[13] Agencies did not report using FRT for medical assessment purposes in fiscal year 2020.

[12]In our questionnaire, we asked, "At any point in fiscal year 2020, did you agency use facial recognition technology for any of the following purposes?" These purposes are: (1) digital access or cybersecurity; (2) domestic law enforcement; (3) physical security; (4) border and transportation security; (5) national security and defense; (6) medical assessment; and (7) other purposes. For the purposes of this questionnaire and report, "use" refers to whether an agency: (1) owned and/or operated a FRT system, (2) accessed (directly or through a third party) an FRT system as part of a program or activity within their agency but that was owned by another federal or nonfederal entity, or (3) tested a FRT system as part of a pilot, proof of concept, trial, or evaluation for potential agency use.

[13]Agencies reported that some FRT systems were used for multiple purpose categories.

Table 2: Reported Purposes of Facial Recognition Technology Systems Used by Federal Agencies in Fiscal Year 2020

	Purpose					
Federal Agency	**Digital access**	**Domestic law enforcement**	**Physical security**	**Border and transportation security**	**National security and defense**	**Other**
Department of Agriculture	●	⊗	⊗	⊗	⊗	⊗
Department of Commerce	●	⊗	●	⊗	⊗	⊗
Department of Defense	⊗	●	●	⊗	●	●
Department of Energy	●	⊗	●	⊗	⊗	⊗
Department of Health and Human Services	●	●	●	⊗	⊗	⊗
Department of Homeland Security	●	●	⊗	●	●	⊗
Department of the Interior	●	●	⊗	⊗	⊗	⊗
Department of Justice	●	●	●	⊗	●	●
Department of State	⊗	⊗	⊗	●	●	⊗
Department of the Treasury	●	●	⊗	⊗	⊗	⊗
Department of Veterans Affairs	●	⊗	⊗	⊗	⊗	⊗
Agency for International Development	●	⊗	⊗	⊗	⊗	⊗
Environmental Protection Agency	●	⊗	⊗	⊗	⊗	⊗
General Services Administration	●	⊗	⊗	⊗	⊗	⊗
National Aeronautics and Space Administration	●	⊗	⊗	⊗	⊗	●
National Science Foundation	●	⊗	⊗	⊗	⊗	⊗
Office of Personnel Management	●	⊗	⊗	⊗	⊗	⊗
Social Security Administration	●	⊗	⊗	⊗	⊗	⊗

● Yes

⊗ No

Source: GAO analysis of survey results. | GAO-21-526

Note: Agencies did not report using FRT for medical purposes in fiscal year 2020.

Examples of how agencies used FRT in each purpose category are described below.

- **Digital access or cybersecurity.** Sixteen agencies reported using FRT for digital access or cybersecurity purposes.[14] Of these, 14 agencies authorized personnel to use FRT to unlock their agency-issued smartphones—the most common purpose of FRT reported by the agencies in our survey.[15] Two agencies—General Services Administration (GSA) and Social Security Administration (SSA)—reported conducting pilots that used agency employees to test FRT systems as a means to control access to certain government websites, such as GSA's login.gov.[16] Specifically, GSA and SSA used FRT to compare two images—a government photo identification and a live image of the individual—to verify the identity of an individual attempting to apply for an account. This FRT system may also conduct a check to detect if there is an attempt to subvert the FRT using a printed image or other non-live object.[17] However, agency officials said that this FRT would not be deployed until additional testing under a range of conditions is completed.

[14]GAO's cybersecurity work encompasses a broad range of issues assessing information security as a government-wide high-risk area, including protecting cyber critical infrastructure and protecting the privacy of personally identifiable information. This body of work also addresses agency compliance with federal cybersecurity requirements and includes assessments of security controls. As used in this report, cybersecurity refers to the general framework that includes digital access and other controls.

[15]The 14 agencies that reported using facial recognition to unlock smartphones or tablets are the Departments of Agriculture (USDA), Commerce, Homeland Security (DHS), Energy (DOE), Justice (DOJ), Health and Human Services (HHS), the Interior, the Treasury, Veterans Affairs (VA), the Environmental Protection Agency (EPA), the National Aeronautics and Space Administration (NASA), the National Science Foundation (NSF), the Office of Personnel Management (OPM), and the U.S. Agency for International Development (USAID). Many of these agencies reported that they did not require FRT when procuring their smartphones; rather it was a feature that was built into the smartphone. We did not inquire whether an agency monitored an employee's use of facial recognition to unlock their agency-issued smartphones or had policies related to its use. However, OPM reported that they no longer authorized personnel to use the feature.

[16]Login.gov is a publicly accessible website that verifies the identities of individuals seeking to access participating agencies' websites.

[17]This check detects whether a facial recognition system sensor is viewing data from a live subject as opposed to recorded data of a non-living object. For example, a picture or a 3D mask or a printed image that may be presented to try to fool the FRT system into false authentication.

- **Domestic law enforcement.** Six agencies—Departments of Homeland Security (DHS), Justice (DOJ), Defense (DOD), Health and Human Services (HHS), the Interior, and the Treasury—reported using FRT to generate leads in criminal investigations, such as identifying a person of interest by comparing images of the person against databases of mugshots or from other law enforcement encounters.[18] For example, DOJ's Federal Bureau of Investigation used the Next Generation Identification Interstate Photo System to generate leads during investigations by comparing photos of unknown individuals suspected of criminal activity against a repository of photos of known individuals, including mugshots and other records. In addition, agencies may access commercially owned FRT systems as part of criminal investigations or to assist in identifying a missing person or victims of crimes, such as exploited children. For example, DHS, DOJ, HHS, and the Interior reported using Clearview AI, a commercially owned facial recognition system that compares a submitted photo against a database of publicly available images from open sources, such as social media, and returns matching images for review.
- **Physical security.** Five agencies—Department of Commerce, DOD, Department of Energy (DOE), DOJ, and HHS—reported using FRT to monitor or surveil locations to determine if an individual is present, such as someone from a watchlist, or to control access to a building or facility. For example, HHS reported that it used an FRT system (AnyVision) to monitor its facilities by searching live camera feeds in real-time for individuals on watchlists or suspected of criminal activity, which reduces the need for security guards to memorize these individuals' faces. This system automatically alerts personnel when an individual on a watchlist is present. In addition, DOJ reported using an FRT system to verify that personnel attempting entry into their on-site, secure network operations centers at federal prisons were authorized for entry.
- **Border and transportation security.** Two agencies—DHS and Department of State—reported using FRT systems to assist with

[18]DOD's criminal investigative organizations (e.g., Naval Criminal Investigative Service and Air Force Office of Special Investigations) and other DOD law enforcement agencies or organizations (e.g., military police departments) can use FRT for domestic law enforcement, in addition to other purposes, when "that information logically relates to the detection, neutralization, or deterrence of criminal activity that affects DOD personnel, property, or mission." *See*, Department of Defense, DOD Instruction No. 5505.17, *Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DOD Law Enforcement Activities*, (Washington, D.C., Dec. 19, 2012, rev. Nov. 29, 2016).

identifying or verifying travelers within or seeking admission to the United States, identifying or verifying the identity of non-U.S. citizens already in the United States, and to research agency information about non-U.S. citizens seeking admission to the United States. For example, DHS's U.S. Customs and Border Protection used its Traveler Verification Service at ports of entry to assist with verifying travelers' identities. The Traveler Verification Service uses FRT to compare a photo taken of the traveler at a port of entry with existing photos in DHS holdings, which include photographs from U.S. passports, U.S. visas, and other travel documents, as well as photographs from previous DHS encounters.[19]

- **National security and defense.** Four agencies—DHS, DOD, DOJ, and State—reported using FRT for national security and defense purposes, including to identify individuals known or suspected to be terrorists, research derogatory information about a suspected threat actor, and monitor or surveil locations to search for a person of interest, such as a suspected terrorist. For example, the State Department reported using the Integrated Biometric System, which uses FRT to perform searches of visa and passport applicants' photos against terrorist watchlist photos. The Integrated Biometric System provides consular posts and passport agencies around the world with additional information to evaluate visa and passport applications to decrease the possibility that a terrorist would be able to fraudulently receive a U.S. visa or passport.
- **Other purposes.** Three agencies—DOD, DOJ, and the National Aeronautics and Space Administration (NASA)—reported using FRT for other purposes, including to verify the identities of individuals receiving identification cards and temporary badges, and demonstrate how FRT works in educational settings. For example, DOD tested a facial detection capability to support issuance of DOD identification cards within its Real-time Automated Personnel Identification System (RAPIDS). Specifically, RAPIDS uses facial detection when capturing the cardholder's picture during initial enrollment or identification card issuance or renewal to ensure that the size of the picture printed on the cards is consistent. Similarly, NASA's Johnson Space Center reported testing a prototype FRT system to confirm an employee's identity by comparing a current camera image of the employee with a photo on file.[20]

[19]See GAO-20-568 for more detail.

[20]NASA reported that it conducted the experiment for a limited time only, and did not continue working on or using the prototype after fiscal year 2020.

Eighteen Agencies Reported Owning and Accessing Facial Recognition Technology

According to our analysis of survey responses, 18 agencies reported they owned FRT systems or accessed other entities' FRT systems in fiscal year 2020. Of these agencies, 17 owned or accessed federal FRT systems, three accessed FRT systems owned by state and local entities, and six accessed FRT systems owned by commercial vendors.

Seventeen Agencies Reported Owning or Accessing Federal FRT Systems

Seventeen agencies reported they owned or accessed 27 federal FRT systems.[21] Fourteen of these agencies owned smartphones that can be unlocked with facial recognition, and three of these agencies—U.S. Agency for International Development, EPA, and OPM—did not own or access any other FRT systems.[22] Nine agencies—Commerce, DOD, DOE, HHS, DHS, DOJ, State, GSA, and NASA—owned FRT systems other than smartphones, as shown in table 3. Three of these agencies—DHS, DOD, and DOJ—owned 18 of the 27 federal FRT systems, in addition to owning smartphones. Finally, one agency—Treasury—did not own an FRT system, but accessed federal and commercially owned systems.[23]

[21]In some cases, agencies reported their systems as owned at the component-level (or below), and that access may be given to other components within the same agency. We report such cases as a single instance of ownership by the agency. Appendix II provides more detailed descriptions of the federal FRT systems, including how agencies use them, whether they were accessed by other agencies, and more information on the systems.

[22]We only counted smartphones that can be unlocked using facial recognition as a single FRT system, even though there are multiple vendors offering similar technologies on their smartphones. Fourteen agencies reported they owned smartphones that can be unlocked with facial recognition. These agencies include: USDA, Commerce, DOE, HHS, DOJ, DHS, Interior, Treasury, VA, USAID, EPA, NASA, NSF, and OPM.

[23]Treasury reported it accessed the General Services Administration's login.gov during testing of the FRT capability. Login.gov is a single-sign on mechanism that uses FRT to match applicants to their identification documents to access accounts on agency websites as mentioned earlier. Treasury also reported a third-party vendor performed facial recognition searches on its behalf in April 2020.

Table 3: Federally Owned Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

Agency	Number of FRT Systems Owned	Accessed FRT Systems Owned by Other Agencies	Purposes
Department of Commerce	1 system	• None	• Physical security
Department of Defense	7 systems	• Department of Justice • Department of Homeland Security	• Physical security • Domestic law enforcement • National security and defense • Other
Department of Energy	1 system	• None	• Physical security
Department of Health and Human Services	3 systems	• None	• Physical security • Domestic law enforcement • Digital access or cyber security
Department of Homeland Security	4 systems	• Department of Defense • Department of Justice • Department of State	• Domestic law enforcement • Border and transportation security • National security and defense
Department of Justice	7 systems	• Department of Defense • Department of State	• Domestic law enforcement • Physical security • National security and defense • Other
Department of State	1 system	• Department of Defense	• Border and transportation security • National security and defense
General Services Administration	1 system	• None	• Digital access or cyber security
National Aeronautics and Space Administration	1 system	• None	• Other

Source: GAO analysis of survey results. | GAO-21-526

Note: The table excludes agencies that only reported owning smartphones that can be unlocked with facial recognition. See appendix II for additional information about agency use of FRT systems.

Of the nine agencies that owned an FRT system other than smartphones, five agencies—Commerce, DOE, GSA, HHS, and NASA—reported they owned federal FRT systems and did not access other federal FRT systems. For example, HHS tested an FRT system that agency personnel could use to unlock their laptops. NASA tested another FRT system that verified an employee's identity by comparing a camera image with a photo on file if the employee forgot their badge. Commerce and DOE owned FRT systems that controlled personnel access to secure facilities.

