United States Government Accountability Office

Report to Congressional Requesters

August 2021

FACIAL RECOGNITION TECHNOLOGY

Current and Planned Uses by Federal Agencies

Accessible Version

GAO-21-526

GAO Hightlight

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

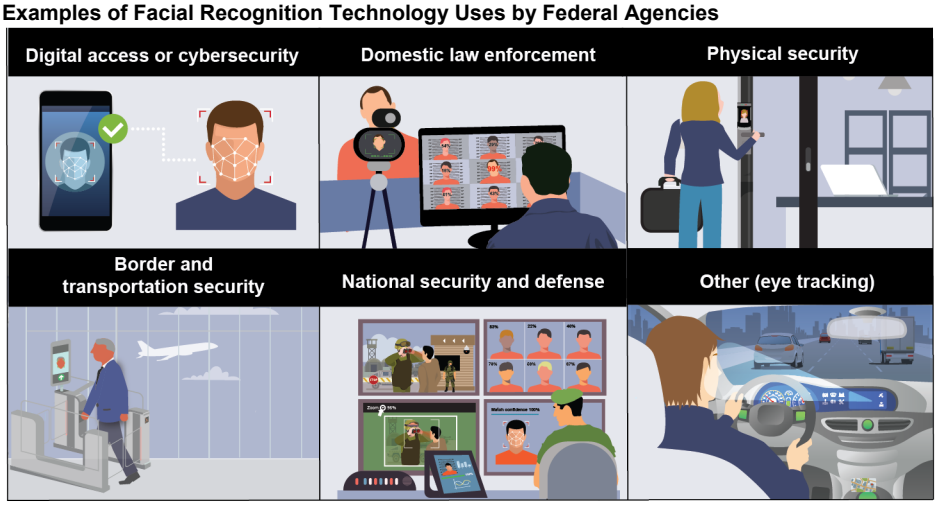
In response to GAO's survey about facial recognition technology (FRT) activities in fiscal year 2020, 18 of the 24 surveyed agencies reported using an FRT system, for one or more purposes, including:

- **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

Tables

Figures

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

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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 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.

[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.

[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).

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 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.

[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.

[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.

