



June 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks

Accessible Version

GAO@100 Highlights

Highlights of [GAO-21-518](#), a report to congressional requesters

Why GAO Did This Study

Federal agencies that employ law enforcement officers can use facial recognition technology to assist criminal investigations, among other activities. For example, the technology can help identify an unknown individual in a photo or video surveillance.

GAO was asked to review federal law enforcement use of facial recognition technology. This report examines the 1) ownership and use of facial recognition technology by federal agencies that employ law enforcement officers, 2) types of activities these agencies use the technology to support, and 3) the extent that these agencies track employee use of facial recognition technology owned by non-federal entities.

GAO administered a survey questionnaire to 42 federal agencies that employ law enforcement officers regarding their use of the technology. GAO also reviewed documents (e.g., system descriptions) and interviewed officials from selected agencies (e.g., agencies that owned facial recognition technology). This is a public version of a sensitive report that GAO issued in April 2021. Information that agencies deemed sensitive has been omitted.

What GAO Recommends

GAO is making two recommendations to each of 13 federal agencies to implement a mechanism to track what non-federal systems are used by employees, and assess the risks of using these systems. Twelve agencies concurred with both recommendations. U.S. Postal Service concurred with one and partially concurred with the other. GAO continues to believe the recommendation is valid, as described in the report.

View [GAO-21-518](#). For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov.

June 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks

What GAO Found

GAO surveyed 42 federal agencies that employ law enforcement officers about their use of facial recognition technology. Twenty reported owning systems with facial recognition technology or using systems owned by other entities, such as other federal, state, local, and non-government entities (see figure).

Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers



Source: GAO analysis of survey data. | GAO-21-518

Note: For more details, see figure 2 in GAO-21-518.

Agencies reported using the technology to support several activities (e.g., criminal investigations) and in response to COVID-19 (e.g., verify an individual's identity remotely). Six agencies reported using the technology on images of the unrest, riots, or protests following the death of George Floyd in May 2020. Three agencies reported using it on images of the events at the U.S. Capitol on January 6, 2021. Agencies said the searches used images of suspected criminal activity.

All fourteen agencies that reported using the technology to support criminal investigations also reported using systems owned by non-federal entities. However, only one has awareness of what non-federal systems are used by employees. By having a mechanism to track what non-federal systems are used by employees and assessing related risks (e.g., privacy and accuracy-related risks), agencies can better mitigate risks to themselves and the public.

Contents

Letter	1
Background	4
Twenty Federal Agencies Reported Owning or Using Systems with Facial Recognition Technology	8
Federal Agencies Reported Using Systems with Facial Recognition Technology to Support Various Activities	18
Most Agencies Do Not Track Non-Federal Systems in Use or Related Risks	22
Conclusions	28
Recommendations for Executive Action	28
Agency Comments and Our Evaluation	31
Appendix I: Objectives, Scope, and Methodology	36
Appendix II: Systems with Facial Recognition Technology Owned by Federal Agencies that Employ Law Enforcement Officers	42
Appendix III: Other Federal Systems with Facial Recognition Technology	62
Appendix IV: Comments from the Department of Health and Human Services	67
Agency Comment Letter	69
Appendix V: Comments from the Department of Homeland Security	71
Agency Comment Letter	75
Appendix VI: Comments from the Department of the Interior	79
Agency Comment Letter	82
Appendix VII: Comments from the Department of State	85
Agency Comment Letter	88
Appendix VIII: Comments from the Department of the Treasury	91
Agency Comment Letter	94
Appendix IX: Comments from the Federal Bureau of Investigation	97
Agency Comment Letter	99
Appendix X: Comments from the United States Postal Service	101
Agency Comment Letter	103

Appendix XI: GAO Contact and Staff Acknowledgments	105
GAO Contact	105
Staff Acknowledgments	105

Tables

Table 1: Systems with Facial Recognition Technology that Federal Agencies Employing Law Enforcement Officers Reported as Owned or in Procurement, January 2015 through March 2020, and System Status	11
Table 2: Reported Use of Other Entities' Facial Recognition Technology by Federal Agencies that Employ Law Enforcement Officers	12
Table 3: Select Systems with Facial Recognition Technology Owned by Federal Agencies	13
Table 4: Federal Agency Reported Use of Facial Recognition Technology on Images of Individuals Suspected of Violating the Law during Civil Unrest, Riots, or Protests, May through August 2020	19
Table 5: Federal Agency Tracking of Employee Use of Non-Federal Systems with Facial Recognition Technology	23
Table 6: 42 Federal Agencies Selected in GAO's Work	37

Figures

Figure 1: Facial Recognition Technology Search Process	6
Figure 2: Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers	9
Figure 3: Selected Federal, State, and Non-government Systems with Facial Recognition Technology Used by Federal Agencies that Employ Law Enforcement Officers, and the Number of Photos in Them	17
Figure 4: Illustration of a Facial Recognition Technology Summary	43

Abbreviations

ABIS	Automated Biometric Identification System
AutoCAT	Automated Credential Authentication Technology
BOP	Federal Bureau of Prisons
CAT-2	Credential Authentication Technology-2
CBP	U.S. Customs and Border Protection
COVID-19	Coronavirus Disease 2019
DHS	Department of Homeland Security

DOD	Department of Defense
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
HART	Homeland Advanced Recognition Technology System
ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
NASA	National Aeronautics and Space Administration
OBIM	Office of Biometric Identity Management
OMB	Office of Management and Budget
PFPA	Pentagon Force Protection Agency
Secret Service	U.S. Secret Service
TSA	Transportation Security Administration
VA	U.S. 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.