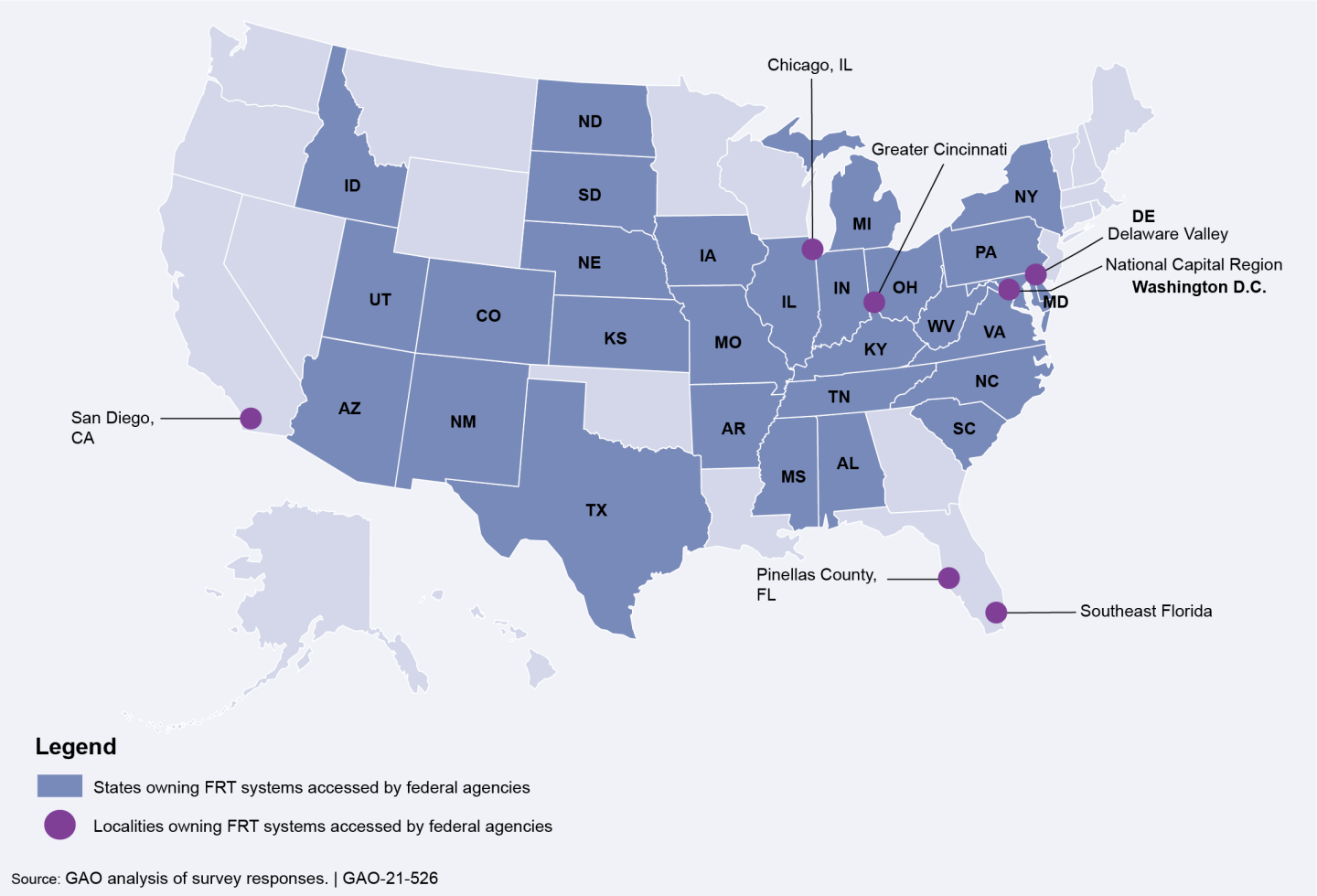
For example, DOE's TacID Guard Dog performs facial matching and facial verification from live video to monitor the entry and exit of agency personnel at access points.

The other four agencies—DOD, DHS, DOJ, and State—reported that they owned an FRT system and also accessed FRT systems owned by other federal agencies. For example, the State Department's Bureau of Consular Affairs reported owning the Integrated Biometric System, which is also accessed by DHS and DOJ. State Department officials used this FRT system to verify a visa applicant's identity or determine whether an individual has previously applied for a visa under an alias. Similarly, DHS accessed the Integrated Biometric System to verify the identity of individuals applying for visas and immigration benefits, and to identify individuals being investigated for identity theft and benefits fraud. In addition, the State Department's Bureau of Diplomatic Security reported accessing DOD's Automated Biometric Identification System to verify the authenticity of an individual's travel documents, among other things.

Three Agencies Reported Accessing FRT Systems Owned by State and Local Entities

Three agencies—DOJ, DHS, and Interior—reported accessing one or more FRT systems owned by 29 states and seven localities for law enforcement purposes. Figure 3 shows the states and localities that own FRT systems accessed by these federal agencies.

Figure 3: States and Localities that Own Facial Recognition Technology (FRT) Systems Accessed by Federal Agencies in Fiscal Year 2020



Source: GAO analysis of survey responses. | GAO-21-526

DOJ and DHS reported direct and indirect access to FRT systems across states and localities.[24] For example, DOJ reported access to FRT systems through personnel in the FBI's Facial Analysis, Comparison, and Evaluation (FACE) Services, which has memoranda of understanding with 21 states and two federal entities to access their FRT systems.

[24]The term 'direct access' refers to cases where federal agency personnel can log into an FRT system and perform a facial recognition search. The term 'indirect access' refers to cases where federal agency personnel request that the owner of an FRT system conduct a facial recognition search.

Specifically, FBI agents can submit a probe photo and request FACE Services examiners perform facial recognition searches for their investigations. FACE Services examiners have direct access to one state FRT system and indirect access to FRT systems owned by 20 other state entities.[25]

In addition, DHS reported it owns the Homeland Security Information Network (HSIN), which enables access to the Multi-State Facial Recognition Community of Interest. While HSIN is not an FRT system, it has a form for authorized users to request indirect facial recognition searches through state and local entities, such as fusion centers.[26] Through various memoranda of understanding, DHS personnel in U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement may submit photos for facial recognition searches to those entities. These searches assist DHS personnel with identifying individuals involved in identity theft and benefit fraud investigations, and targets connected to criminal investigations or to a known terrorist organization. In fiscal year 2020, DHS officials reported the agency made facial recognition search requests to 15 state and four local partner agencies, including state and local law enforcement fusion centers.

Finally, Interior reported it accessed the National Capital Region Facial Recognition Investigative Leads System (NCRFRILS). NCRFRILS is an FRT system that contains copies of information, including photos, from participating law enforcement agencies in the Washington, D.C. metro area. Interior's U.S. Park Police reported that in July 2020 it requested the Maryland National Capital Park Police perform a facial recognition search of NCRFRILS on its behalf to generate investigative leads.

[25]According to FBI officials, for direct access to the Maryland Department of Public Safety and Correctional Services' FRT system, examiners have completed related training requirements, so a memorandum of understanding is unnecessary. FACE Services has direct access to two federal FRT systems—the FBI's Next Generation Identification Interstate Photo System and the Department of State's visa holdings. The FBI can request the Department of State perform facial recognition searches on passport holdings on the FBI's behalf and return only a limited number of photos that are likely matches.

[26]HSIN is for trusted sharing of Sensitive but Unclassified information—such as that related to law enforcement or homeland security—between federal, state, local, territorial, tribal, international, and private sector partners. Generally, fusion centers are collaborative information-sharing efforts to detect, prevent, investigate, and respond to potential criminal activity, including terrorism.

Six Agencies Accessed Commercial FRT Systems

Six agencies—HHS, DHS, Interior, DOJ, Treasury, and SSA—reported accessing eight FRT systems owned by commercial vendors.

Table 4: Commercially Owned Facial Recognition Technology (FRT) Systems Accessed by Federal Agencies in Fiscal Year 2020

Agency	Number of FRT Systems Accessed	Commercial Vendor	Purposes
Department of Health and Human Services	1 system	• Clearview AI	• Domestic law enforcement
Department of Homeland Security	2 systems	• Clearview AI • Vigilant Solutions	• Domestic law enforcement • Border and transportation security • National security and defense
Department of the Interior	1 system	• Clearview AI	• Domestic law enforcement
Department of Justice	2 systems	• Clearview AI • Vigilant Solutions	• Domestic law enforcement
Department of the Treasury	1 system	• Other	• Domestic law enforcement
Social Security Administration	1 system	• Acuant FaceID	• Digital access or cybersecurity

Source: GAO analysis of survey results. | GAO-21-526

Note: See appendix II for additional information about agency use of FRT systems.

As shown in table 4, four agencies—HHS, DHS, Interior, and DOJ—accessed Clearview AI, which conducts facial recognition searches using publicly available images.[27] For example, HHS's Office of the Inspector General reported it began a pilot of Clearview AI in September 2020 to assist with identifying subjects of a criminal investigation. Similarly, DHS reported the U.S. Secret Service and U.S. Immigration and Customs Enforcement piloted Clearview AI in fiscal year 2020, to identify individuals in federal criminal investigations, and to identify perpetrators and victims in domestic and international child exploitation cases, respectively. DHS also reported that, since June 2019, U.S. Customs and Border Protection agents had direct, albeit temporary, access to a Clearview AI through their participation with the New York State Intelligence Center. These agents used Clearview AI to identify criminals, as well as subjects who have been arrested previously, were deported, and attempted to re-enter the United States at the border.

[27]Interior's U.S. Park Police reported that it stopped using Clearview AI in June 2020 after conducting a pilot test in April 2020.

Ten Agencies Reported Conducting or Supporting FRT-related Research and Development

Based on our analysis, 10 of the 24 agencies surveyed—Commerce, DHS, DOD, DOJ, the Department of Transportation (DOT), HHS, VA, NASA, the National Science Foundation (NSF), and State—conducted or supported research and development (R&D) for FRT in fiscal year 2020.[28] Of these agencies, DOT did not report any other FRT-related activities.

Four agencies—DHS, DOD, DOJ, and State—generally focused their R&D on agency-specific needs, such as to develop new applications or improve existing capabilities. Examples from each of these agencies include:

- DHS reported sponsoring Biometric Technology Rallies, which are ongoing industry challenges to develop innovative solutions for biometric collection and matching, including facial recognition. For example, the 2020 Rally focused on the ability of FRT systems to reliably collect or match images of individuals wearing masks. DHS intended this research to improve the technology's ability to recognize individuals without requiring them to remove their protective equipment.
- DOD reported researching new capabilities for RAPIDS, which would support identity verification during online identification card renewal and PIN reset requests.
- DOJ reported conducting applied research on the relationship between skin tone and false match rates in facial recognition algorithms, the capabilities and limitations of current synthetic face detection, such as deepfakes, and the development of software to detect synthetic faces.[29] DOJ also explored the potential benefits of combining FRT systems with trained forensic examiners to achieve better matching performance than by the technology or by humans alone.
- The State Department reported conducting research and development and contributing to international image standards for travel documents. For example, State conducted research on morphing detection and the impact of aging on the accuracy of facial recognition

[28]In our questionnaire, we asked, "In fiscal year 2020, did your agency conduct research and development (R&D) involving facial recognition technologies?"

[29]For more information on deepfakes, see GAO, *Science & Tech Spotlight: Deepfakes*, GAO-20-379SP (Washington, D.C.: Feb. 20, 2020).

algorithms, such as for children's passport photos.[30] State is also developing the ability to match images of individuals against passport images and a repository of known or suspected terrorists using the Personal Identification Secure Comparison and Evaluation System.[31]

Two agencies—Commerce and NSF—conducted or supported FRT-related research more broadly, including for commercial vendors and other agencies. For example, Commerce reported that its National Institute of Standards and Technology performed research to support the development of standards and methods in performance measurement, image quality, testing and evaluating technologies, and interoperability for facial recognition technology. The National Institute of Standards and Technology also conducted research through the Face Recognition Vendor Test program, which most recently released reports quantifying facial recognition accuracy with facemasks using post-COVID-19 algorithms and across demographic effects.[32]

The NSF reported that it awards grants to universities and others to conduct research on facial recognition. Specifically, NSF's Directorate for Computer and Information Science and Engineering supported FRT-related research, including a project assessing how to prevent identifying an individual from facial images used in research, such as recordings of a driver's face during driver behavior studies. Furthermore, NSF supported a program called the Center for Identification Technology Research, in which university partners work with government and industry stakeholders on biometrics, including research on FRT.[33]

Finally, four agencies—DOT, HHS, the Department of Veterans Affairs (VA), and NASA—reported using FRT as a tool to conduct other research. For example, DOT reported that the Federal Railroad Administration used eye tracking to study alertness in train operators.

[30]Face morphing is when, for example, two images of different individuals are combined so that the resulting image could be used as identification for both of them, such as on a passport. Morphing detection attempts to identify these images.

[31]The State Department's Bureau of Counterterrorism offers the Personal Identification Secure Comparison and Evaluation System, or PISCES, for border management under the Terrorist Interdiction Program to foreign partners, and incorporates enhanced screening technologies to ensure those partners are able to protect themselves from attempts by terrorists to enter, transit, or depart their country.

[32]DHS and DOJ have interagency agreements with the National Institute of Standards and Technology for related FRT research and evaluation.

[33]DHS also sponsored the Center for Identification Technology Research.

Like DOT, NASA also reported that it used eye tracking to conduct human factors research.

In addition, VA reported it used eye tracking as part of a clinical research program that treats post-traumatic stress disorder in veterans. Specifically, the eye tracking system evaluates pupil response to evaluate impairment. Similarly, HHS's National Institutes of Health awarded grants for research that use eye tracking as a tool for clinical research. For example, characterizing how children with and without autism spectrum disorder visually followed conversations in videos, among other areas of research.

Four Agencies Reported Other FRT-Related Activities with Nonfederal Entities

According to our analysis of survey responses, four agencies—DHS, DOJ, VA, and State—reported FRT-related activities with nonfederal entities in fiscal year 2020. Specifically, these agencies reported entering into transactions that enabled nonfederal entities to obtain their own FRT.[34] These transactions included agreements with foreign governments and commercial entities, grants, and medical equipment purchases. In addition, DHS was the only agency that reported it regulated an airline's use of FRT in fiscal year 2020.[35]

Transactions with Nonfederal Entities to Obtain FRT

Agreements. Two agencies—DHS and State—reported entering into FRT-related agreements in fiscal year 2020 with foreign governments, and DHS reported having FRT-related agreements with commercial entities. Specifically, DHS entered into agreements, called project arrangements, with two foreign governments—Australia and the United Kingdom—related to the assessment of facial recognition software. The State Department reported transactions with two foreign governments. Specifically, State contracted trainers to instruct Mexican government personnel on how to use previously donated FRT equipment, and it purchased FRT equipment to donate to the Guatemalan government. DHS also had cooperative research and development agreements with two commercial entities focused on making digital identity credentials

[34]In our questionnaire we asked, "In fiscal year 2020, did your agency enter into transactions to enable a nonfederal entity to obtain facial recognition technology for their own uses? In other words, the support (financial or in-kind) would enable nonfederal entities to develop, purchase, or use facial recognition technology for their own uses—not for your agency's use." For the purposes of this questionnaire and report, "transactions" refers to an agency that awarded grants; entered into contracts, leases, or cooperative agreements; provided direct loans or loan guarantees; or entered into any other transactions with nonfederal entities using other transactional authority.