Background

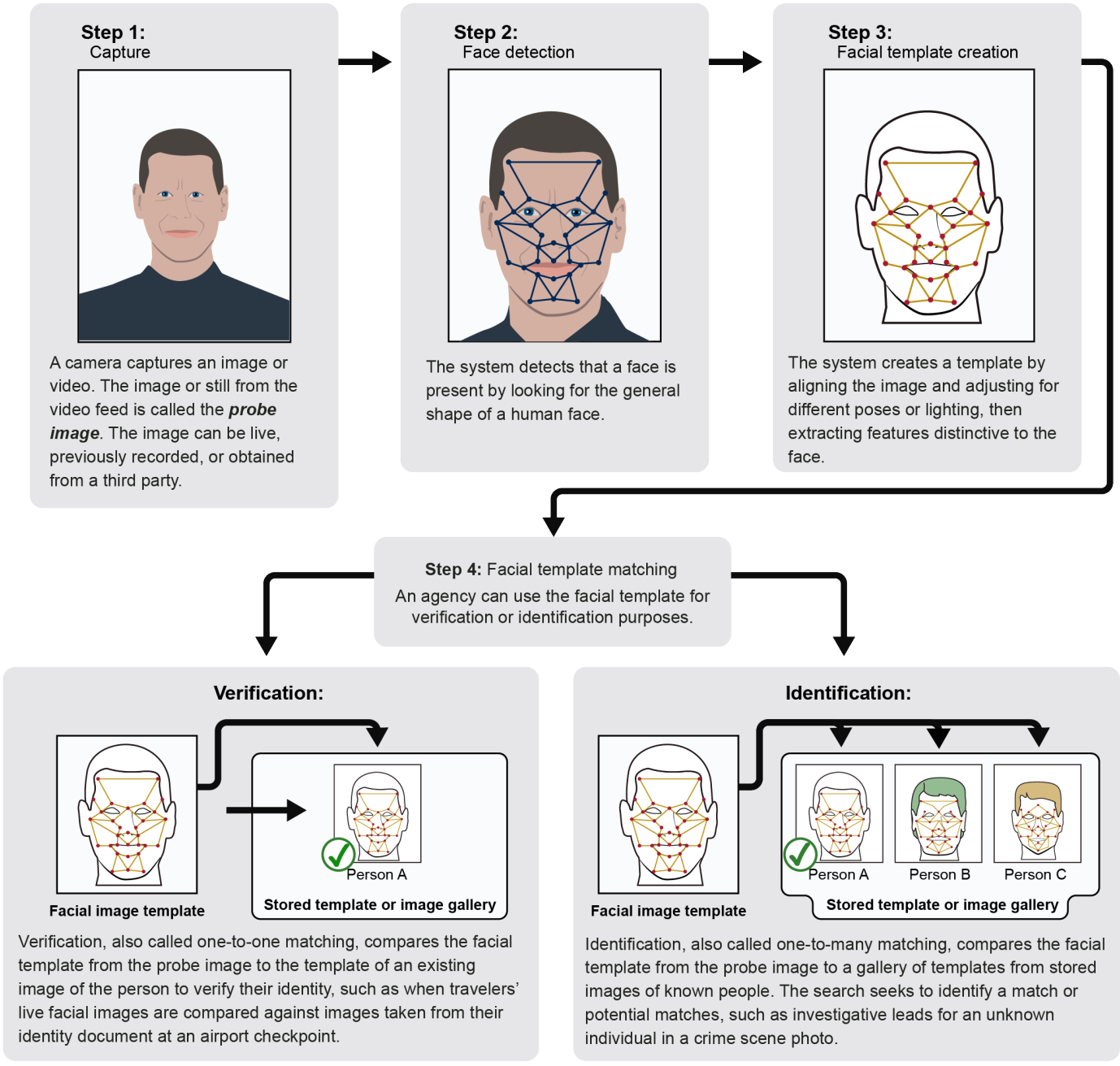
How Facial Recognition Technology Works

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 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.

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

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.

[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.

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]

- **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.

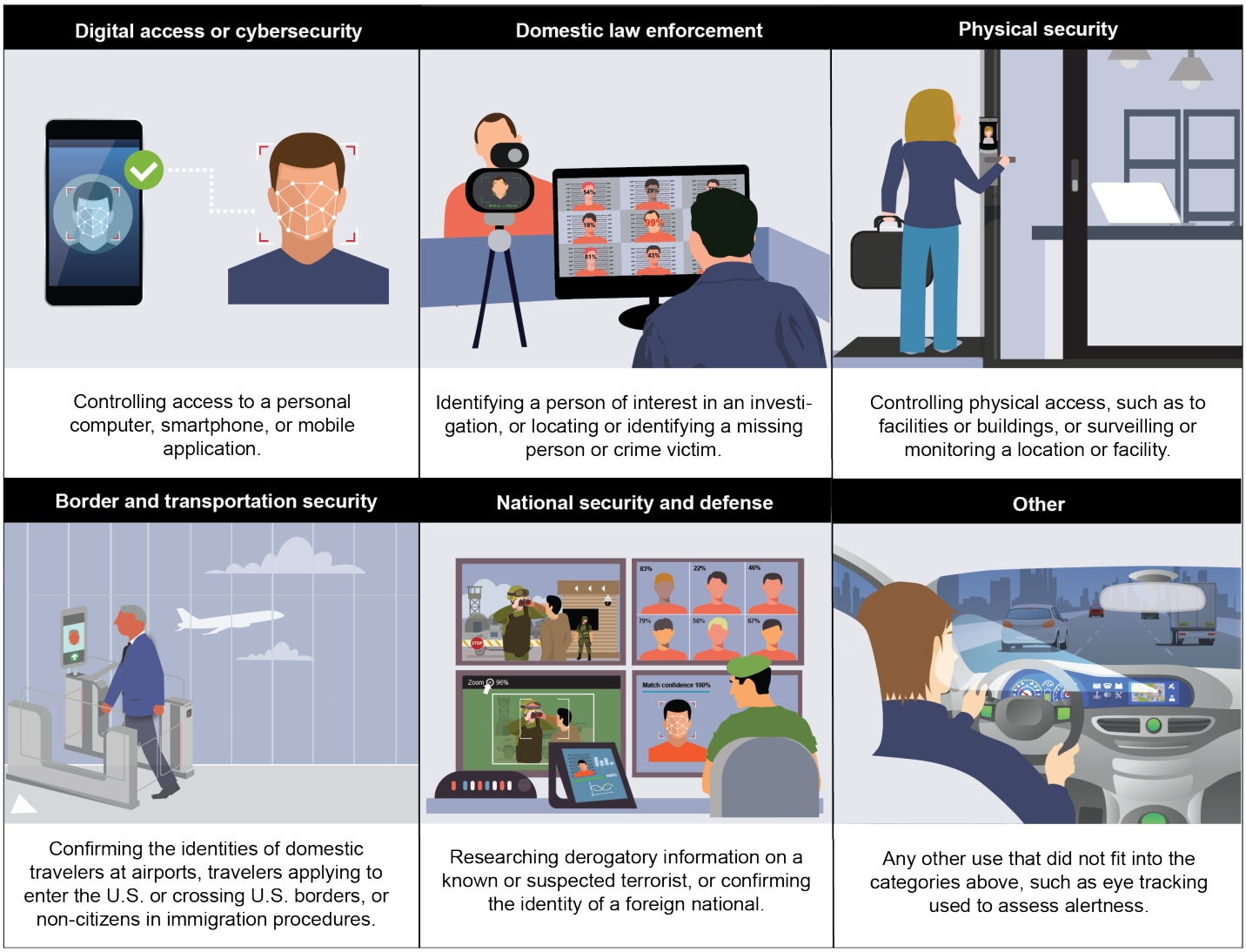
Illustrative examples of these purposes are shown in figure 2.