June 3, 2021

Congressional Requesters

Of all the technologies used to identify people based on their biological and behavioral characteristics, facial recognition most closely mimics how people identify others: by examining their face. Law enforcement can use facial recognition technology to assist criminal investigations, among other activities. For example, the technology can help identify an unknown individual from a photo or image from video surveillance. There are multiple ways to access the technology. Law enforcement may own facial recognition technology, or use technology that is owned by another entity (e.g., federal, state, or non-government entity). However, with use of facial recognition technology expanding, members of Congress and academics have highlighted the importance of understanding what technologies are owned and how they are used by federal law enforcement.

We previously examined aspects of federal agencies' use of facial recognition technology. In September 2020, we reported the U.S. Customs and Border Protection's (CBP) and Transportation Security Administration's (TSA) use of the technology at U.S. ports of entry.¹ In May 2016, we reported on the Federal Bureau of Investigation's (FBI) use of facial recognition technology.²

You asked us to review federal law enforcement use of facial recognition technology. This report examines:

¹GAO, *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.: September 2, 2020). In this report, GAO made five recommendations to CBP related to its use of facial recognition technology. The Department of Homeland Security concurred with our recommendations, but as of April 2021, has not implemented them.

²GAO, *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 regarding the FBI's use of facial recognition technology. The Department of Justice has addressed all six recommendations.

- 1) what federal agencies that employ law enforcement officers own and use facial recognition technology;
- 2) the type of activities these federal agencies use facial recognition technology to support; and
- 3) the extent that these federal agencies track employee use of facial recognition technology owned by non-federal entities, including state, local, tribal, territorial, and non-government entities.

This report is a public version of a sensitive report that we issued in April 2021.³ Some federal agencies deemed information in our April report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information about agency ownership and use of facial recognition technology. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To address all three objectives, we surveyed 42 federal agencies that employ law enforcement officers. Consistent with our prior work, we define federal law enforcement officers as full-time employees with federal arrest authority and who are authorized to carry firearms while on duty. To identify which agencies employ federal law enforcement officers, we reviewed the Bureau of Justice Statistics' 2016 Census of Federal Law Enforcement Officers.⁴ We included 42 of the 86 agencies identified in the 2016 census in our survey population. See appendix I for a list of the 42 federal agencies we surveyed, and information about why we selected 42 of the 86 agencies in the 2016 census.

To answer our first and second objectives, we administered a survey questionnaire to each of these 42 federal agencies. The questionnaire asked agencies whether at any point from January 2015 through March 2020, they owned a system with facial recognition technology, including

³GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-243SU (Washington, D.C.: April 28, 2021).

⁴Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016 – Statistical Tables*, NCJ 251922 (Washington, D.C.: October 2019).

systems in the process of being developed.⁵ The questionnaire asked agencies that owned a system to complete additional questions, such as the operational status of the system. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology owned by another entity.⁶ We requested additional information, through interviews and written requests, from agencies that reported in their questionnaire that they owned or used facial recognition technology. For example, if an agency reported having a system in operation, we requested privacy impact assessments and system descriptions.

To answer our third objective, we reviewed statutes and regulations, such as the Privacy Act of 1974. In addition, we interviewed or requested information from officials from 14 agencies that reported using (1) non-federal systems, and (2) facial recognition technology to support criminal investigations. We asked these officials about their process for gathering information on what non-federal systems are used by employees, and compared this information against our risk management framework and key aspects of *Standards for Internal Control in the Federal Government*

⁵We used this time frame because March 2020 was the most recent full month for which information was available when we issued our questionnaire. Also, using a 5-year period allowed us to identify technology that was recently developed but not put in operation, and identify trends in facial recognition search data. In our questionnaire, we stated that the term “own” includes systems that were procured or developed by the respective entity. In addition, we stated that a system with facial recognition technology may include a facial recognition algorithm, hardware, software, and a photo database.

⁶When pretesting our questionnaire, some agencies indicated that they could not guarantee the accuracy of the answers to this question because they did not track the use of systems owned by other entities. In some instances, employees and contractors had to work from their memory on the usage of another entity’s systems. To help mitigate this issue, we gathered this information from April 2018 (a 2-year period) instead of January 2015 (a 5-year period). For the purposes of this report, by saying an agency “used” another entity’s system, we mean that an agency’s offices, employees, and contractors (1) accessed a system owned or operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf.

(Principles 7, 10, and 16).⁷ See appendix I for additional information on our scope and methodology.

The performance audit upon which this report is based was conducted from August 2019 to April 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 based on our audit objectives. We subsequently worked with the relevant entities from April 2021 to June 2021 to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Background

How Facial Recognition Technology Works

Biometric technologies can identify individuals by measuring and analyzing biological and behavioral characteristics such as a fingerprint, face, iris, heartbeat, voice, and gait (i.e., a person's manner of walking). Facial recognition is one type of biometric technology. 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.⁸