[35]The Transportation Security Administration within the Department of Homeland Security regulated an airline's use of FRT in fiscal year 2020.

(e.g., digital driver's licenses) interoperable with airport checkpoint security systems.

Contract. DHS's U.S. Immigration and Customs Enforcement reported that it awarded a contract to the Lehigh County, Pennsylvania District Attorney's Office to enhance U.S. Immigration and Customs Enforcement's future access to the Gang Intelligence Application, which is a database of transnational gang members and associated information.

Grants. Two agencies—DHS and DOJ—reported awarding FRT-related grants to nonfederal entities. Specifically, DHS's Federal Emergency Management Agency awarded preparedness grants to sustain or build facial recognition and other capabilities, such as intelligence sharing, among state and local law enforcement, emergency management, and other local entities.[36]

DOJ reported it awarded a grant to the Police Foundation for the development of techniques to automate analysis of body-worn camera audio and video data of police and community interactions. For example, these techniques could allow for an evaluation of officers' adherence to principles of procedural justice.

Medical equipment. VA reported two FRT-related transactions for nonfederal entities. Specifically, VA purchased two types of eye tracking equipment for veterans. According to the VA, speech-impaired veterans were provided a prosthetic device that tracks eye movements to assist their use of a computer or tablet for communication.

Regulating Nonfederal Entities' Use of FRT

Of the 24 agencies in our survey, one agency—DHS—reported regulating the use of FRT by other entities in fiscal year 2020.[37] Specifically, the TSA issued security program amendments to aircraft operators that

[36]DHS officials provided a list of the following preparedness grant programs that included "FRT" or "facial recognition" in the project description for awards in fiscal year 2020: Nonprofit Security Grant Program-Urban Area, State Homeland Security Program, and Urban Area Security Initiative.

[37]In our questionnaire, we asked, "In fiscal year 2020, did your agency engage in any regulatory functions over nonfederal entities that use facial recognition technology?" Regulated refers to using regulatory authority over a nonfederal entity to regulate that entity's use of its own FRT. For the purposes of this questionnaire and report, we defined "regulated" as regulatory functions in which the agency engaged, including but not limited to, investigatory and inspections activities, taking enforcement actions, prescribing requirements or guidance, conducting oversight, and maintaining performance standards.

permit the use of FRT to identify passengers checking baggage for transportation on flights, in lieu of the standard passenger identification measures in the applicable TSA-issued security program.[38]

Ten Agencies Plan to Expand Use of FRT, Mostly through Use of New FRT Systems

According to our analysis of survey responses, 10 of the 24 agencies surveyed—USDA, Commerce, DOD, HHS, DHS, Interior, DOJ, State, Treasury, and VA—plan to expand their use of FRT systems in one or more ways through fiscal year 2023.[39] We categorized plans to expand FRT use in three ways: (1) using new FRT systems, (2) evaluating existing FRT systems (e.g., pilot testing), and (3) upgrading existing FRT systems.[40] See table 5 for additional information.

Table 5: Federal Agencies That Reported Plans to Expand Their Use of Facial Recognition Technology (FRT) Systems, through Fiscal Year 2023

Federal Agency	Plan to use new FRT systems	Plan to evaluate FRT systems	Plan to upgrade FRT systems or capabilities
Department of Agriculture	●	⊗	⊗
Department of Commerce	●	⊗	⊗

[38]The TSA responded that it has broad authority to ensure transportation security (See, for example, 49 U.S.C. §§ 114, 44901, 44903), including research and development of new technologies (49 U.S.C. § 44912). Specific to biometrics, Congress authorized the TSA to use "voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation." (Aviation and Transportation Security Act of 2001 (Pub. L. No. 107-71, §109(a)(7), 115 Stat. 597, (2001)), codified at 49 U.S.C. § 114 note.

[39]In our questionnaire, we asked, "Does your agency have plans to begin using facial recognition technology (including upgrading a system to include facial recognition) for internal agency use between fiscal year 2020 and fiscal year 2023? In other words, your agency has not yet begun to use the facial recognition technology, but it has taken steps to begin by fiscal year 2023." For the purposes of this questionnaire and report, by "plans," we meant that the agency has initiated a process to use facial recognition technology, which could include an ongoing acquisition process, a contract with a vendor or another agency, a memorandum of understanding, or a budget request. It did not include hypothetical or exploratory conversations about potential uses of facial recognition technology within the agency. Furthermore, we did not ask agencies to confirm if they were planning to continue using their existing FRT systems beyond fiscal year 2020. However, we included existing FRT systems in the planned use section when an agency reported plans to change the way it will use the FRT system from fiscal year 2020 through fiscal year 2023.

[40]For the purposes of this report, "upgrades" refers to cases where agencies reported adding FRT capabilities to existing systems or to enhance system processes and updating a previously deactivated FRT system. It is not typical system maintenance.

Federal Agency	Plan to use new FRT systems	Plan to evaluate FRT systems	Plan to upgrade FRT systems or capabilities
Department of Defense	●	●	⊗
Department of Health and Human Services	●	⊗	⊗
Department of Homeland Security	●	●	●
Department of the Interior	●	⊗	⊗
Department of Justice	●	⊗	⊗
Department of State	●	⊗	⊗
Department of the Treasury	●	●	⊗
Department of Veterans Affairs	●	⊗	⊗

● Yes

⊗ No

Source: GAO analysis of survey results. | GAO-21-526

Using New FRT Systems

Ten agencies—USDA, Commerce, DOD, HHS, DHS, Interior, DOJ, State, Treasury, and VA—reported plans to use 17 new FRT systems through fiscal year 2023 as shown in table 6.[41] New FRT systems refers to systems that are new to federal agencies, including newly-developed FRT systems and commercial-off-the-shelf systems, and new access to existing FRT systems that agencies did not report using in fiscal year 2020.

According to our analysis of survey results, agencies reported that 13 of the 17 new FRT systems will be owned by federal agencies, and two by local governments. Two agencies reported they plan to access Clearview AI, a commercial system, for the first time.[42]

Table 6: New Facial Recognition Technology (FRT) Systems Federal Agencies Reported they Plan to Use, through Fiscal Year 2023

Agency	Planned Number of Newly Owned and Accessed FRT Systems	Planned Access to FRT Systems Owned by Other Agencies	Purposes
Department of Agriculture	2 systems	• None	• Physical security • Domestic law enforcement
Department of Commerce	1 system	• None	• Physical security

[41]See appendix II for additional information about agency use of FRT systems.

[42]Multiple agencies already accessed Clearview AI in fiscal year 2020 (noted above).

Agency	Planned Number of Newly Owned and Accessed FRT Systems	Planned Access to FRT Systems Owned by Other Agencies	Purposes
Department of Defense	2 systems	• None	• Physical security • Domestic law enforcement • National security and defense
Department of Health and Human Services	1 system	• None	• Domestic law enforcement
Department of Homeland Security	2 systems	• None	• Domestic law enforcement • National security and defense
Department of the Interior	2 systems	• None	• Domestic law enforcement
Department of Justice	2 systems	• None	• Physical security • Border and transportation security
Department of State	1 system	• None	• Border and transportation security
Department of the Treasury	2 systems	• Department of Defense • Department of Homeland Security • Department of Justice	• Domestic law enforcement
Department of Veterans Affairs	2 systems	• None	• Physical security • Domestic law enforcement

Source: GAO analysis of survey results. | GAO-21-526

Note: See appendix II for additional information about agency use of FRT systems.

Use of new federal FRT systems. Nine agencies—USDA, Commerce, DOD, HHS, DHS, DOJ, State, Treasury, and VA—plan to use new federal FRT systems. For example, the U.S. Treasury Inspector General for Tax Administration reported that it purchased an FRT system that can identify facial images of persons of interest who may be involved in criminal activity across multiple investigations in December 2020. The FRT system searches images in an online storage locker, which contains evidence such as photos from seized mobile devices, and will notify investigators of potential matches of individuals linked to other investigations.

The State Department reported plans for a pilot in late 2021, using FRT developed for the Personal Identification Secure Comparison and Evaluation System (PISCES) border management system. State plans to screen individuals against passport images and a repository of suspicious

individuals, such as known and suspected terrorists attempting to travel through partner countries.

New access to existing FRT systems. Three agencies—DOD, Interior, and Treasury—reported plans to access existing FRT systems.[43] For example, DOD's U.S. Air Force Office of Special Investigations reported it began an operational pilot using Clearview AI in June 2020, which supports the agency's counterterrorism, counterintelligence, and criminal investigations. The agency reported it already collects facial images with mobile devices to search national databases and plans to enhance searches by accessing Clearview AI's large repository of facial images from open sources to search for matches.

Evaluating Existing Systems

Three agencies—DHS, DOD, and Treasury—reported plans to conduct new pilot tests or continue evaluating existing FRT systems. Of the four FRT systems these agencies plan to evaluate, federal agencies own three systems, and a commercial vendor owns the other system.

For example, DHS reported plans to initiate a new pilot and continue an ongoing pilot of an existing FRT system. As of March 2021, the TSA is collaborating with U.S. Customs and Border Protection and a commercial airline at the Detroit Metropolitan Wayne County Airport to evaluate the use of biometric technology, including facial recognition, to automate the identity verification process at TSA checkpoints and streamline traveler experience.

In addition, DOD and Treasury reported plans to conduct new pilots of existing FRT systems. For example, DOD plans to conduct a pilot in late fiscal year 2021 of an FRT enhancement to an electronic physical access control FRT system, called Automated Installation Entry, to improve processing and minimize security risks.[44] DOD personnel that volunteer for the new pilot will proceed to the enhanced access control points, which will match their faces against a database of DOD participants.

Upgrading Existing Systems

DHS reported plans to upgrade an existing FRT system and capabilities through fiscal year 2023. In December 2021, DHS plans to replace IDENT, which is its current system for processing and storing biometric data, with the Homeland Advanced Recognition Technology system.

[43]These systems are already used by other agencies.

[44]The U.S. Army purchased the FRT system in fiscal year 2014 to verify individuals seeking access to military installations.

Initially, the Homeland Advanced Recognition Technology system will replace IDENT's current capabilities, to include FRT, with DHS planning additional capabilities in subsequent years.

Agency Comments

We provided a draft of this report to the 24 CFO Act agencies for their review and comment. We received written comments from USAID and SSA that are reprinted in appendices III and IV, respectively. USAID in its written comments did not comment on the content of the report. SSA in its written comments noted that the report was accurate with respect to their experience with facial recognition technologies. We received technical comments from six agencies, which we incorporated as appropriate. We did not receive comments from the Department of the Treasury's offices, but received technical comments from some of its bureaus and components. The remaining 15 agencies informed us that they had no comments.

We are sending copies of this report to the appropriate congressional committees, the heads of the 24 CFO Act agencies, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Candice N. Wright at (202) 512-6888 or wrightc@gao.gov, or Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Candice N. Wright
Director
Science, Technology Assessment, and Analytics

Gretta L. Goodwin
Director
Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

This report identifies and describes (1) how agencies used facial recognition technologies (FRT) in fiscal year 2020, including any FRT-related research and development activities and interactions with nonfederal entities, and (2) how agencies plan to expand their use of FRT through fiscal year 2023.

To obtain the information needed for both objectives, we conducted a survey of the 24 agencies listed in the Chief Financial Officers (CFO) Act of 1990, as amended.[1] These departments and independent agencies (hereafter referred to as agencies) are as follows:

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of the Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Department of the Treasury
- Department of Veterans Affairs
- Agency for International Development
- Environmental Protection Agency
- General Services Administration
- National Aeronautics and Space Administration

[1]The 24 agencies are those identified in the Chief Financial Officers Act of 1990, as amended (31 U.S.C. § 901(b)). This Act does not include many independent agencies and commissions, such as the Office of the Director of National Intelligence or the Central Intelligence Agency, so they were not included in our survey.

- National Science Foundation
- Nuclear Regulatory Commission
- Office of Personnel Management
- Small Business Administration
- Social Security Administration

We administered a questionnaire by email to each of the 24 CFO Act agencies from October 2020 through January 2021.[2] During survey administration, we asked agencies to provide responses for all their components, bureaus, and offices in a consolidated response. We received responses from all 24 agencies.[3]

To develop the questionnaire, we used information from prior GAO reports and early interviews with the agencies to determine the areas of inquiry. For the purposes of our survey and report, we defined facial recognition technology as systems, components, or modules of systems, software applications, or devices with automated facial recognition capabilities, such as face recognition algorithm, hardware, or software. Facial recognition generally refers to facial matching, which includes both verification (one-to-one matching)—to automatically confirm whether a facial image in one photo matches a facial image in a different photo—and identification (one-to-many matching)—to automatically determine whether a facial image has any match in a database or gallery of photos.

Though they are generally considered distinct technologies, we also considered facial analysis—identifying attributes about a person based on their face, such as sex, age, or emotion—and facial detection—determining if a photo or video contains a face— to be facial recognition technologies.

We also determined that facial recognition technology could be used for a variety of applications, such as verifying the identity claimed by an individual or controlling access to buildings or computers. We grouped these applications into seven purposes based on prior GAO reports, such as those on law enforcement, transportation security, and commercial

[2]These dates cover the initial response for all 24 agencies. It does not include updated or additional responses received because of follow-up activities.

[3]We also asked agencies to include the 24 Offices of Inspectors General and the Treasury Inspector General for Tax Administration in their response.

uses of facial recognition, and a review of relevant literature.[4] We asked agencies to include all uses of facial recognition technology and identify which purpose(s) described their uses. The purposes are: (1) physical security; (2) digital access or cybersecurity; (3) domestic law enforcement; (4) border and transportation security; (5) national security and defense; (6) medical assessment; and (7) other purposes not already listed.