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

[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	Yes	No	No	No
Department of Commerce	Yes	Yes	No	No
Department of Defense	Yes	Yes	No	No
Department of Education	No	No	No	No
Department of Energy	Yes	No	No	No
Department of Health and Human Services	Yes	Yes	No	No
Department of Homeland Security	Yes	Yes	Yes	Yes
Department of Housing and Urban Development	No	No	No	No
Department of the Interior	Yes	No	No	No
Department of Justice	Yes	Yes	Yes	No
Department of Labor	No	No	No	No
Department of State	Yes	Yes	Yes	No
Department of Transportation	No	Yes	No	No
Department of the Treasury	Yes	No	No	No
Department of Veterans Affairs	Yes	Yes	Yes	No
U.S. Agency for International Development	Yes	No	No	No
Environmental Protection Agency	Yes	No	No	No
General Services Administration	Yes	No	No	No
National Aeronautics and Space Administration	Yes	Yes	No	No
National Science Foundation	Yes	Yes	No	No

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]
Nuclear Regulatory Commission	No	No	No	No
Office of Personnel Management	Yes	No	No	No
Small Business Administration	No	No	No	No
Social Security Administration	Yes	No	No	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	Yes	no	no	no	no	no
Department of Commerce	Yes	no	Yes	no	no	no
Department of Defense	no	Yes	Yes	no	Yes	Yes
Department of Energy	Yes	no	Yes	no	no	no
Department of Health and Human Services	Yes	Yes	Yes	no	no	no
Department of Homeland Security	Yes	Yes	no	Yes	Yes	no
Department of the Interior	Yes	Yes	no	no	no	no
Department of Justice	Yes	Yes	Yes	no	Yes	Yes
Department of State	no	no	no	Yes	Yes	no
Department of the Treasury	Yes	Yes	no	no	no	no
Department of Veterans Affairs	Yes	no	no	no	no	no
Agency for International Development	Yes	no	no	no	no	no
Environmental Protection Agency	Yes	no	no	no	no	no
General Services Administration	Yes	no	no	no	no	no
National Aeronautics and Space Administration	Yes	no	no	no	no	Yes
National Science Foundation	Yes	no	no	no	no	no
Office of Personnel Management	Yes	no	no	no	no	no
Social Security Administration	Yes	no	no	no	no	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.