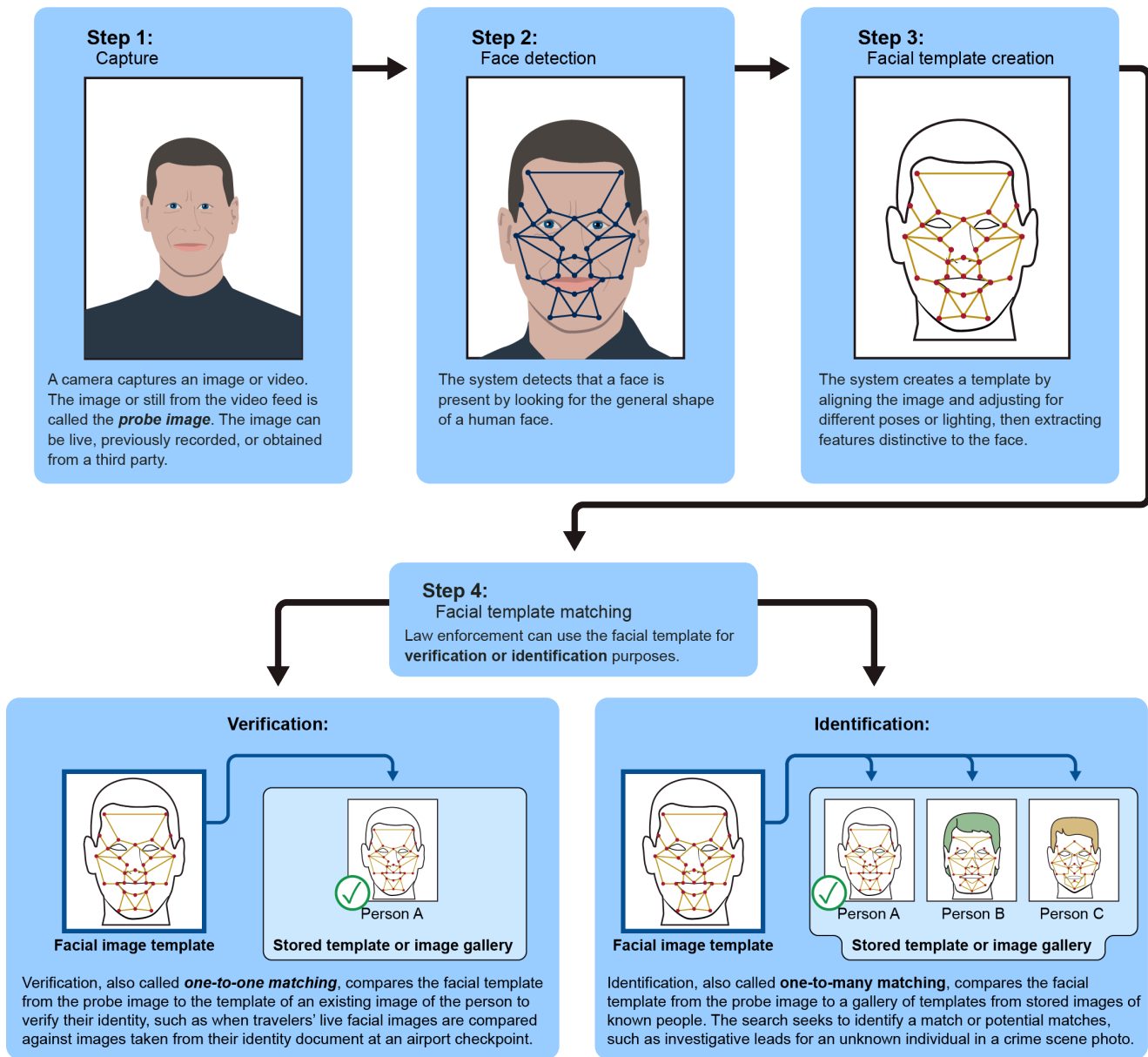
Facial recognition searches generally fall into two categories: verification and identification. Verification (or one-to-one searches) compares a photo to another photo of the same individual. For example, this type of search

⁷GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C.: Dec. 1, 2016). Also see: GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014). Principle 7 states that management should identify, analyze, and respond to risks related to achieving the defined objectives. Principle 10 states that management should design control activities to achieve objectives and respond to risks. Principle 16 states that management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

⁸An algorithm is a set of rules that a computer or program follows to compute an outcome. Private companies have developed facial recognition algorithms for a variety of uses.

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 photos from a number of individuals to determine if there is a potential match. Importantly, identification searches can be used to generate investigative leads (i.e., potential matches) for criminal investigations. Figure 1 shows the process of a facial recognition search, including verification and identification searches.

Figure 1: Facial Recognition Technology Search Process



Source: GAO analysis. | GAO-21-518

Federal and Non-Federal Systems with Facial Recognition Technology

Federal law enforcement can use systems with facial recognition technology owned by their respective agencies. They can also use systems owned by other government entities, including federal, state, local, tribal, and territorial governments. Moreover, federal law enforcement can use non-government facial recognition service providers, such as Vigilant Solutions and Clearview AI. For example, law enforcement officers with a Clearview AI account can use a computer or smartphone to upload a photo of an unknown individual to Clearview AI's facial recognition system. The system can return search results that show potential photos of the unknown individual, as well as links to the site where the photos were obtained (e.g., Facebook). According to Clearview AI, its system is only used to investigate crimes that have already occurred and not for real-time surveillance. In addition, Clearview AI noted that its system uses images publicly available on the internet, and search results should only be used by law enforcement as investigative leads.

Law enforcement officers may also have access to another entity's system—that is, the officer can log into the system and conduct a facial recognition search. Alternatively, a law enforcement officer can request that another entity use its system to conduct facial recognition searches on their behalf. For example, a federal law enforcement officer may ask a state entity to conduct facial recognition searches on their behalf.

Privacy Laws and Rules

Several statutory requirements govern the protection of personal information by federal agencies, including federal law enforcement's use of facial images. For example, the Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records (e.g. photos). According to Office of Management and Budget (OMB) officials, the Privacy Act and OMB Circular A-130 generally provide that agencies must ensure that privacy requirements apply to systems operated by contractors or other entities on behalf of the Federal Government, which could include facial recognition service providers.

Accuracy of Facial Recognition Technology

The accuracy of facial recognition technology can be characterized in a number of ways. For example, a false positive rate is how often the technology incorrectly declares two images to be a match when they are actually from two different people. In addition, a false negative rate is how often the technology fails to declare two images to be a match when they are actually from the same person. Matching errors can be caused not only by the quality of the facial recognition technology, but also by the quality of the photos used in the matching process and other factors. The National Institute of Standards and Technology has conducted research into the accuracy of facial recognition algorithms. It has evaluated hundreds of commercial facial matching algorithms for accuracy and speed since 2000.

Twenty Federal Agencies Reported Owning or Using Systems with Facial Recognition Technology

Of the 42 agencies we surveyed, 20 reported that they owned a system with facial recognition technology or used another entity's system.⁹ As shown in figure 2, three agencies only owned a system, 12 agencies only used another entity's system, and five agencies both owned a system and used another entity's system. These 20 federal agencies collectively employ roughly 120,000 federal law enforcement officers.¹⁰ According to agencies that owned or used systems, these systems can include hundreds of millions or billions of photos of various types.