Finally, we met with both agency liaisons, who would be administering the survey to their respective agencies, and subject matter experts, who helped ensure respondents clearly understood specific questions.

We used a questionnaire with two sections: (1) a Main Questionnaire, and (2) five Attachments that followed up on positive responses in the Main Questionnaire. For agencies that had activities or planned activities related to facial recognition technology in the Main Questionnaire, we asked that, as appropriate, the agencies complete an Attachment that covered the following areas:

1. owned or accessed, including tested, facial recognition technology in fiscal year 2020;
2. plans to own or access, including testing, facial recognition technology through fiscal year 2023;
3. research and development conducted or supported in fiscal year 2020;
4. any transactions the agency entered into with nonfederal entities for that entity to obtain facial recognition technology in fiscal year 2020; and

[4]GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016); *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); *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015); and *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522 (Washington, D.C.: July 13, 2020).

5. any regulation of a nonfederal entity's use of its own facial recognition technology.[5]

We used these timeframes because fiscal year 2020 was the most recent fiscal year for which information was available when we issued our questionnaire and through fiscal year 2023 for planned systems, because agencies were most likely to have information covering this timeframe, such as in strategic plans.

Each of the Attachments had detailed questions, such as a description of the activity, how the agency used the technology, including the purpose(s) and obligations related to the activity. For how agencies used facial recognition technology, we asked whether the federal agency owned or accessed it directly (e.g., logging into a system) or via a third party (e.g., asking another entity to run the search on its behalf). For example, we asked the name of the technology and the entity that owned it, including how best to describe that entity (e.g., federal, state, tribal, or local). For obligations, we asked the agency to provide the amount obligated in fiscal year 2020 and whether it was disbursed. If the agency could not provide an obligated amount we asked for a range or the reason why an agency did not know (e.g., facial recognition was a small part of a larger, biometric system and was not specifically tracked). Finally, we also asked if agencies had classified systems.[6]

After determining the areas of inquiry, we conducted pretests with five agencies to test the questionnaire's applicability to all agencies and a variety of facial recognition technology uses, and revised the questionnaire based on those pretests. We selected agencies for pretests based on information provided during initial meetings with agency officials to capture a variety of facial recognition technologies and purposes, in order to test different parts of our questionnaire. For example, National Aeronautics and Space Administration officials told us they used facial recognition technology for research and development, so we focused the pretest on the research and development questions with that agency. On

[5]Regulated refers to using regulatory authority over a nonfederal entity to regulate that entity's use of its own FRT. For the purposes of our questionnaire, we defined "regulated" as regulatory functions in which the agency engaged, including, but not limited to, investigatory and inspections activities, taking enforcement actions, prescribing requirements or guidance, conducting oversight, and maintaining performance standards.

[6]This report only discusses unclassified systems.

the other hand, Department of Defense officials were able to pretest the majority of the questions, so we met with them multiple times.

Once the design process was completed, we administered the questionnaire by email to agency liaisons, or their designees, for an agency-level response about facial recognition technology use. To do this, we instructed the liaisons to provide the agency-level response in the Main Questionnaire. We asked the liaisons to disseminate the Attachments to relevant and knowledgeable facial recognition technology subject matter experts at the agency, component, bureau, or office levels, which the liaisons would consolidate into the Main Questionnaire and return it and all the Attachments to us.[7] We provided detailed instructions in writing and in the questionnaire itself. We also followed up by email and phone, when appropriate, to ensure that the agency liaisons received the questionnaire and to ask if they had any questions about it. Once the liaison determined their agency's survey responses were complete, we asked the liaison to total the Attachments and enter the total number of completed Attachments on the Main Questionnaire to ensure we received all of the expected agency Attachments in their survey responses.

When agencies submitted their survey responses, we conducted an initial review for completeness, inconsistencies, or logical errors within the responses. We asked agencies to re-submit or clarify responses if necessary.

Because we surveyed and obtained responses from all 24 agencies in the population defined by our scope, the summary results describing this group are not subject to errors from sampling and nonresponse. However, the practical difficulties of conducting any survey may introduce other errors, such as:

- Difficulties in how a particular question is interpreted by respondents. For example, some agencies were not sure which Attachment to fill out or completed one for an activity that did not meet our criteria, so we followed up with them to determine which was the most appropriate in some cases. Furthermore, as part of our analysis of agency responses, we determined that some information could have been included correctly in more than one Attachment. In one case, for

[7]For example, the Departments of the Treasury and Defense did not consolidate their responses. We informed them that we would take the responses provided by these agencies and consolidate them on behalf of the agency and provide them with an opportunity to review this information in the report.

agencies that reported using facial recognition technology, such as eye tracking, as part of research unrelated to facial recognition for other purposes, we determined that those technologies would only be reported as research and development activities, even if some agencies reported it as a system "used." In another case, for agencies that filled out the regulatory attachment, we excluded responses that did not meet both of our criteria: (1) that an agency had authority over a nonfederal entity's use of facial recognition technology and (2) actually used that authority to regulate the nonfederal entity's use of facial recognition technology.

- Sources of information that are available to respondents differ across agencies. For example, one agency expressed concern to us about their ability to provide a comprehensive response that included every accessed facial recognition technology because they did not track this information. We asked that agencies provide what they could, but to focus their efforts on facial recognition technology access that had a memorandum of agreement or understanding. Furthermore, we relied on the agency liaisons to provide Attachments to subject matter experts on facial recognition technology use within their agencies. We provided suggestions to these liaisons of possible areas where facial recognition technology could be used, such as security and information technology offices, to ensure that the agency-level responses were comprehensive.

  To help corroborate the information agencies provided in the questionnaire, we conducted a search of government contracting information and reviewed information provided for prior reports. Specifically, we conducted a search of several terms, such as "facial recognition," "FRT," and known vendor names, in the Federal Procurement Data System Next Generation and Grants.gov databases. We used two analysts to independently review and determine if a result was related to FRT in our scope, such as excluding non-human related results and other technologies. We used this list to review each agency's responses for completeness. When we discovered discrepancies, we followed up with the agency as appropriate to change their response or fill out new Attachments from the questionnaire.

  Furthermore, we reviewed responses from a survey of federal law enforcement use of facial recognition technology to determine if there

were inconsistencies in responses to our survey.[8] If there were, we requested clarification of the agency-provided information, such as system descriptions, in interviews and multiple rounds of follow up (i.e., information requests), to those agencies. For example, if an agency filled out an Attachment, but indicated "no" on the Main Questionnaire for the applicable question related to the Attachment, we determined that was an incorrect response on the Main Questionnaire.

- How we processed and analyzed the responses we received can influence the accuracy of the survey results. For example, we consolidated some agency responses, such as the Department of Defense. We independently verified the consolidated information internally and presented it to those agencies prior to issuing the report.

We took steps in the development of the questionnaire, such as pretesting, data collection, and data analysis, including multiple rounds of follow up through interviews and information requests as noted above to minimize these potential errors and to help ensure the accuracy of the answers obtained. Based on these quality assurance and control actions we determined that for the purposes of this report, the information provided is an accurate and valid representation of the extent of facial recognition use across the 24 CFO Act agencies.

We conducted this performance audit from April 2020 through August 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

[8]For more information about the survey of federal law enforcement's use of facial recognition technology, see GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Washington, D.C., June 3, 2021).

Appendix II: Summaries of Selected Federal Agencies' Facial Recognition Technology Activities

This appendix provides summaries of those Chief Financial Officers Act agencies that reported facial recognition technology (FRT) activities in fiscal year 2020, and planned FRT systems through fiscal year 2023. We asked the following questions of each agency, which correspond to the responses provided in each agency's summary:

1. "At any point in fiscal year 2020, did your agency use facial recognition technology for any of the following purposes? By 'use,' we mean your agency: (1) owned and/or operated facial recognition technology for internal agency purposes, (2) accessed another federal or nonfederal entity's (including local government or private company) facial recognition technology under an agreement or arrangement as part of an agency program or activity, or (3) tested facial recognition technology as part of a pilot, proof of concept, trial, or evaluation for potential agency use."

2. "Does your agency have plans to begin using facial recognition technology (including upgrading a system to include facial recognition) for internal agency use between fiscal year 2020 and fiscal year 2023? In other words, your agency has not yet begun to use the facial recognition technology, but it has taken steps to begin by fiscal year 2023. By 'plans,' we mean your agency has initiated a process to use facial recognition technology, which could include an ongoing acquisition process, a contract with a vendor or another agency, a memorandum of understanding, or a budget request. Do not include hypothetical or exploratory conversations about potential uses of facial recognition technology within your agency."

3. "In fiscal year 2020, did your agency conduct research and development (R&D) involving facial recognition technologies? This could include funding another entity to conduct R&D on your agency's behalf. R&D includes basic research, applied research, or experimental development (technology readiness levels 1-6). R&D could include developing facial recognition algorithms or evaluating existing algorithms."

4. "In fiscal year 2020, did your agency enter into transactions to enable a nonfederal entity to obtain facial recognition technology for their own uses? In other words, the support (financial or in-kind) would enable nonfederal entities to develop, purchase, or use facial recognition technology for their own uses—not for your agency's use. By 'transactions,' we mean your agency awarded grants, entered into contracts, leases, or cooperative agreements, provided direct loans or

loan guarantees, or entered into any other transactions using other transactional authority."

5. "In fiscal year 2020, did your agency engage in any regulatory functions over nonfederal entities that use facial recognition technology? For our purposes, 'regulatory functions' includes, but is not limited to, investigatory and inspections activities, taking enforcement actions, prescribing requirements or guidance, conducting oversight, and maintaining performance standards."

Specifically, we provide summaries for the following 16 agencies:

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of the Interior
- Department of Justice
- Department of State
- Department of Transportation
- Department of the Treasury
- Department of Veterans Affairs
- General Services Administration
- National Aeronautics and Space Administration
- National Science Foundation
- Social Security Administration

The information in these summaries is from survey responses or requests for more information from the agencies. We present details on FRT systems reported by agencies that own their FRT systems or access the FRT systems of other government entities, including federal and nonfederal governments, and commercial facial recognition service providers. Agencies can have direct access to an FRT system, such as by logging into the system, or indirect access, such as by requesting a

state government (i.e., a third party) run a facial recognition search on behalf of the agency.

We also present obligations for FRT systems as applicable. Each agency provided information on obligations in its survey response. However, we are presenting obligations data for informational purposes only, because we did not corroborate it through other means, such as document requests, and some agencies reported facial recognition obligations as part of a larger biometric system. We do not include information on obligations related to unlocking smartphones or tablets because agencies reported obligations of (1) none or free, because the smartphones were included in the service contract, (2) the cost of individual devices, or (3) the total of all purchased smartphones. [1] The facial recognition feature of the smartphones was included with the phones, so there is no specific obligation.

The Department of Education, the Department of Housing and Urban Development, the Nuclear Regulatory Commission, and the Small Business Administration do not have summaries because they reported they had no FRT activities in fiscal year 2020 and no plans to have FRT activities through fiscal year 2023. The Department of Labor, the U.S. Agency for International Development, the Environmental Protection Agency, and the Office of Personnel Management do not have summaries because they reported that they only use facial recognition to unlock smartphones or tablets.

[1]The 14 agencies that reported using facial recognition to unlock smartphones or tablets are the Departments of Agriculture, Commerce, Homeland Security, Energy, Justice, Health and Human Services, the Interior, the Treasury, Veterans Affairs, the Environmental Protection Agency, the National Aeronautics and Space Administration, the National Science Foundation, the Office of Personnel Management, and the U.S. Agency for International Development.

The U.S. Department of Agriculture (USDA) reported that it did not have facial recognition technology (FRT) activities in fiscal year 2020. However, it reported plans to use a new FRT system through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

None reported.

FRT System Obligations in Fiscal Year 2020

None reported.

Research & Development in Fiscal Year 2020

None reported.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

USDA reported it plans to use two other FRT systems through fiscal year 2023, both of them for physical security purposes and one of them also for domestic law enforcement purposes.

U.S. Department of Agriculture (USDA) Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New federal FRT systems		
Agricultural Research Service IDEMIA VisionPass	IDEMIA VisionPass is a facial recognition device that will be used to verify the identity of personnel for access within secure areas of a facility.	USDA plans to use the technology beginning in fiscal year 2022.
Office of Safety, Security, and Protection Avigilon Control Center	The Avigilon Control Center facial recognition software will assist with accelerating response times by identifying individuals of interest based on secure watch lists.	USDA plans for the facial recognition software to be operational by fiscal year 2022, if funding is approved.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to USDA, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Agricultural Marketing Service
- Animal and Plant Health Inspection Service
- Economic Research Service
- Farm Service Agency
- Food and Nutrition Service
- Food Safety and Inspection Service
- Foreign Agricultural Service
- Forest Service
- National Agricultural Statistics Service
- National Institute of Food and Agriculture
- Natural Resources Conservation Service
- Office of the Chief Information Officer
- Office of the Chief Economist
- Office of the General Counsel
- Office of the Inspector General
- Office of Partnerships & Public Engagement
- Office of the Assistant Secretary for Civil Rights
- Office of Tribal Relations
- Office of Homeland Security
- Office of Operations
- Risk Management Agency
- Rural Development
- Rural Utilities Service
- Rural Housing Service
- Rural Business-Cooperative Service

The Department of Commerce reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, Commerce reported owning one FRT system and conducting FRT-related research and development (R&D) in fiscal year 2020. Commerce also reported plans to use one other FRT system through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

Commerce reported it owned one FRT system in fiscal year 2020, for physical security purposes.

Department of Commerce Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other Commerce and federal users
Commerce-owned FRT system		
Office of Chief Information Officer TYCO StoneLock infrared biometric facial recognition device	This system uses FRT to control access to a secure data center by infrared facial matching as part of its three-factor authentication process. Commerce reported that it did not continue to use the system after fiscal year 2020.	• None

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

Commerce reported it did not obligate funds in fiscal year 2020, because the technology was purchased in 2016.