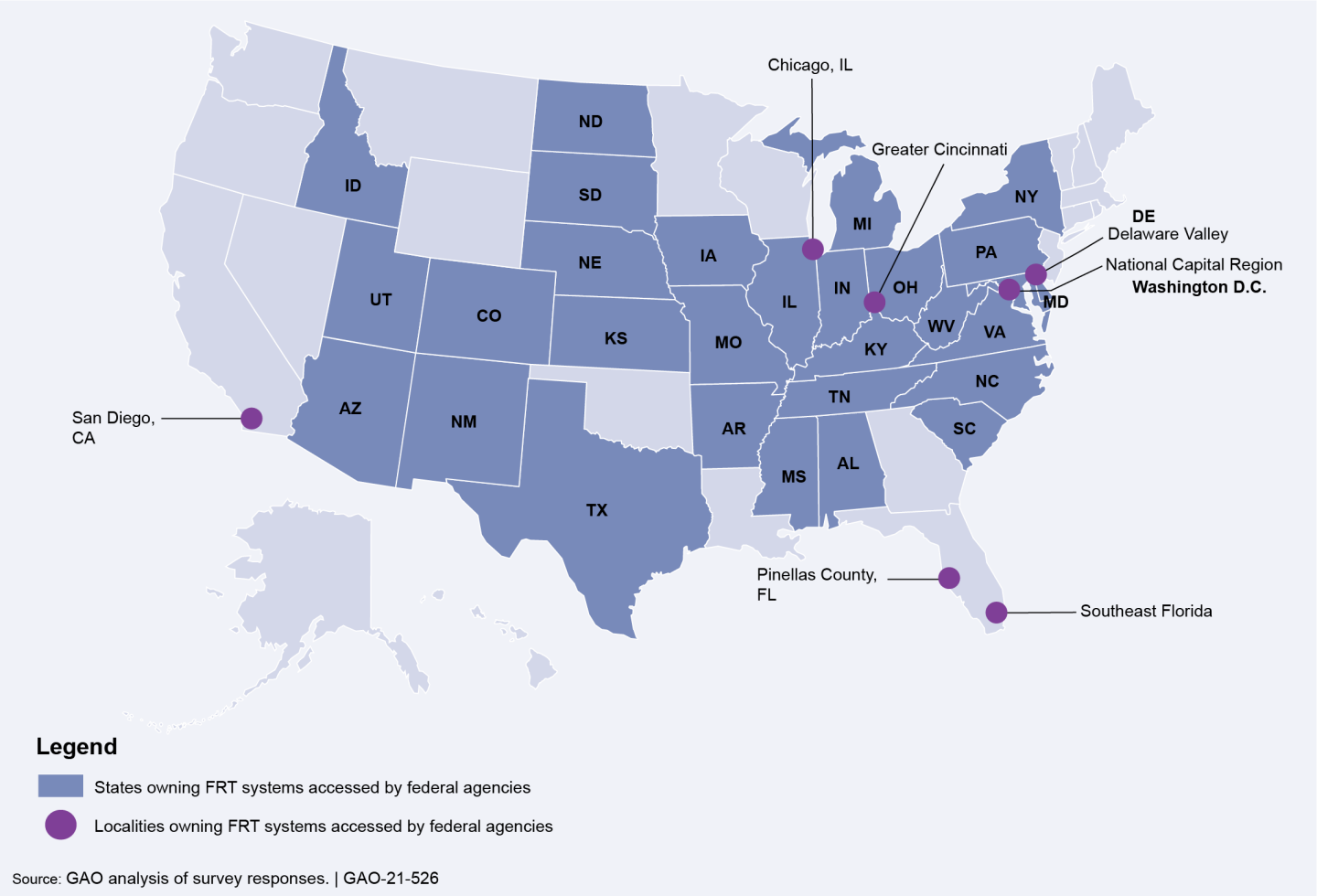
For example, DOE's TacID Guard Dog performs facial matching and facial verification from live video to monitor the entry and exit of agency personnel at access points.

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. Specifically, FBI agents can submit a probe photo and request FACE

[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.

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

[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).

documents. For example, State conducted research on morphing detection and the impact of aging on the accuracy of facial recognition 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

[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.

research. For example, DOT reported that the Federal Railroad Administration used eye tracking to study alertness in train operators. 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

[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.

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 (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.

[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.

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 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

[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.

[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.

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	Yes	no	no
Department of Commerce	Yes	no	no
Department of Defense	Yes	Yes	no
Department of Health and Human Services	Yes	no	no
Department of Homeland Security	Yes	Yes	Yes
Department of the Interior	Yes	no	no
Department of Justice	Yes	no	no
Department of State	Yes	no	no
Department of the Treasury	Yes	Yes	no
Department of Veterans Affairs	Yes	no	no

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

[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.

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
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

[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 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.

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

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. 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

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

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

[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.

- Agency for International Development
- Environmental Protection Agency
- General Services Administration
- National Aeronautics and Space Administration
- 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—

[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.

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 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]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).