⁹We asked agencies whether at any point from January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned/operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf. See the complete list of agencies that received our questionnaire in appendix I.

¹⁰These agencies employed roughly 120,000 federal law enforcement officers as of September 30, 2016, based on Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016 – Statistical Tables*, NCJ 251922 (Washington, D.C.: October 2019).

Figure 2: Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers



Source: GAO analysis of survey data. | GAO-21-518

Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. We asked agencies whether at any point during January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned or operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf.

The owned system columns include systems in the process of being developed. The National Aeronautics and Space Administration's Office of Protective Services reported that it did not purchase

facial recognition technology. However, we included the agency in the owned column because they used a commercial-off-the-shelf product with facial recognition technology to conduct a proof of concept test to determine whether the technology was suitable for its purposes.

Eight Agencies Reported Owning Systems with Facial Recognition Technology

Eight of the 42 federal agencies reported owning 17 systems with facial recognition technology from January 2015 through March 2020.¹¹ In addition, one of the eight agencies reported that it was in the process of procuring two systems during this time period, but had not finalized the purchase as of March 2020.¹²

Table 1 below lists these 19 systems (17 owned and two in procurement) and their statuses as of March 31, 2020. Four of the 19 systems were in operation as of March 31, 2020, and were owned by three agencies: the FBI, Federal Bureau of Prisons, and CBP. Detailed descriptions of the 19 systems can be found in appendix II.

Detailed System Descriptions, Including Systems Listed in Table 1, Can be Found in Appendix II and III of This Report


An example of a system description is illustrated below. These descriptions include how agencies use the systems with facial recognition technology, whether the systems have a photo database, system users, and system statuses, among other information.

DESCRIPTION OF OWNED SYSTEMS

Traveler Verification Service

PURPOSE AND DESCRIPTION

The Traveler Verification Service uses facial recognition technology to verify the identity of international travelers entering and exiting the United States. CBP is testing and evaluating the Traveler Verification Service in phases throughout the air, sea, and land travel environments at ports of entry. The system uses real-time capability to compare a traveler's live photo to photos stored in DHS databases (such as passport photos, or to a photo embedded in a travel identification document. Specifically, the system searches DHS databases of photos associated with individuals listed on the travel manifest, and it then creates a preselected "gallery" of templates created from those photos. CBP uses these "galleries" for matching purposes only and deletes them from the system within 12 hours. CBP plans to use the Traveler Verification Service for all travel environments, but the agency prohibits facial recognition technology in the air environment.



Source: U.S. Customs and Border Protection | GAO-21-518

SYSTEM CHARACTERISTICS

Type of searches: **One-to-one and One-to-many**

Real-time or near real-time capability: **Yes**

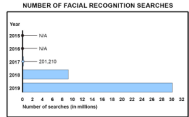
Includes photo database: **Yes**

Number of photos in database: **Not applicable (see description)**

Types of photos in database

- Passport photos
- U.S. entry/exit photos
- Visa application photos

NUMBER OF FACIAL RECOGNITION SEARCHES



Year
2014
2015
2016
2017
2018
2019

Number of searches (in millions)

OTHER SYSTEM USERS (EXAMPLES)

Transportation Security Administration

STATUS

As of March 31, 2020, the Traveler Verification Service was in operation and one external entity had access to the system. Specifically, the Transportation Security Administration is piloting the Traveler Verification Service to determine whether it can leverage the capability to improve and automate security processes.

¹¹According to CBP, this system is covered by a Privacy Impact Assessment and a System of Records Notice. In addition, while legislation and CBP's collection of biometric information to certain foreign nationals entering and exiting the United States, CBP's domestic entry/exit capabilities may also use biometric data (such as fingerprints) from exempt foreign nationals and U.S. citizens. However, exempt foreign nationals and U.S. citizens are routinely able to "opt out" of using this technology to verify their identity and can instead photos in a range of circumstances for identity verification.

¹²Although the Traveler Verification Service system accesses photos from other DHS photo databases for matching purposes, it does not share the photos long term. The photos are deleted from the Traveler Verification Service system within 12 hours. More information on the Traveler Verification Service can be found at GAO-20-568.

¹³In one instance, we mean comparing a probe photo to a photo of a person of unknown or unconfirmed identity to another single photo. By one-to-many, we mean comparing a probe photo to two or more photos.

Source: GAO. I GAO-21-518

¹¹This report omits some information about systems owned by agencies we surveyed, as the relevant agencies deemed the information sensitive.

¹²The Department of Veterans Affairs Police Service was in the process of procuring the AnyVision and Motorola Avigilon Appearance Search systems as of March 31, 2020. The agency also owned the Aventura and Veritone aiWARE systems during the period of our review.

Table 1: Systems with Facial Recognition Technology that Federal Agencies Employing Law Enforcement Officers Reported as Owned or in Procurement, January 2015 through March 2020, and System Status

Department	Federal Agency	System Name	System Status as of March 31, 2020 ^a
Justice	Federal Bureau of Investigation	Next Generation Identification Interstate Photo System	In operation
		Horus	In development
		Rank One	In development
		Automatic Face Detection and Recognition/Cluster Base	Not in use
		Camera with Facial Recognition Software	Not in use
		NeoFace Reveal	Not in use
Homeland Security	Federal Bureau of Prisons	Facial Recognition Access Control System	In operation
	U.S. Customs and Border Protection	Automated Targeting System	In operation
		Traveler Verification Service	In operation
	Transportation Security Administration	Automated Credential Authentication Technology	In development
		Credential Authentication Technology-2	In development
U.S. Secret Service	Facial Recognition Pilot	Not in use	
Veterans Affairs	Police Service	AnyVision	In development
		Motorola Avigilon Appearance Search	In development
		Aventura	Not in use
		Veritone aiWARE	Not in use
Defense	Pentagon Force Protection Agency	Briefcam ^b	Not in use
		Sirchie	Not in use
National Aeronautics and Space Administration	Office of Protective Services	FaceFirst	Not in use

Legend: ● In operation; ○ In development (e.g., being tested) or procurement; ⊗ Not in use

Source: GAO analysis of survey data. | GAO-21-518

Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. We asked agencies whether, at any point from January 2015 through March 2020, they owned or were in the process of procuring a system with facial recognition technology, including systems in the process of being developed. This table omits some information about systems owned by agencies we surveyed, as the relevant agency deemed the information sensitive.