Research & Development in Fiscal Year 2020

Commerce reported conducting FRT-related R&D, specifically by the National Institute of Standards and Technology (NIST), to support federal agencies and commercial vendors in fiscal year 2020, as follows:

- NIST supported the development of standards and methods in performance measurement, image quality, testing and evaluating technologies, and interoperability for FRT.
- NIST also runs the Facial Recognition Vendor Test program, which evaluates the performance of various facial recognition algorithms against a host of performance metrics, such as accuracy and speed in facial identification/matching, system performance across different demographics, and, more recently, facial detection of individuals wearing masks due to COVID-19.

Commerce reported that while there was no FRT-specific funding, it obligated approximately $500,000 in fiscal year 2020 for biometrics research and standards work at NIST.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

Commerce reported plans to use one other FRT system through fiscal year 2023, for physical security purposes.

Department of Commerce Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New federal FRT system		
Office of the Chief Information Officer Continuity of Operations Data Center access control system	This system uses infrared facial matching to control access to a secure data center as part of a three-factor authentication process.	Commerce is constructing a data center with this physical security system. Commerce expects to move to the new data center by August 2021.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to Commerce, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Bureau of Economic Analysis
- Bureau of Industry and Security
- U.S. Census Bureau
- Economic Development Administration
- Office of the Under Secretary for Economic Affairs
- International Trade Administration
- Minority Business Development Agency
- National Oceanic and Atmospheric Administration
- National Technical Information Service
- National Telecommunications and Information Administration
- Office of the Inspector General
- Office of the Secretary
- U.S. Patent and Trademark Office

The Department of Defense (DOD) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, DOD reported using nine FRT systems and conducting research and development (R&D). DOD also reported plans to use three other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

DOD reported it used nine FRT systems in fiscal year 2020, including seven owned by the department and two systems owned by other entities that DOD accessed. Of those nine FRT systems, six are for domestic law enforcement, three are for physical security, five are for national security and defense, and one is for identification card enrollment purposes. Some of these systems are used for multiple purposes.

Department of Defense (DOD) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other DOD and federal users
DOD-owned FRT systems		
U.S. Army Department of Defense Automated Biometric Identification System (DOD ABIS)	DOD ABIS contains a database of military-collected biometrics of foreign nationals, including faces. It is used to identify threat actors related to terrorism or counterintelligence as well as to research information about a person of interest or identify an individual for an investigative lead.	• DOD (multiple components) • Department of Homeland Security • Department of Justice • Department of State
Defense Manpower Data Center Defense Facial Comparison Tool	The Defense Facial Comparison Tool is used to compare a law enforcement probe photo to a DOD captured photo to identify or verify DOD affiliated individuals.	• DOD (U.S. Navy and U.S. Air Force)
Defense Manpower Data Center Real-Time Automated Personnel Identification System (RAPIDS)	RAPIDS is DOD's enterprise tool for identification card issuance. It uses facial detection to ensure the consistent size of a picture printed on the DOD identification card, during identification card issuance.	• DOD (all components) • Other agencies that issue these identification cards (e.g., the Uniformed Services)
U.S. Navy TacID Guard Dog	TacID Guard Dog is used to monitor camera feeds of individuals seeking access to DOD facilities for possible matches to a watchlist of potential threats.	• None
Pentagon Force Protection Agency M.C. Dean access control device	The device uses FRT to control access to the Pentagon Force Protection Agency door by verifying the identity of authorized individuals.	• DOD (U.S. Army)
U.S. Air Force InCadence Ares Javelin+	Javelin+ is biometrics software installed on mobile devices. The FRT system collects facial images from the devices and submits them to DOD's ABIS to identify an individual in a criminal investigation. This FRT system also performs immediate facial, fingerprint, and iris matching to individuals on watch lists.	• None

U.S. Navy Facial Automated Biometric Identification System (FABIS) Mobile	FABIS Mobile is an FRT phone application that can hold a watchlist. DOD personnel use it during public events, such as airshows, to take photos of individuals who act erratically or suspiciously to determine if they are a potential match to the watchlist. If they are a match, then other biometrics may be taken to verify the individual's identity; if they do not match, DOD personnel send the photo for a manual comparison.	• None
Accessed federal FRT systems		**DOD users**
Department of Justice Next Generation Identification Interstate Photo System (NGI IPS)	NGI IPS can be used by DOD personnel to identify suspected terrorists or for counterintelligence. For example, if an individual is identified as a potential threat actor, DOD may forward the request for a search through NGI IPS.	
Department of Homeland Security Automated Biometric Identification System (IDENT)	IDENT can be used to verify an individual's identity, determine whether an individual in two separate photos is the same person, and compare a probe photo against images stored in IDENT to create a list of potential matches. For example, if an individual is identified by DOD as a potential threat actor, DOD may forward the request for a search through IDENT.	

Source: GAO analysis of survey results. | GAO-21-526

Note: DOD components that reported classified systems not described above, include U.S. Central Command, Defense Intelligence Agency, U.S. European Command, U.S. Indo-Pacific Command, and U.S. Special Operations Command.

FRT System Obligations in Fiscal Year 2020

DOD reported obligating funds to operate its own FRT systems in fiscal year 2020.

- DOD reported obligating funds for four of the seven FRT systems it owned in fiscal year 2020.
  - DOD reported obligating about $3.6 million for DOD ABIS of which a portion is used for facial recognition, about $100,000 for TacID Guard Dog, $865,000 for the Defense Facial Comparison Tool, and $80,000 for FABIS Mobile.
  - DOD did not report obligating funds for Javelin+ or the facial detection portion of RAPIDS, noting that the specific obligation for the FRT portion of that system is unknown because it was included as part of many changes to the RAPIDS system in fiscal year 2020. DOD also reported it obligated no funds for the M.C. Dean access control device, because it was purchased prior to fiscal year 2020.
- DOD reported it did not obligate funds for the two FRT systems it accessed in fiscal year 2020, because federal partners provided them at no cost.

Research & Development in Fiscal Year 2020

DOD reported conducting FRT-related R&D to support its mission needs. For example, DOD reported researching new capabilities for RAPIDS, which would support identity verification during online identification card renewal and personal identification number reset requests.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

DOD reported it plans to use three other FRT systems through fiscal year 2023. Specifically, of those three FRT systems, it plans to use two for physical security, one for national security and defense, and one for domestic law enforcement. Of these, one system will be used for multiple purposes.

Department of Defense (DOD) Recognition Technology (FRT) Systems Plans for Facial through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New federal FRT system		
Defense Advanced Research Projects Agency (DARPA) Visitor Welcome System	DARPA plans to use this FRT to pull a visitor's record automatically, if they have previously been to their Visitor Welcome Center. It will be used to expedite visitor processing, while reducing personnel data entry task errors and duplication.	As of May 2020, DARPA is seeking a license to the algorithm through the U.S. Army.
New access to commercial FRT system		
U.S. Air Force Clearview AI	The U.S. Air Force plans to collect facial images with mobile biometric devices, including phones, to compare against Clearview AI's repository of facial images from open sources for matching individuals.	The U.S. Air Force plans to evaluate the product as part of an operational pilot in June 2020.
Evaluation of federal FRT system		
U.S. Army Automated Installation Entry	The U.S. Army's FRT pilot at Redstone Arsenal performs digitized photo matching in real time at automated access control points using registered Automated Installation Entry system volunteers. It is intended to improve the access vetting process speed and reduce security risks.	The U.S. Army began the pilot in the second quarter of fiscal year 2021.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to DOD, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- U.S. Transportation Command
- Department of Defense Chief Information Officer
- Department of Defense Office of the Inspector General

The Department of Energy (DOE) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, DOE reported using one FRT system. DOE reported it does not plan to use FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

DOE reported it owned one FRT system in fiscal year 2020 for physical security purposes.

Department of Energy (DOE) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other DOE and federal users
DOE-owned FRT system		
National Nuclear Security Administration TacID Guard Dog	TacID Guard Dog performs facial matching and facial detection from live video. DOE uses TacID Guard Dog to monitor entry and exit from controlled locations for personnel accountability and to log individuals' arrivals at an evacuation point.	• None

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

DOE reported it purchased TacID Guard Dog in December 2019, and obligated $150,000 for testing the FRT system during fiscal year 2020.

Research & Development in Fiscal Year 2020

None reported.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

None reported.

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to DOE, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Office of the Chief Information Officer
- Office of the Inspector General
- Office of Science, including National Laboratories

The Department of Health and Human Services (HHS) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, HHS reported using four FRT systems and conducting research and development (R&D). HHS reported plans to expand its use of other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

HHS reported it owned three FRT systems and accessed one commercial FRT system in fiscal year 2020. Of those four FRT systems, one was for digital access, one for physical security, and three were for domestic law enforcement purposes. One of these systems was used for multiple purposes.

Department of Health and Human Services (HHS) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other HHS and federal users
HHS-owned FRT systems		
Centers for Disease Control and Prevention (CDC) AnyVision	AnyVision allows real time facial matching from security camera videos and images. CDC piloted using this system to supplement the manual review and memorization of watchlist faces by security guards at their facilities.	• None
Centers for Medicare and Medicaid Services (CMS) Laptop unlocking	This FRT system allows laptop users that have an appropriate camera to use FRT to unlock their laptop. CMS conducted a small pilot of less than 20 participants using this feature on their laptops.	• None
Office of the Inspector General (OIG) Griffeye Digital Investigate Pro	Griffeye Digital Investigate Pro uses FRT to support automated analysis of digital video and images. The OIG used the system in support of investigations involving child exploitation, child sexual assault, and trafficking to locate or identify victims.	• None
Accessed commercial FRT system		**HHS users**
Clearview AI	Clearview AI is a facial image matching software system that operates as an internet search engine for faces using publicly available images, such as from social media. The OIG conducted an evaluation of the system in an attempt to identify unknown subjects of criminal investigation.	• OIG

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

HHS reported obligating funds for two of the three FRT systems it owned in fiscal year 2020.

- HHS reported obligating $1,590 for Griffeye Digital Investigate Pro and $126,896 for AnyVision. HHS reported it obligated no funds for the pilot using facial recognition to unlock laptops because the feature was included with the operating system.

- HHS reported it obligated no funds for its access of Clearview AI, because it was a free trial to evaluate the system.

Research & Development in Fiscal Year 2020

HHS supported research involving facial analysis technology, for purposes other than facial matching. For example, HHS's National Institutes of Health awarded grants for research that use eye tracking as a tool for clinical research, such as characterizing where children with and without autism spectrum disorder looked while following conversations in videos. NIH does not specifically report dollar amounts tied to research eye tracking technology.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

HHS reported it plans to use one other FRT system through fiscal year 2023 for domestic law enforcement purposes.

Department of Health and Human Services (HHS) Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT System	Description of system use	Planned New Use Status
New federal FRT system		
Office of the Inspector General Vintra	Vintra will be used to search surveillance video for investigator-defined actions and objects, such as directional movement, vehicles, or people. The system does not maintain a database of known users but may be able to match a submitted image to an image on the surveillance video.	HHS has tested the system, established security protocols and plans to begin operational usage of Vintra by the end of May 2021.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to HHS, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Administration for Children and Families
- Administration for Community Living
- Agency for Healthcare Research and Quality
- Agency for Toxic Substances and Disease Registry
- Food and Drug Administration
- Health Resources and Services Administration
- Indian Health Service
- Substance Abuse and Mental Health Services Administration

The Department of Homeland Security (DHS) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, DHS reported owning four FRT systems and accessing three federal FRT systems, FRT systems in 17 states and five localities, and two commercial FRT systems. DHS also reported conducting research and development (R&D) related to FRT, entering into transactions with nonfederal entities for FRT, and regulating nonfederal entities use of FRT. DHS also reported it plans to use five other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

DHS owned four federal FRT systems and accessed multiple systems owned by other entities. DHS used four FRT systems for domestic law enforcement, six for border and transportation security, and four for national security and defense purposes. Some of these systems were used for multiple purposes. DHS had access to at least 24 state, local, and commercial FRT systems for domestic law enforcement, for border and transportation security, and for national security and defense purposes.