4. any transactions the agency entered into with nonfederal entities for that entity to obtain facial recognition technology in fiscal year 2020; and
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

[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.

pretest on the research and development questions with that agency. On 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

[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.

been included correctly in more than one Attachment. In one case, for 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

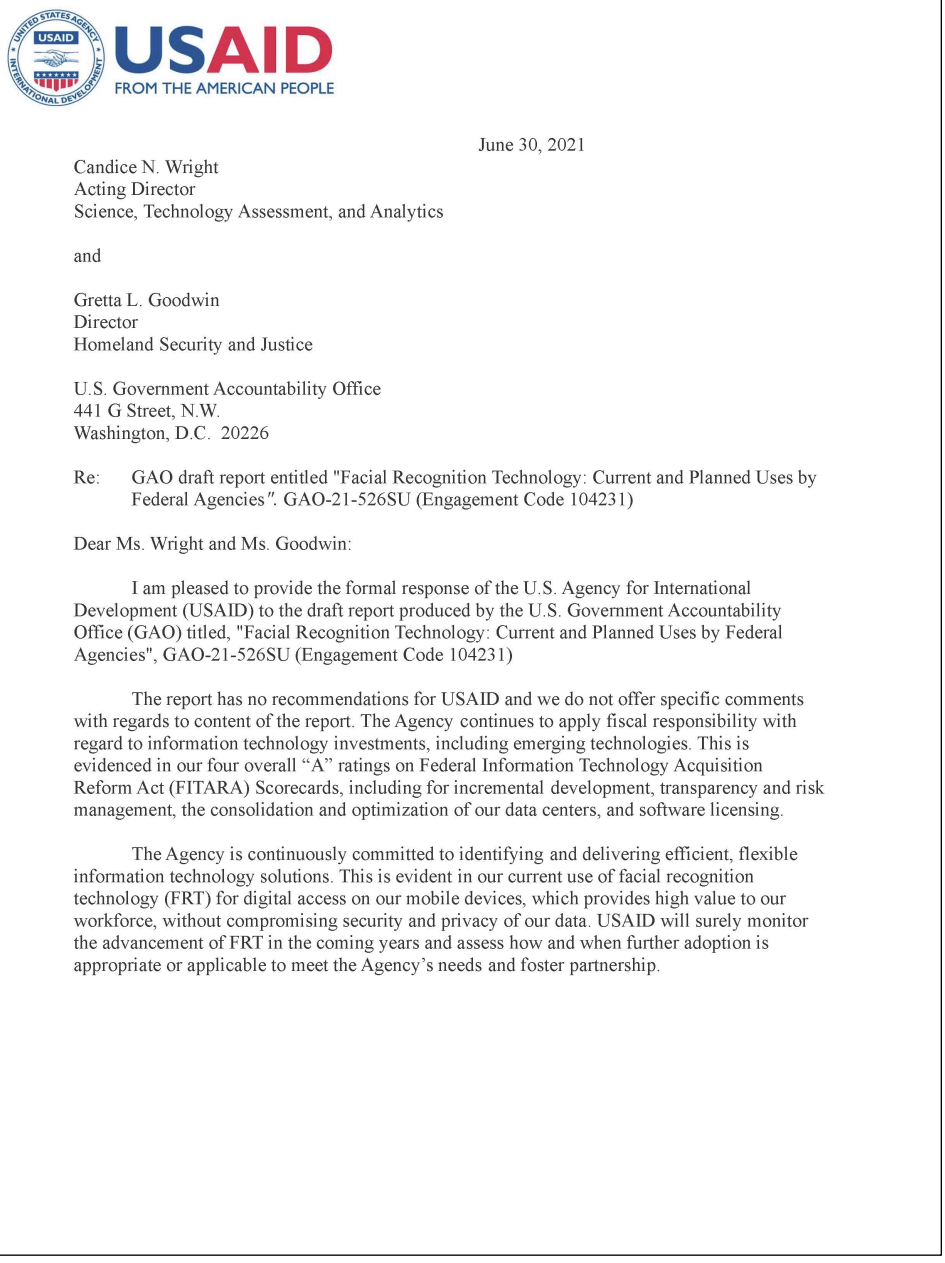
The information in these summaries is from survey responses or requests for more information from the agencies. We present details on FRT systems reported by agencies that own their FRT systems or access the FRT systems of other government entities, including federal and nonfederal governments, and commercial 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.

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



USAID
FROM THE AMERICAN PEOPLE

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

Agency Comment Letter

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

Page 1

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.

Page 2

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
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

Agency Comment Letter

Text of Appendix IV: Comments from the Social Security Administration

Page 1

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

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

Please Print on Recycled Paper.