^aThe system status category “Not in use” refers to systems that agencies owned from January 1, 2015 through March 31, 2020; however, the system was not in use as of March 31, 2020. For example, agencies reported that they no longer used a system, or tested a system and determined it was not suitable for their purposes.

^bThe Briefcam system was in operation as of March 31, 2020; however, according to Pentagon Force Protection Agency officials, the facial recognition technology component of this system was not in operation. As such, the status of this system is marked “Not in use.”

Seventeen Federal Agencies Reported Using Systems Owned by Other Entities

Seventeen of the 42 federal agencies reported using another entity’s system with facial recognition technology from April 2018 through March 2020. Of the 17 agencies, 15 reported using systems owned by another federal entity; 14 reported using systems owned by state, local, tribal, or territorial entities; and 11 reported using systems owned by non-government entities. Furthermore, nine of the 17 agencies reported using systems owned by all three types of entities. See table 2 for additional information.

Table 2: Reported Use of Other Entities’ Facial Recognition Technology by Federal Agencies that Employ Law Enforcement Officers

Federal Agency That Used System	Type of Entity That Owned System				
	Other Federal	State, Local, Tribal, Territorial	Non-Government ^a		
			Clearview AI	Vigilant Solutions	Other Non-Government ^b
Bureau of Diplomatic Security	Used	Used	Used	Used	Used
U.S. Customs and Border Protection	Used	Used	Used	Used	Used
U.S. Marshals Service	Used	Used	Used	Used	Used
Bureau of Alcohol, Tobacco, Firearms and Explosives	Used	Used	Used	Used	Did not use
U.S. Immigration and Customs Enforcement	Used	Used	Used	Did not use	Used
U.S. Postal Inspection Service	Used	Used	Used	Used	Did not use
Drug Enforcement Administration	Used	Used	Used	Did not use	Did not use
Federal Bureau of Investigation	Used	Used	Used	Did not use	Did not use
U.S. Secret Service	Used	Used	Used	Did not use	Did not use
U.S. Capitol Police	Used	Used	Did not use	Did not use	Did not use
U.S. Fish and Wildlife Service	Used	Used	Did not use	Did not use	Did not use
Food and Drug Administration, Office of Criminal Investigations	Used	Used	Did not use	Did not use	Did not use
Internal Revenue Service, Criminal Investigation Division	Used	Used	Did not use	Did not use	Did not use
U.S. Park Police	Did not use	Used	Used	Did not use	Did not use
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	Did not use	Did not use	Did not use	Did not use	Used
Pentagon Force Protection Agency	Used	Did not use	Did not use	Did not use	Did not use
Transportation Security Administration	Used	Did not use	Did not use	Did not use	Did not use
Total	15	14	10	5	5

Legend:

✓ Agency used a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020. For federal, state, local, tribal, and territorial entities, the term “used” includes an agency’s offices, employees, or contractors (1) accessing a system owned/operated by the respective entity type, or (2) requesting that the respective entity type use its system to conduct a facial recognition search on the agency’s behalf. For non-government entities, the term “used” means the agency’s offices, employees, or contractors submitted photos to the respective non-government service provider for the purpose of conducting a facial recognition search.

— Agency did not use a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020.

Source: GAO analysis of survey data. | GAO-21-518

^aSome agencies reported that they only used Clearview AI or Vigilant Solutions on a free trial basis, and thus, did not enter into a formal contract with the service provider.

^bOther non-government entities that agencies reported using included Amazon Rekognition, BI SmartLink, and Giant Oak Social Technology, among others.

As discussed above, 15 agencies reported using a system owned by another federal entity. Ten of these agencies reported using systems owned by other federal agencies we surveyed. For example, the Transportation Security Administration reported using the U.S. Customs and Border Protection’s Traveler Verification Service. Agencies also reported using systems that were owned by federal entities that we did not survey. Specifically, based on survey responses, multiple agencies reported using the three systems listed in the table below. More information on each of these systems can be found in appendix III.

Table 3: Select Systems with Facial Recognition Technology Owned by Federal Agencies

System Name	Federal Agency That Owns System
Automated Biometric Identification System (ABIS)	Defense Forensic Science Center (Department of Defense)
Automated Biometric Identification System (IDENT)	Office of Biometric and Identity Management (Department of Homeland Security)
Integrated Biometric System	Bureau of Consular Affairs (Department of State)

Source: GAO analysis of survey data. | GAO-21-518

Examples of Federal Agencies Partnering with State and Local Entities

- Food and Drug Administration’s (FDA) Office of Criminal Investigations reported using the Georgia Department of Driver Services’ facial recognition technology. FDA reported using the technology to verify the identity of an individual under investigation who had assumed a stolen identity.
- U.S. Immigration and Customs Enforcement (ICE) reported helping to fund the development of a system with facial recognition technology that Lehigh County Regional Investigation and Intelligence Center (the Center) will own. Specifically, ICE and the Center are developing the National Capital Region Gang Intelligence Application to combat transnational gangs, according to ICE officials. Officials told us that once developed, ICE can use the system’s facial recognition technology to compare images of unknown individuals to a gallery of known and suspected gang members.
- U.S. Park Police reported that it asked a state agency to use facial recognition technology to help identify a deceased individual in a park. The state agency used a free trial with a non-government service provider to conduct the search, according to U.S. Park Police.