Department of Homeland Security (DHS) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other DHS and federal users
DHS-owned FRT systems		
U.S. Customs and Border Protection Automated Targeting System (ATS)	U.S. Customs and Border Protection uses ATS's FRT for the following populations: (1) individuals seeking to enter or exit the United States whose names appear on a flight or vessel manifests, or voluntary manifests submitted by bus or rail manifest ("manifested travelers"); (2) individuals applying for CBP programs facilitating travel to the United States, and (3) subjects of interest who require additional research and analysis. It matches photos for these three populations against a predetermined gallery of photos associated with derogatory information.	• Department of Justice • Department of State
U.S. Customs and Border Protection Traveler Verification Service (TVS)	TVS uses facial recognition to verify traveler identities upon arrival at or departure from ports of entry. TVS compares a live photo of a traveler against a gallery of photos (e.g., passport photos) in DHS databases.	• DHS (Transportation Security Administration)
Office of Biometric Identity Management Automated Biometric Identification System (IDENT)	IDENT offers facial recognition services to partners to verify an individual's identity, determine whether an individual in two separate photos is the same, and compare a probe photo against images stored in IDENT for potential matches.	• DHS (all components) • Department of Justice • Department of Defense
Transportation Security Administration Self-Service Version of Credential Authentication Technology with Camera (CAT-2) and AutoCat[a]	CAT-2 machines provide facial matching services to assist with identity verification of travelers by capturing live images at airport checkpoints. AutoCat is an electronic gate version of CAT-2.	• DHS (Science and Technology Directorate)

Accessed federal FRT systems		DHS users
Department of Defense Automated Biometric Identification System (DOD ABIS)	DHS uses DOD ABIS's facial recognition to identify foreign nationals connected to a national security investigation or to a known terrorist organization.	• U.S. Immigration and Customs Enforcement
Department of Justice Next Generation Identification Interstate Photo System (NGI IPS)	DHS uses NGI IPS to identify individuals of interest. Specifically, U.S. Customs and Border Protection submits probe photos via ATS to IDENT and are forwarded to NGI IPS. NGI IPS returns a list of potential matching photos.	• Office of Biometric Identity Management • U.S. Customs and Border Protection
Department of State Integrated Biometric System (IBS)	DHS uses IBS to identify visa applicants for travel documents and individuals involved in identity theft and benefit fraud investigations. DHS employees have direct and indirect access to IBS—performing facial recognition searches in IBS while others submit photos for matching from apprehensions and bookings, among others.	• U.S. Citizenship and Immigration Services • U.S. Customs and Border Protection • U.S. Immigration and Customs Enforcement
Accessed state and local FRT systems		**DHS users**
15 states: Alabama, Arizona, Delaware, Indiana, Kansas, Kentucky, Michigan, Mississippi, Missouri, Nebraska, North Dakota, South Dakota, Utah, Virginia, and West Virginia 4 localities: Chicago, Greater Cincinnati, Delaware Valley, Southeast Florida	DHS's Homeland Security Information Network (HSIN) is a system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international, and private sector partners. HSIN contains a mechanism to request third party facial recognition searches through the listed state and local entities, such as fusion centers.	• U.S. Customs and Border Protection • U.S. Immigration and Customs Enforcement
Michigan Law Enforcement Information Network (MLEIN)	DHS uses MLEIN to identify individuals involved in a crime. DHS submits U.S. Border Patrol apprehension photos and others to the Statewide Network of Agency Photos.	• U.S. Customs and Border Protection
New York State Intelligence Center Photo Imaging Mugshot System (PIMS)	DHS uses PIMS to identify unknown individuals of interest in state and federal cases, including individuals who have been deported and re-entered the country. DHS has direct access to PIMS through Border Patrol Agents working at the New York State Intelligence Center.	• U.S. Customs and Border Protection
Ohio Law Enforcement Gateway (OHLEG)	DHS uses OHLEG to identify individuals involved in a crime. DHS submits photos, such as U.S. Border Patrol apprehension photos.	• U.S. Customs and Border Protection
Pinellas County Face Analysis Comparison and Examination System (FACES)	DHS uses FACES to identify unknown individuals to support operations, criminal investigations, and administrative cases. DHS submits photos to the Pinellas County Sheriff's Office.	• U.S. Customs and Border Protection
Accessed commercial FRT systems		**DHS users**
Clearview AI	DHS uses Clearview AI to identify unknown individuals of interest in state, federal, and international cases, such as child exploitation cases. DHS may submit photos (e.g., surveillance photos) or receive requests to match photos against the Clearview AI database.	• U.S. Customs and Border Protection • U.S. Immigration and Customs Enforcement • U.S. Secret Service
Vigilant Solutions	DHS uses Vigilant Solutions to identify individuals involved in a crime and submits photos for matching.	• U.S. Customs and Border Protection

Source: GAO analysis of survey results. | GAO-21-526
Note: DHS also reported using classified systems.
[a]This system was only tested and not deployed.

FRT System Obligations in Fiscal Year 2020

DHS reported obligating funds to operate its own FRT systems or access other ones, including state and commercial systems, in fiscal year 2020.

- DHS reported obligating funds for three of the four FRT systems it owns in fiscal year 2020. Specifically, DHS reported obligating $7.96 million for the annual maintenance cost of the license for IDENT, $61.5 million for TVS, and $2.5 million for CAT-2. DHS reported it obligated no funds for ATS, because ATS is funded through the license for IDENT.
- DHS reported obligating funds for two FRT systems it accessed in fiscal year 2020. Specifically, DHS reported obligating about $23.67 million for HSIN and $31,592 to fund approximately seven licenses under its contract for access to the Michigan State Police's MLEIN. For the remaining federal, state, and local FRT systems it accessed,
  - DHS reported obligating no funds to access three federal FRT systems—DOD ABIS, NGI IPS, and IBS—because those systems are funded by DOD, DOJ, and State, respectively.
  - DHS reported obligating no funds for state and local FRT systems, because they were accessed at no cost through respective state and local owners.
- DHS reported obligating funds to access one of two commercial FRT systems in fiscal year 2020. Specifically, DHS' Immigration and Customs Enforcement reported obligating $214,000 to purchase Clearview AI licenses, while Secret Service has not yet made a decision to purchase services after conducting a pilot in April 2019. U.S. Customs and Border Protection accessed Clearview AI at no cost through an agent stationed at the New York State Intelligence Center. Finally, DHS reported it has limited access to Vigilant Solutions at no cost.

Research & Development in Fiscal Year 2020

DHS reported conducting R&D for testing on one FRT system and additional research to improve face detection, analysis, and matching capabilities:

- The Transportation Security Administration reported obligating over $2.17 million for independent testing and planning for CAT-2. The tests will validate facial matching performance through a series of pilots of the Transportation Security Administration's specific use case at checkpoints.
- The Science and Technology Directorate reported obligating $1.2 million to sponsor Biometric Technology Rallies, which are ongoing industry events with challenges to develop innovative solutions for biometric collection and matching, including facial recognition, and the reliability of collecting and matching information on travelers wearing masks during COVID-19.
- The Science and Technology Directorate and Office of Biometric Identity Management reported obligating about $553,000 for National Science Foundation's Center for Identification Technology Research university grants. Specifically, S&T sponsors R&D and awards grants to university partners that focus on work related to face detection, analysis, and matching. OBIM sponsors R&D with a portion of work including fingerprint matching, presentation attack detection, and matching of biometrics from juveniles.
- The Science and Technology Directorate reported obligating $300,000 to sponsor R&D on face detection, analysis, and matching through its interagency agreement with the National Institute of Standards and Technology.

Transactions with Nonfederal Entities in Fiscal Year 2020

DHS reported that it entered into agreements with foreign governments and private entities, and awarded grants to local governments and other entities:

- The Transportation Security Administration reported it had a Cooperative Research and Development Agreement with a technology company and an air carrier focused on ways to make mobile digital identity credentials (e.g., mobile digital driver's licenses) interoperable with Transportation Security Administration's checkpoint security systems.

- The Science and Technology Directorate entered into project arrangements with two foreign governments—Australia and the United Kingdom—related to the assessment of face recognition software.
- DHS awarded a contract to the Lehigh County, Pennsylvania District Attorney's Office to enhance the U.S. Immigration and Customs Enforcement Homeland Security Investigation's future access to the Gang Intelligence Application. DHS reported spending about $200,000 on the application in fiscal year 2020.
- The Federal Emergency Management Agency reported it obligated about $1.25 million across several grants that included facial recognition, such as equipment for emergency responders and state and local law enforcement.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

DHS reported regulated a nonfederal entity's use of FRT. Specifically, the Transportation Security Administration issued security program amendments to Delta Air Lines to permit the use of facial identification technology to identify passengers checking baggage for air transportation.

Planned Use of FRT Systems through Fiscal Year 2023

DHS reported it plans to use five other FRT systems through fiscal year 2023. Of those five FRT systems, three will be used for border and transportation security, two will be used for national security and defense, and two will be used for domestic law enforcement purposes. Some of these systems will be used for multiple purposes.

Department of Homeland Security (DHS) Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New access to local FRT system		
Lehigh County, Pennsylvania District Attorney's Office Gang Intelligence Application	U.S. Immigration and Customs Enforcement plans to develop facial recognition access to its data in an automated criminal justice information system.	U.S. Immigration and Customs Enforcement is working with the Lehigh County District Attorney's Office to complete access by May 2021.
Evaluation of federal FRT system		
U.S. Customs and Border Protection Traveler Verification Service (TVS)	The Transportation Security Administration plans to initiate a new pilot of U.S. Customs and Border Protection's TVS to evaluate use of biometric technology, including facial recognition, to automate identity verification at checkpoints and modernize screening.	The Transportation Security Administration began a pilot at the Detroit Metropolitan Wayne County Airport in March 2021 with U.S. Customs and Border Protection.

Department of Homeland Security (DHS) Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023		
FRT system	**Description of system use**	**Planned new use status**
Transportation Security Administration Credential Authentication Technology with Camera System (CAT-2) and AutoCAT	The Transportation Security Administration plans to test this technology to automate identity verification at checkpoints and modernize screening of travelers.	The Transportation Security Administration began demonstrating CAT-2 at Ronald Regan Washington National Airport in August 2020. In March 2021, it started field site testing of CAT-2 at additional airport checkpoints to identify, evaluate, and mitigate system performance issues across diverse operational environments and passenger demographics. Data collected during field tests will be used for qualitative and quantitative analysis by the Science and Technology Directorate. It is also testing and monitoring AutoCAT at the TSA Systems Integration Facility in preparation for future field pilots.
Upgrade of federal FRT system		
Office of Biometric Identity Management Homeland Advanced Recognition Technology (HART)	HART will replace IDENT's capabilities initially, to include FRT, and additional capabilities will be added in subsequent years.	The Office of Biometric Identity Management plans to replace IDENT with HART by December 2021.

Source: GAO analysis of survey results. | GAO-21-526
Note: We included DHS's plans to pilot an additional federal FRT system, the details of which are sensitive, in the reported number of planned use of FRT systems.

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to DHS, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- U.S. Coast Guard
- Cybersecurity and Infrastructure Security Agency
- Federal Law Enforcement Training Center
- Countering Weapons of Mass Destruction
- Office of the Inspector General
- Office of Operations Coordination

The Department of the Interior reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, Interior reported accessing two FRT systems in fiscal year 2020 and planning to use two FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

Interior reported it accessed one locally owned FRT system and one commercial FRT system in fiscal year 2020, for domestic law enforcement.

Department of the Interior Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other Interior and federal users
Accessed Local FRT system		**Interior users**
National Capital Region Facial Recognition Investigative Leads System (NCRFRILS)	NCRFRILS is an FRT system that contains copies of information, including photos, from participating law enforcement agencies. Interior requested a third party search of NCRFRILS to compare an image obtained from twitter (as an example) against the photo database to generate investigate leads.	• Interior (U.S. Park Police)
Accessed commercial FRT system		**Interior users**
Clearview AI	Clearview AI is an FRT system that can identify an individual through facial matching by comparing a photo against its facial image database. Interior uses Clearview AI to verify the identity of an individual involved in a crime and research information on a person of interest. Interior may submit photos (e.g., surveillance photos) for matching against the Clearview AI's repository of facial images from open sources. U.S. Park Police reported it stopped using Clearview AI as of June 2020.	• Interior (U.S. Park Police)

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

Interior reported it obligated no funding to access NCRFRILS in fiscal year 2020, because Interior (specifically, the U.S. Park Police) accessed this system through a third party—the Maryland National Capital Park Police. In addition, Interior reported it obligated no funding to access Clearview AI in fiscal year 2020, because it was a free trial of Clearview AI.

Research & Development in Fiscal Year 2020

None reported.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

Interior reported it plans new access to a local FRT system and a commercial FRT system through fiscal year 2023, for domestic law enforcement purposes.

Department of the Interior Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New access to local FRT system		
National Capital Region Facial Recognition Investigative Leads System (NCRFRILS)	NCRFRILS is an FRT system that contains copies of information, including photos, from participating law enforcement agencies. Interior requested a third party search of NCRFRILS to compare an image obtained from twitter (as an example) against the photo database to generate investigate leads.	In April 2021, U.S. Park Police officials told us their plans to establish a memorandum of understanding for direct access to NCRFRILS.
New access to commercial FRT system		
Clearview AI	Clearview AI is an FRT system that can identify an individual through facial matching by comparing a photo against its facial image database. Interior will use Clearview AI to verify the identity of an individual involved in a crime and research information on a person of interest. Interior may submit photos (e.g., surveillance photos) for matching against the Clearview AI repository of facial images from open sources	Interior reported its U.S. Fish and Wildlife Service began using a trial version of Clearview AI in May 2020, and purchased an annual subscription in June 2020.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to Interior, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Bureau of Indian Affairs
- Bureau of Indian Education
- Bureau of Land Management
- Bureau of Ocean Energy Management
- Bureau of Reclamation
- Bureau of Safety and Environmental Enforcement
- Bureau of Trust Funds Administration
- Office of the Assistant Secretary for Policy, Management and Budget
- Office of the Inspector General
- Office of the Secretary
- Office of Surface Mining Reclamation and Enforcement
- Office of the Solicitor
- U.S. Geological Survey

The Department of Justice (DOJ) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, DOJ reported using federal, state, local, and commercial FRT systems, conducting research and development (R&D) related to FRT, and entering into transactions with nonfederal entities for FRT. DOJ also reported plans to expand its use of FRT through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

DOJ reported it used 11 federal and commercial FRT systems in fiscal year 2020, in addition to a number of state and local systems. Of those 11 FRT systems, DOJ used eight for domestic law enforcement, one for physical security, two for national security and defense, one for video management, and two for educational purposes. Some of these systems were used for multiple purposes. All of the state and local systems were used for domestic law enforcement and some national security and defense purposes.