Source: GAO analysis of survey data, zfmbe/stock.adobe.com. | GAO-21-518

Fourteen federal agencies reported using systems owned by state, local, tribal, and territorial entities. For example, FBI’s Facial Analysis, Comparison, and Evaluation Services had memorandums of understanding with certain state agencies, allowing it to leverage the state-owned systems for facial recognition searches.¹³ According to the FBI, these state-owned systems include driver’s license photos, mugshots, or corrections photos.

Eleven agencies we surveyed used systems with facial recognition technology belonging to non-government entities, including Clearview AI (10 agencies) and Vigilant Solutions (five agencies).¹⁴ Ten agencies reported having used non-government facial recognition service providers on a free trial basis. For example, according to the U.S. Postal Inspection Service, it had a free trial with Vigilant Solutions that lasted approximately 10 months in 2017.

¹³The FBI’s Facial Analysis, Comparison, and Evaluation Services is located in the Investigative Services Support Unit of the Criminal Justice Information Services Division. It conducts facial recognition searches on the FBI’s Next Generation Identification Interstate Photo System and can request external partners perform searches on their facial recognition systems to support FBI active investigations.

¹⁴Information regarding the extent that agencies used Clearview AI and Vigilant Solutions has been omitted from this report, as some agencies deemed the information sensitive.

Agencies Reported Using Systems that Varied in the Number and Type of Photos

Types of Photos Used by Federal Agencies that Employ Law Enforcement Officers

Federal agencies reported using a number of systems with facial recognition technology. The following list includes examples of the types of photos included in these systems, as reported by system owners and users:

- Mug shot
- Publicly available on the internet
- Passport
- Visa application
- U.S. entry/exit
- Video/Closed Circuit Television
- Terrorist Screening Database
- Foreign nationals and U.S. citizens who are known or suspected threats to the nation
- Employee
- State identification
- Driver's license
- Corrections
- Individuals under supervision

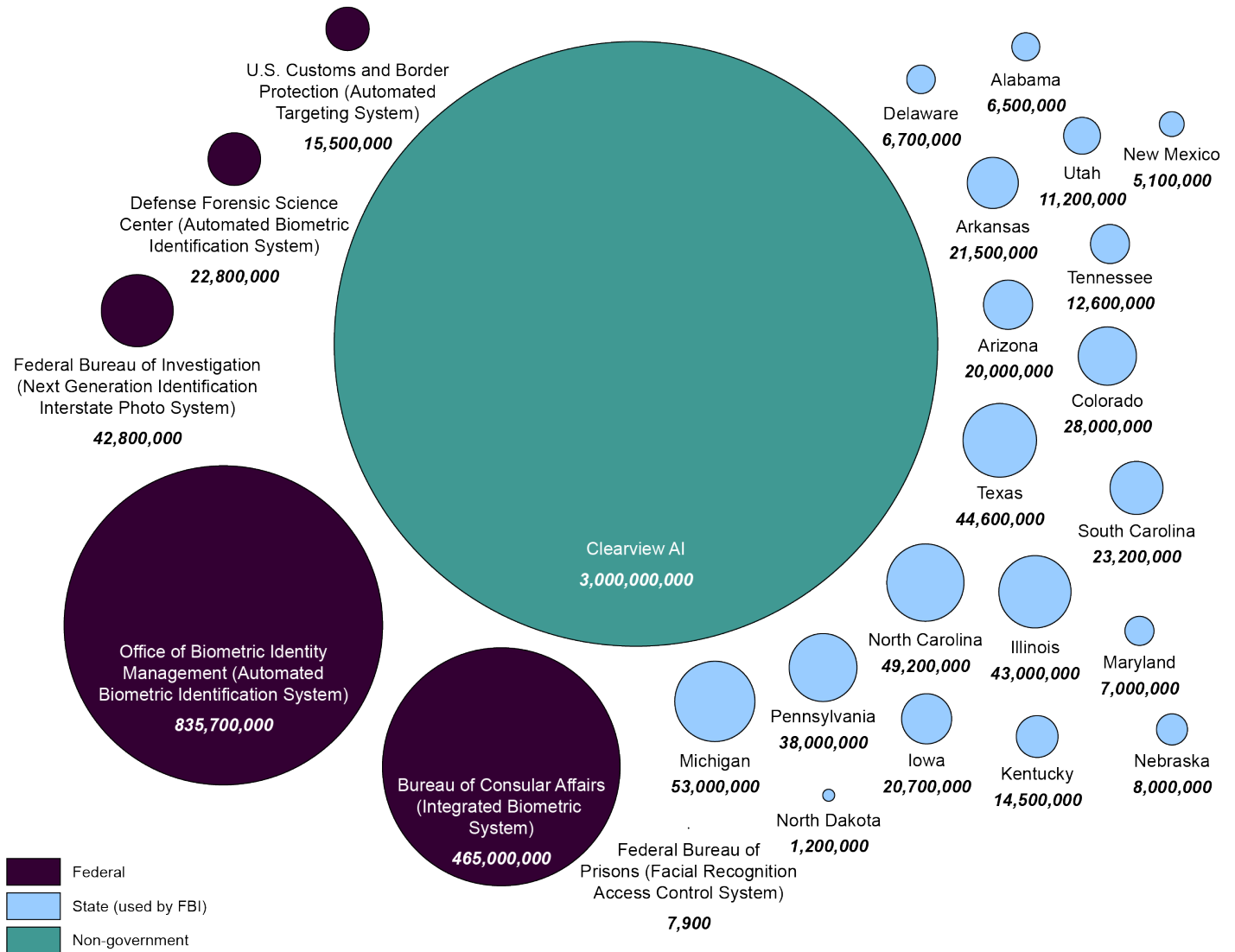


Source: GAO analysis of survey data, liidiiia/stock.adobe.com.
I GAO-21-518

Federal agencies reported using numerous systems with facial recognition technology, and sometimes these systems included stored photos. The number and types of photos within these systems can vary, based on information reported by agencies and system owners. For example, as of March 31, 2020, the Bureau of Prisons' Facial Recognition Access Control System included roughly 8,000 photos of its employees and contractors. Other systems include millions or billions of photos. For example, the Office of Biometric and Identity Management reported that its Automated Biometric Identification System (IDENT) included roughly 836 million facial images as of March 31, 2020. According to agency officials, the types of photos include visa application, passport, mug shot, and others. Clearview AI told us its system includes roughly 3 billion publicly available photos gathered from the internet.

Figure 3 below shows examples of federal, state, and non-government systems with facial recognition technology that federal agencies reported using, and the number of photos in them. Appendix II includes additional information on photos, including the number and type of photos in systems owned by federal agencies we surveyed.

Figure 3: Selected Federal, State, and Non-government Systems with Facial Recognition Technology Used by Federal Agencies that Employ Law Enforcement Officers, and the Number of Photos in Them



Source: GAO analysis of information provided by system users or owners. | GAO-21-518

Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. This figure includes examples of systems used by one or more federal agencies we surveyed. It does not include all systems used by these agencies. The figure includes the number of photos stored in the respective entity's system with facial recognition technology, as of March 31, 2020.

The same individual may be included in multiple photos within one photo database or across multiple databases, and the same photo can exist within multiple databases. Some entities providing these numbers indicated they were estimates. The number of photos for federal and non-government entities were reported by the respective system owner. The number of photos for state entities were all reported by the Federal Bureau of Investigation (FBI). Specifically, the FBI's Facial Analysis,

Comparison, and Evaluation Services has memorandums of understanding with several state agencies, allowing it to leverage the state-owned systems for facial recognition searches. The FBI provided the number of photos they can access via these memorandums of understanding.

Federal Agencies Reported Using Systems with Facial Recognition Technology to Support Various Activities

Most federal agencies that owned or used facial recognition technology reported using it to support criminal investigations. Agencies also reported using facial recognition technology for activities such as surveillance, traveler verification, and research and education.

Of the 20 federal agencies that owned or used facial recognition technology, 14 reported using the technology to support criminal investigations. For example, the FBI's Next Generation Identification Interstate Photo System allows users to search a database of over 40 million photos. The system returns a list of potential candidates that law enforcement can use to generate investigative leads. According to the FBI, the system has been used for investigations of violent crimes, credit card and identity fraud, missing persons, and bank robberies, among others. The Department of Homeland Security's Office of Biometric Identity Management offers a similar service to its partners (e.g., U.S. Immigration and Customs Enforcement). Specifically, the agency's Automated Biometric Identification System can be used to search a photo of an unknown individual and provide potential matches (i.e., generate leads) to support criminal investigations. Federal agencies also reported using state, local, and non-government systems to support criminal investigations.

Six agencies reported using facial recognition technology during May through August 2020 to support criminal investigations related to civil unrest, riots, or protests.¹⁵ Following the death of George Floyd while in the custody of the Minneapolis, Minnesota police department on May 25,

¹⁵We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system. See more information on our methodology in appendix I.

2020, nationwide civil unrest, riots, and protests occurred.¹⁶ Six agencies told us that they used images from these events to conduct facial recognition searches during May through August 2020 in order to assist with criminal investigations (see table 4). All six agencies reported that these searches were on images of individuals suspected of violating the law.

Table 4: Federal Agency Reported Use of Facial Recognition Technology on Images of Individuals Suspected of Violating the Law during Civil Unrest, Riots, or Protests, May through August 2020

Federal Agency	How Agency Reported Using Facial Recognition Technology
Bureau of Alcohol, Tobacco, Firearms and Explosives	In a single instance, used facial recognition technology owned by another law enforcement entity. The search was conducted to help identify an individual suspected of violating the law during the period of civil unrest, riots, or protests.
U.S. Capitol Police	Requested that the Montgomery County Department of Police (Montgomery County, Maryland) conduct facial recognition searches to assist with a criminal investigation. The purpose of the searches was to help identify individuals that confronted and made threats to a member of Congress and the member's spouse outside the White House during the period of civil unrest, riots, or protests.
Federal Bureau of Investigation	Created a digital media tip line and solicited images of people involved in criminal activity during the period of civil unrest, riots, or protests. The agency sought to identify or locate criminal suspects seen in images and video depicting criminal behavior by conducting facial recognition searches using its Next Generation Identification Interstate Photo System.
U.S. Marshals Service	Used a non-government facial recognition service provider, to conduct facial recognition searches related to criminal investigations on images from the period of civil unrest, riots, or protests.
U.S. Park Police	Requested that the Maryland National Capital Park Police conduct a facial recognition search using an image from Twitter to identify an individual who allegedly assaulted an officer during the period of civil unrest, riots, or protests. The search was conducted on the National Capital Region Facial Recognition Investigative Leads System. The subject was ultimately charged with Felony Civil Disorder and two counts of Assault on a Police Officer.
U.S. Postal Inspection Service	Used Clearview AI to help identify individuals suspected of criminal activity that took place in conjunction with the period of civil unrest, riots, or protests. This criminal activity included damaging U.S. Postal Service property, stealing mail, opening mail, burglarizing U.S. Postal Service buildings, and committing arson.

Source: GAO analysis of survey data. | GAO-21-518

In addition, with regard to the January 6, 2021 events at the U.S. Capitol complex, three agencies reported using facial recognition technology to support criminal investigations related to the civil unrest, riots, or

¹⁶In September 2020, we reported that federal agencies deployed 16 tactical teams in relation to the civil unrest and protests. See: GAO, *Federal Tactical Teams: Characteristics, Training, Deployments, and Inventory*, [GAO-20-710](#) (Washington, D.C.: September 2020).

protests.¹⁷ The three agencies reported using the technology to support criminal investigations as follows:

- U.S. Capitol Police used Clearview AI to help generate investigative leads. The agency also requested that another federal agency use its system to conduct facial recognition searches on behalf of the U.S. Capitol Police.
- CBP used its Automated Targeting System to conduct searches at the request of another federal agency.
- Bureau of Diplomatic Security used the Department of State's Integrated Biometric System to conduct searches at the request of another federal agency.