Department of Justice (DOJ) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other DOJ and federal users
DOJ-owned FRT systems		
Federal Bureau of Investigation Horus	Horus is being tested to determine if it can be used to improve the accuracy and efficiency of one-to-one comparison processes by serving as an aid to examiners. It is also used in educational settings to demonstrate how FRT works.	• None
Federal Bureau of Investigation Next Generation Identification Interstate Photo System (NGI IPS)	NGI IPS uses facial matching from an unknown image of interest to law enforcement against mugshots in the photo database to generate possible matches for investigators.	• Department of Homeland Security • Department of Defense
Federal Bureau of Investigation RankOne	Similar to Horus, this system is being tested to determine if it can be used to improve the accuracy and efficiency of one-to-one comparison processes by serving as an aid to examiners. It is also used in educational settings to demonstrate how FRT works.	• None
Federal Bureau of Prisons Facial Recognition Access Control System	This system uses FRT to control access by identifying and verifying individuals entering onsite secure network operations centers at federal prisons. Federal Bureau of Prisons officials noted the system will not be in use after fiscal year 2022.	• None
U.S. National Central Bureau (USNCB) International Criminal Police Organization (INTERPOL) Facial Recognition System (IFRS)	At the request of U.S. law enforcement officials, including state, local, tribal and federal authorities, the U.S. National Central Bureau can send photos, such as missing persons and suspects, in investigative cases for comparison against the holdings in IFRS. IFRS contains facial images received from more than 160 countries, and member countries can provide facial images for matching. These results are returned to the requesting country and also to the country that provided the images.	• Any U.S. law enforcement agency, including federal, via the U.S. National Central Bureau

U.S. Marshals Service Axon Facial Detection	Axon Facial Detection is used to review footage from body-worn cameras for faces (i.e., face detection) that a human then selects/deselects for redaction across multiple video frames.	• None
Accessed federal FRT systems		**DOJ users**
Department of Defense Automated Biometric Identification System (DOD ABIS)	DOD ABIS is owned and operated by the Department of Defense and is used to identify foreign nationals connected to a national security investigation, such as a known terrorist organization, or suspected of criminal activity. DOJ can request an image search on DOD ABIS through FBI's NGI IPS.	• Federal Bureau of Investigation
Department of State Integrated Biometric System (IBS)	IBS is owned and operated by the Department of State and is used to identify visa applicants for travel documents and individuals involved in identity theft and benefit fraud investigations. Specifically, FBI has direct access to perform facial recognition searches within the Department of State Consular Consolidated Database's visa holdings, and FBI's Facial Analysis, Comparison, and Evaluation (FACE) Services has indirect access to passport photos. FACE Services must request a Department of State passport officer perform facial recognition searches of passport photos on the FBI's behalf.	• Federal Bureau of Investigation
Accessed state and local FRT systems		**DOJ users**
21 states: Alabama, Arizona, Arkansas, Colorado, Delaware, Idaho, Illinois, Indiana, Iowa, Kentucky, Maryland, Michigan, Nebraska, New Mexico, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, and Utah	The FBI's FACE Services is an internal provider of facial recognition searches and requests for FBI investigations. FACE Services examiners have direct or third party access through memorandums of understandings with 21 different states' FRT systems. FACE Services also has direct and indirect (i.e., by request) access to various holdings within the Department of State's IBS and indirect access to DOD ABIS.	• Federal Bureau of Investigation
15 states: Alabama, Arizona, Delaware, Indiana, Kansas, Kentucky, Michigan, Mississippi, Missouri, Nebraska, North Dakota, South Dakota, Utah, Virginia, and West Virginia 4 localities: Chicago, Greater Cincinnati, Delaware Valley, Southeast Florida	DHS's Homeland Security Information Network (HSIN) is a system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international and private sector partners. HSIN contains a mechanism to request third party facial recognition searches through the listed state and local entities, such as fusion centers.	• U.S. Marshals Service
Other states: Arkansas, Arizona, Ohio, Pennsylvania, and Tennessee Other localities: Pinellas County, Florida and San Diego, California	DOJ requested third-party searches of these systems separately by the state or local owner in order to identify fugitives, individuals involved in a crime, or people using fraudulent identification (i.e., aliases), among other persons of interest.	• U.S. Marshals Service
National Capital Region Facial Recognition Investigative Leads System (NCRFRILS)	Authorized DOJ employees can directly search NCRFRILS for matches against photos from participating local law enforcement agencies. For example, an examiner reviewed video evidence from a retail store's surveillance cameras with facial recognition software, comparing the still image from the video with regional booking photos.	• Bureau of Alcohol, Tobacco, Firearms, and Explosives • U.S. Marshals Service

Accessed commercial FRT systems		DOJ users
Clearview AI	DOJ uses Clearview AI to identify unknown individuals of interest in state, federal, and international cases such as child exploitation. DOJ may submit photos (e.g., surveillance photos) or receive requests to match photos against the Clearview AI database.	• Bureau of Alcohol, Tobacco, Firearms, and Explosives • Drug Enforcement Administration • Federal Bureau of Investigation • U.S. Marshals Service
Vigilant Solutions	DOJ uses Vigilant Solutions to identify individuals involved in a crime. For example, an examiner reviewed photos from social media (e.g., Facebook) regarding a string of convenience store robberies, and compared them with arrest photos using facial recognition software.	• Bureau of Alcohol, Tobacco, Firearms, and Explosives

Source: GAO analysis of survey results. | GAO-21-526
Note: We included an additional FRT system owned by DOJ, the details of which are sensitive, in the reported number of FRT systems used. DOJ also reported using classified systems.

FRT System Obligations in Fiscal Year 2020

DOJ reported obligating funds to operate its own FRT systems and to access commercial ones in fiscal year 2020.

- DOJ reported obligating funds for one of the nine FRT systems it owns in fiscal year 2020. Specifically, DOJ reported obligating $17 million for its biometrics contract, which included the facial recognition algorithm used for NGI IPS.
    - DOJ reported it obligated no funds for the following systems:
        - Facial Recognition Access Control System, because it was purchased in 2014;
        - Axon Facial Detection, because the vendor upgraded the capabilities at no cost to a system already in procurement; and
        - Horus and RankOne, because they were developed by DOJ or by a partner agency that provided copies to DOJ at no cost.
- DOJ reported obligating funds for none of the federal, state, and local FRT systems it accessed in fiscal year 2020, because respective partners provided them at no cost. For example, DOJ reported that access to the INTERPOL Face Recognition System is also at no cost, because it is a dues paying member of the INTERPOL organization.
- DOJ reported obligating funds to access one of two commercial FRT systems in fiscal year 2020. Specifically, DOJ obligated $9,000 for some Clearview AI licenses and all access to Vigilant Solutions at no cost through federal, state, and local partner agencies.

Research & Development in Fiscal Year 2020

DOJ reported conducting and supporting R&D to support its mission needs. Specifically, the FBI reported obligating $1.56 million for several types of FRT research, as follows:

- An interagency agreement with the National Institute of Standards and Technology for (1) testing and evaluation of current industry face image quality tools and identification of best practices; (2) a facial recognition algorithm benchmark for testing overall accuracy and continued analysis of the effect demographics has on accuracy; and (3) benchmark testing technology to detect face image manipulation, such as a deepfake, with the goal of discerning industry capabilities.
- Applied research at the West Virginia University Research Corporation into (1) the relationship between skin tone and false match rates in facial recognition algorithms and (2) assessing the capabilities and limitations of current synthetic face detection, such as deepfakes, and developing synthetic face detection software prototypes.

- FBI's Operational Technology Division is conducting applied research on facial matching. For example, the Horus and RankOne systems were tested for the potential benefits of combining FRT systems with trained forensic examiners for verification.

Transactions with Nonfederal Entities in Fiscal Year 2020

DOJ reported that it awarded an $836,000 grant to the Police Foundation for the development of techniques to automate analysis of body worn camera audio and video data of police and community interactions. In particular, these techniques could (1) allow an evaluation of officers' adherence to principles of procedural justice and (2) validate the ratings generated by the automated process using a randomized control trial comparing software ratings of videos to evaluations performed by human raters under conditions of high and low procedural justice.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

DOJ reported it plans to use two other FRT systems through fiscal year 2023. Of these, one will be used for border and transportation security, and one will be used for physical security purposes.

Department of Justice (DOJ) Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New Federal FRT systems		
Drug Enforcement Administration (DEA) Security video management system	DEA plans to use the facial recognition component of a security video management system to control access, monitor, and surveil its headquarters facility.	This system is not operational as of June 2021 because DEA's headquarters facility is being renovated. DEA plans to begin using the FRT features after completing a privacy assessment.
U.S. Marshals Service (USMS) Justice Prisoner and Alien Transportation System (JPATS) Mobile Application	USMS plans to develop software to perform touchless prisoner identity verification, such as during prisoner transport, searching for a match against booking and prisoner photos within the JPATS mobile application for transportation security purposes.	USMS planned to begin using the JPATS Mobile Application in mid-to-late 2021, but has been delayed because the bid was protested.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to DOJ, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- U.S. Attorneys
- Office on Violence Against Women
- Community Oriented Policing Services
- Office of Information Policy
- Foreign Claims Settlement Commission
- DOJ Divisions (Antitrust, Civil, Civil Rights, Criminal, Environment & Natural Resources, Justice Management, Tax, and National Security)
- Community Relations Service
- Office of the Solicitor General
- Office of Professional Responsibility
- Office of the Inspector General
- Office of the Pardon Attorney

- U.S. Parole Commission
- Executive Office for Immigration Review
- Executive Office for Organized Crime Drug Enforcement Task Forces
- Executive Office for U.S. Trustees
- Professional Responsibility Advisory Office

The Department of State reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, State reported owning one FRT system and accessing one FRT system in fiscal year 2020. State also reported conducting FRT-related research and development (R&D), and entering into transactions with nonfederal entities for FRT. State reported it plans to use one other FRT system through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

State reported it owned one FRT system and accessed one other FRT system in fiscal year 2020, for border and transportation security and national security and defense purposes.

Department of State Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other State and federal users
State-owned FRT system		
Bureau of Consular Affairs Integrated Biometric System (IBS)	State uses IBS to verify an applicant's identity or determine whether an individual has applied for a visa. State uses FRT to search visa and passport photos contained in IBS for matches with individuals who previously applied for travel documents or may be involved in visa fraud. Potential matches from IBS are sent to the Kentucky Consular Center and National Visa Center for review before a final determination is made by consular officers at posts or passport specialists at passport agencies and centers.	• Department of State (Bureau of Diplomatic Security) • Department of Justice • Department of Homeland Security
Accessed federal FRT system		**State users**
Department of Defense Automated Biometric Identification System (DOD ABIS)	State uses DOD ABIS to verify the authenticity of travel documents. State submits multimodal biometric files (e.g., fingerprints and face and iris scans) to DOD ABIS through a U.S. Special Operations Command portal or the Department of Justice's Next Generation Identification Interstate Photo System.	• Bureau of Diplomatic Security

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

In fiscal year 2020, State reported it obligated over $8.5 million for IBS. In addition, State reported it obligated no funds to access DOD ABIS, because DOD funded the FRT system.

Research & Development in Fiscal Year 2020

State reported conducting the following FRT-related R&D to enhance facial analysis and facial matching in fiscal year 2020, as follows:

- State's Bureau of Consular Affairs reported conducting R&D to enhance facial analysis, including morphing detection (e.g., making a synthetic face image using two faces to allow both individuals to use the image for identification purposes) and the impact of aging on the accuracy of facial recognition algorithms, such as for children's passports. State reported this R&D will contribute to International Organization for Standardization and International Civil Aviation Organization image standards for travel documents. State reported obligating over $1.7 million for these projects in fiscal year 2020.
- State's Bureau of Counterterrorism reported conducting R&D to enhance the facial matching of screening technology used in the Personal Identification Secure Comparison and Evaluation System (PISCES) border management system. The system matches images of individuals against passport images and a repository of images of suspicious individuals. State reported obligating approximately $3 million for a larger effort to improve program technology, including the enhanced screening technology.

Transactions with Nonfederal Entities in Fiscal Year 2020

State reported it entered into the following transactions to assist foreign governments with purchasing and using previously donated FRT equipment:

- State's Bureau of International Narcotics and Law Enforcement reported entering into an interagency agreement and contract with Mexico's National Migration Institute. Specifically, State assisted with building the institute's capacity to collect, store, and share biometric data on third-country nationals with donated FRT equipment. In addition, State reported it funded technical advisors to train Mexican government employees to use the equipment. State reported obligating approximately $2.6 million for the technical assistance and training.
- State's Bureau of International Narcotics and Law Enforcement also reported it obligated approximately $333,000 to purchase 10 workstations for the Guatemalan Immigration Institute. The institute plans to install the workstations at three locations—the La Aurora International Airport, the Guatemalan Immigration Institute Detention Facility, and the Valle Nuevo port of entry on the El Salvador-Guatemala border.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

State reported it plans to use one other FRT system through fiscal year 2023 for border and transportation security.

Department of State Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New federal FRT system		
Bureau of Counterterrorism Personal Identification Secure Comparison and Evaluation System (PISCES)	The FRT system matches individuals against passport images and a repository of known or suspected terrorists using the system. State reported plans to incorporate enhanced screening technologies in PISCES to ensure foreign partners under the Terrorist Interdiction Program are able to protect themselves from attempts by terrorists to enter, transit, or depart their country.	State plans to pilot the new FRT system in the summer of 2021. If the testing is successful, State will deploy the software to operational locations.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to State, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Office of the Secretary of State
- Office of the Deputy Secretary
- Office of the Under Secretary for Arms Control and International Security
- Office of the Under Secretary for Economic Growth, Energy, and Environment
- Office of the Under Secretary for Political Affairs
- Office of the Under Secretary for Public Diplomacy and Public Affairs

The Department of Transportation (DOT) reported conducting facial recognition technology (FRT) related research and development (R&D) activities in fiscal year 2020. Specifically, DOT used FRT to conduct human factors research in a variety of transportation-related areas. DOT reported it did not have any other FRT activities in fiscal year 2020, and does not plan to use FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

None reported.

FRT System Obligations in Fiscal Year 2020

None reported.

Research & Development in Fiscal Year 2020

DOT reported the following R&D projects in fiscal year 2020 that used FRT, specifically facial detection and analysis, to conduct human factors research, such as:

- The Federal Motor Carrier Safety Administration conducted human factors research involving commercial motor vehicle drivers' behavior and safety performance. For example, an onboard monitoring system analyzes a driver's face to identify fatigue and distraction while driving. The FRT has eye glance analysis, which measures visual attention or inattention, rates drowsiness, and measures the percent of eye closure as an indicator of fatigue.
- The Federal Highway Administration used FRT at its lab, which has a simulator and test vehicle, to conduct human factors research. They use the results to incorporate highway driver needs into roadway design, construction, repair, and improvement. In addition, it obligated $150,580 through an interagency agreement to the National Science Foundation's Big Data Hubs program to support research into better ways to protect the privacy of drivers who participated in a mandated naturalistic driver study that recorded their in-cabin behavior. This research is intended to improve other researchers' access to the driver data, helping them use it to improve traffic safety. It also obligated $300,000 to Oak Ridge National Laboratory, which included facial detection research.
- The Federal Railroad Administration reported operating the Cab Technology Integration Lab—a full-sized locomotive cab simulator—that uses an eye tracking device and software to determine what a train engineer is looking at on a display screen or when scanning the environment outside the cab. This data helps researchers determine what objects in the environment capture the engineer's attention while driving a train.
- The Federal Aviation Administration reported conducting human factors research that uses eye tracking technology to observe how air traffic controllers scan their instruments to determine eye motion workload and the time spent looking at each object. This research is intended to ensure that systems that include human operators and maintainers perform as effectively and safely as possible.

DOT reported it could not provide specific obligations for individual R&D projects that used FRT, because the programs do not track obligations at that level.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

None reported.

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to DOT, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Office of the Secretary of Transportation
- Office of Inspector General
- National Highway Traffic Safety Administration
- Federal Transit Administration
- Pipeline and Hazardous Materials Safety Administration
- Great Lakes Saint Lawrence Seaway Development Corporation
- Maritime Administration

The Department of the Treasury reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, Treasury reported accessing two FRT systems. Treasury also reported plans to use three other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

Treasury reported it accessed two FRT systems in fiscal year 2020, one for digital access and one for domestic law enforcement purposes.

Department of the Treasury Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other Treasury and federal users
Accessed federal FRT system		**Treasury users**
General Services Administration login.gov	This login.gov pilot used FRT that compared two photos to verify the identity of an individual accessing the website or application. Login.gov takes a picture of the individual and their photo identification to determine a match using FRT.	• Internal Revenue Service (IRS)
Accessed commercial FRT system		**Treasury users**
Vendor facial recognition search services	A third-party vendor performed facial recognition searches on behalf of the IRS for domestic law enforcement purposes. Additional details on the search are sensitive.	• IRS

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

Treasury reported it obligated no funding to access the two FRT systems in fiscal year 2020. Specifically, GSA funded its login.gov FRT system, and a vendor provided a demonstration of their FRT system at no additional cost.

Research & Development in Fiscal Year 2020

None reported.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

Treasury reported it plans to use three FRT systems through fiscal year 2023 for domestic law enforcement purposes.

Department of the Treasury Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023

FRT system	Description of system use	Planned new use status
New federal FRT system		
U.S. Treasury Inspector General for Tax Administration (TIGTA) Facebox	Facebox identifies facial images of similar persons linked to multiple investigations through an online storage locker that contains information, including photos from other investigations. The FRT system notifies the investigators of potential matches.	TIGTA purchased Facebox in June 2020, and plans to begin use of the FRT system in December 2020.
New access to federal FRT system		
Internal Revenue Service (IRS) Memoranda of Understanding (MOUs) to access federal FRT systems	The MOUs will allow IRS agents direct access to other federal biometric databases, including facial recognition. The additional access will assist IRS agents with criminal investigations. For example, an IRS agent may submit a surveillance photo to the National Forensic Laboratory, which will conduct a facial recognition search against one of the FRT systems.	The IRS's National Forensic Laboratory is in the process of establishing MOUs with the Departments of Defense, Homeland Security, and Justice. As of April 2021, the IRS was determining whether separate MOUs are needed.
Evaluation of commercial FRT system		
IRS Vendor facial recognition search services	A third-party vendor performed facial recognition searches on behalf of the IRS for domestic law enforcement purposes. Additional details on the search are sensitive.	IRS plans to conduct an additional pilot pending additional funding.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to Treasury, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Alcohol and Tobacco Tax and Trade Bureau
- Bureau of Engraving and Printing
- Bureau of the Fiscal Service
- Financial Crimes Enforcement Network
- Office of Inspector General
- Office of the Comptroller of the Currency
- U.S. Mint
- Treasury Departmental Offices

The Department of Veterans Affairs (VA) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, VA reported conducting FRT-related research and development (R&D), and entering into transactions with nonfederal entities for FRT. VA reported plans to use two other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

None reported.

FRT System Obligations in Fiscal Year 2020

None reported.

Research & Development in Fiscal Year 2020

VA reported using FRT as a tool to conduct research for purposes other than facial matching. Specifically, VA reported using eye tracking to conduct clinical research for treating post-traumatic stress disorder. The eye tracking system evaluates pupil response to evaluate impairment. VA reported obligating $22,840 for the equipment.

Transactions with Nonfederal Entities in Fiscal Year 2020

VA purchased two types of eye tracking equipment for veterans.

- VA reported it purchased prosthetics that enable veterans with speech impairment or loss to communicate using a computer or tablet device. VA reported purchasing 42 devices for $416,284.
- VA reported it purchased a prosthetic device that enabled one veteran to use eye gaze to manipulate a laptop computer for $18,860.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

VA reported it plans to use two FRT systems through fiscal year 2023, for physical security and domestic law enforcement purposes.

Department of Veterans Affairs (VA) Plans for Facial Recognition Technology (FRT) Systems through Fiscal Year 2023		
FRT system	**Description of system use**	**Planned new use status**
New federal FRT systems		
VA Police Service Chicago, IL Motorola Avigilon	The FRT system can sort through video quickly locating a specific person, such as a missing patient or to input a photo from a police bulletin (e.g., 'Be On the Lookout'), to alert officers when that person enters the VA medical center campus.	VA reported that they plan to obligate funding for a project design to install Motorola Avigilon by fiscal year 2022.
VA Police Service West Palm Beach, FL Veritone ai Ware	The web-based FRT can detect and follow selected, moving objects, such as a previously disruptive individual or to track missing patients, and will alert officers when on the VA medical center campus.	VA purchased FRT software for 12 cameras in 2019, and is working with the contractor to ensure the system is operational by the middle of fiscal year 2022.

Source: GAO analysis of survey results. | GAO-21-526

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to VA, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Veterans Benefits Administration
- National Cemetery Administration

The General Services Administration (GSA) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, GSA reported owning one FRT system. GSA reported it does not plan to use other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

GSA reported it owned one FRT system in fiscal year 2020, for digital access purposes.

General Services Administration (GSA) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other GSA and federal users
GSA-owned federal FRT system		
Technology Transformation Service login.gov	Login.gov conducted a pilot with Department of the Treasury employees to test FRT services that compared two photos to verify the identity of an individual accessing the website or application. Login.gov takes a picture of the individual and their photo identification to determine a match.	• Department of the Treasury

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

GSA reported it obligated over $90,000 for login.gov in fiscal year 2020.

Research & Development in Fiscal Year 2020

None reported.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

None reported.

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to GSA, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- National Services (Public Building Service)
- Regional Offices
- Staff Offices
- Independent Offices (Office of Inspector General)

The National Aeronautics and Space Administration (NASA) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, NASA reported testing one FRT system and conducting FRT-related research and development (R&D). NASA reported it does not plan to use other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

NASA reported it owned one FRT prototype system in fiscal year 2020. Specifically, NASA tested this system for issuing badges.

National Aeronautics and Space Administration (NASA) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other NASA and federal users
NASA-owned FRT system		
Johnson Space Center Forgotten badge prototype	The forgotten badge prototype confirms an employee's identity by comparing a current camera image of the employee with a photo on file. NASA reported that it would not continue work on the prototype due to cost.	• None

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

NASA reported it did not obligate funds for its forgotten badge prototype in fiscal year 2020, because funding for the prototype was obligated in fiscal year 2019.

Research & Development in Fiscal Year 2020

NASA reported using FRT as a tool to conduct human factors research. Specifically, the Langley Research Center conducted a series of controlled research experiments from 2013 to 2020, to understand the cognitive states of aircraft and space flight crew. These experiments included the use of eye tracking and facial muscle tracking devices to understand cognitive states (e.g., surprised, focused) and other human factors during simulations. NASA reported it obligated $60,000 for the R&D experiments in fiscal year 2020.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

None reported.

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to NASA, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Administrator Staff Offices
- Mission Directorates
- Mission Support Directorate
- Office of the Administrator
- Office of the Inspector General

The National Science Foundation (NSF) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, NSF reported it supported FRT-related research and development (R&D) in fiscal year 2020. NSF also reported it does not plan to use other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

None reported.

FRT System Obligations in Fiscal Year 2020

None reported.

Research & Development in Fiscal Year 2020

NSF reported it supported FRT-related R&D conducted by external organizations in fiscal year 2020. Specifically, NSF's Directorate for Computer and Information Science and Engineering awarded three grants to universities and others to conduct research on FRT and related areas. For example:

- The University of Chicago conducted research using machine learning for facial recognition.
- The Columbus State University conducted research on facial privacy.
- The University of Nebraska conducted research using eye tracking to optimize programmer productivity.

NSF reported obligating $1,696,146 for these grants in fiscal year 2020, but this amount includes areas of research other than FRT.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

None reported.

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to NSF, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Chief Information Officer
- Directorate for Biological Sciences
- Directorate for Education and Human Resources
- Directorate for Engineering

- Directorate for Geosciences
- Directorate for Mathematical and Physical Sciences
- Directorate for Social, Behavioral, and Economic Sciences
- National Science Board (Office of Inspector General)
- Office of Budget, Finance, and Award Management
- Office of the Director
- Office of Diversity and Inclusion
- Office of the General Counsel
- Office of Information Resource Management
- Office of Integrative Activities
- Office of International Science and Engineering
- Office of Legislative and Public Affairs

The Social Security Administration (SSA) reported facial recognition technology (FRT) activities in fiscal year 2020. Specifically, SSA reported accessing one FRT system in fiscal year 2020. SSA reported it does not plan to use other FRT systems through fiscal year 2023.

Use of FRT Systems in Fiscal Year 2020

SSA reported it accessed one FRT system in fiscal year 2020, for digital access purposes.

Social Security Administration (SSA) Facial Recognition Technology (FRT) Systems Used in Fiscal Year 2020

FRT system	Description of system use	Other SSA and federal users
Accessed commercial FRT system		**SSA users**
Acuant FaceID	This pilot of Acuant FaceID was conducted using agency employees to verify the identity of employees within the test group for access to SSA's public online services by remotely confirming that the facial image on an identity document (e.g., state-issued IDs) matches the facial image of the applicant.	• Office of Digital Transformation

Source: GAO analysis of survey results. | GAO-21-526

FRT System Obligations in Fiscal Year 2020

SSA reported that it could not provide the specific amount that was obligated for FRT, because this FRT was included as part of a larger task order. Instead, SSA reported that it obligated $809,179 as part of a larger contract to support digital identity enhancements, including the pilot.

Research & Development in Fiscal Year 2020

None reported.

Transactions with Nonfederal Entities in Fiscal Year 2020

None reported.

Regulation of Nonfederal Entities' Use of FRT in Fiscal Year 2020

None reported.

Planned Use of FRT Systems through Fiscal Year 2023

None reported.

Components with No FRT-Related Activities in Fiscal Year 2020 or Planned Uses through Fiscal Year 2023

According to SSA, the following components reported no FRT-related activities in fiscal year 2020 or planned uses through fiscal year 2023 listed above:

- Office of Analytics, Review, and Oversight
- Office of Budget, Finance, and Management
- Office of the Chief Actuary
- Office of the Commissioner
- Office of Communications
- Office of General Counsel
- Office of the Inspector General
- Office of Hearings Operations
- Office of Human Resources
- Office of Legislation and Congressional Affairs
- Office of Operations
- Office of Retirement and Disability Policy

Appendix III: Comments from the U.S. Agency for International Development

June 30, 2021

Candice N. Wright
Acting Director
Science, Technology Assessment, and Analytics

and

Gretta L. Goodwin
Director
Homeland Security and Justice

U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: GAO draft report entitled "Facial Recognition Technology: Current and Planned Uses by Federal Agencies". GAO-21-526SU (Engagement Code 104231)

Dear Ms. Wright and Ms. Goodwin:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, "Facial Recognition Technology: Current and Planned Uses by Federal Agencies", GAO-21-526SU (Engagement Code 104231)

The report has no recommendations for USAID and we do not offer specific comments with regards to content of the report. The Agency continues to apply fiscal responsibility with regard to information technology investments, including emerging technologies. This is evidenced in our four overall "A" ratings on Federal Information Technology Acquisition Reform Act (FITARA) Scorecards, including for incremental development, transparency and risk management, the consolidation and optimization of our data centers, and software licensing.

The Agency is continuously committed to identifying and delivering efficient, flexible information technology solutions. This is evident in our current use of facial recognition technology (FRT) for digital access on our mobile devices, which provides high value to our workforce, without compromising security and privacy of our data. USAID will surely monitor the advancement of FRT in the coming years and assess how and when further adoption is appropriate or applicable to meet the Agency's needs and foster partnership.

Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our Facial Recognition initiative.

Sincerely,

Colleen R. Allen

Colleen R. Allen
Acting Assistant Administrator
Bureau for Management

Appendix IV: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

July 6, 2021

Candice N. Wright
Director, Science, Technology Assessment, and Analytics
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Wright:

Thank you for the opportunity to review the draft report "FACIAL RECOGNITION TECHNOLOGY: Current and Planned Uses by Federal Agencies" (GAO-21-526SU). The report is an accurate assessment of our experience related to facial recognition technology.

If you have any questions, please contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Scott Frey
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Candice N. Wright at (202) 512-6888 or wrightc@gao.gov
Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov

Staff Acknowledgments

In addition to the contact named above, Adam Hoffman (Assistant Director) and Richard Hung (Assistant Director), Katrina Pekar-Carpenter (Analyst-in-Charge), Kelsey Burdick, Jehan Chase, Nirmal Chaudhary, Caitlin Cusati, Khaki LaRiviere, Sarah Prokop, and Carl Ramirez made key contributions to this report. Also contributing were Christina Bixby, Cheron Brooks, April Gillens, Sig Janoska-Bedi, Tom Lombardi, Robert Rivas and Benjamin Shouse.

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