Agencies also reported using facial recognition technology beyond criminal investigations. The following list includes examples of use cases, as reported by agencies. Appendix II includes more information on these use cases and others.

- **Surveillance.** The U.S. Secret Service (Secret Service) piloted a system with facial recognition technology to determine whether it could be incorporated into the agency's White House Complex security operations. Specifically, the Secret Service stored photos of 23 volunteer employees within the system. As volunteers moved throughout the White House Complex, their images were captured by closed-circuit television cameras. In real time, the system compared the stored photos to images from the video footage to determine whether they represented the same individual. Secret Service told us it did not plan to implement the system based on the results of the pilot.
- **Response to Coronavirus Disease 2019 (COVID-19).** In response to COVID-19, the Administrative Office of the U.S. Courts, Probation and Pretrial Services office began using facial recognition technology. The technology allowed individuals under court-ordered supervision to verify their identity via a smart phone application rather than physical contact with a probation or pretrial officer. According to agency

¹⁷We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system. See more information on our methodology in appendix I. Twelve agencies reported that they did not use the technology for these purposes, three agencies reported using the technology, and two agencies told us they could not answer our questions because the information pertains to ongoing investigations.

officials, the program is limited to voluntary use by individuals under supervision in connection with court-ordered location or alcohol monitoring.

- **Traveler verification.** CBP's Traveler Verification Service uses facial recognition technology to verify the identity of travelers entering and exiting the United States.¹⁸ CBP is testing and deploying the Traveler Verification Service in phases throughout the air, sea, and land travel environments at ports of entry. The system uses real-time capability to compare a traveler's live photo to photos stored in Department of Homeland Security databases, such as passport photos, or to a photo embedded in a travel identification document.
- **Area access.** The Federal Bureau of Prisons (BOP) uses its Facial Recognition Access Control System to authenticate entry into secure network operations centers at certain BOP facilities. The system verifies BOP employees' identities using facial recognition technology, and once confirmed, employees can enter the operations centers.
- **Research and education.** The FBI is using systems for research and education purposes. For example, it is examining how well systems perform when used on its casework. In addition, the bureau is trying to determine whether these systems could be incorporated into its one-to-one comparisons process. Currently, FBI forensic examiners manually compare two images to validate whether faces within the images represent the same individual (i.e., one-to-one comparisons). The FBI is researching whether it would be beneficial to use a facial recognition system in addition to forensic examiners. It is also using systems in educational settings to demonstrate how facial recognition technology works.

¹⁸While regulations limit CBP's collection of biometric information to certain foreign nationals entering and exiting the United States, CBP's biometric entry-exit capabilities may also capture biometric data (facial images) from exempt foreign nationals and U.S. citizens. However, exempt foreign nationals and U.S. citizens are routinely able to "opt out" of using this technology to verify their identity and can instead choose a manual check of documentation for identity verification. For more information, see [GAO-20-568](#).

Most Agencies Do Not Track Non-Federal Systems in Use or Related Risks

Thirteen federal agencies do not have awareness of what non-federal systems with facial recognition technology are used by employees.¹⁹ These agencies have therefore not fully assessed the potential risks of using these systems, such as risks related to privacy and accuracy. Most federal agencies that reported using non-federal systems did not own systems. Thus, employees were relying on systems owned by other entities, including non-federal entities, to support their operations.

Tracking Use of Non-Federal Systems

We found that 13 of 14 agencies that reported using non-federal systems do not have complete, up-to-date information on what non-federal systems are used by employees.²⁰ For example, when we requested information from one of the agencies about its use of non-federal systems, agency officials told us they had to poll field division personnel because the information was not maintained by the agency. These agency officials also told us that the field division personnel had to work from their memory about their past use of non-federal systems, and that they could not ensure we were provided comprehensive information about the agency's use of non-federal systems. Officials from another agency initially told us that its employees did not use non-federal systems; however, after conducting a poll, the agency learned that its employees had used a non-federal system to conduct more than 1,000 facial recognition searches.

One agency—the U.S. Immigration and Customs Enforcement—reported that it was in the process of implementing a mechanism to track what

¹⁹Throughout this section, when we say that an agency did not have awareness of what systems are used by employees, we are referring to both the agency's employees and contractors. By non-federal systems, we are referring to systems owned by state, local, tribal, territorial, and non-government entities.

²⁰By complete, up-to-date information, we mean that an agency has ongoing knowledge of what non-federal systems with facial recognition technology are used by employees. Fifteen agencies reported using non-federal systems; however, we excluded U.S. Probation and Pretrial Services because it does not use facial recognition technology to support criminal investigations. All 14 agencies discussed in this section reported using the technology to support criminal investigations.

non-federal systems are used by employees.²¹ According to U.S. Immigration and Customs Enforcement officials, in November 2020 they were in the process of developing a list of approved facial recognition technologies that employees can use. In addition, log-in sheets will be made available to employees, allowing supervisors to monitor employee use of the technologies. The agency will allow the use of non-reviewed systems under exigent circumstances; however, supervisor approval is required. The use of systems that have been reviewed and not approved for use is strictly prohibited, even in exigent circumstances, according to U.S. Immigration and Customs Enforcement.

However, the other 13 agencies do not have complete, up-to-date information because they do not regularly track this information and have no mechanism in place to do so (see table 5).²² For example, the Criminal Investigation Division within the Internal Revenue Service told us it does not track what non-federal systems are used by employees because it is not the owner of these technologies. Similarly, the U.S. Postal Inspection Service said it did not track what systems employees use because it is the responsibility of the system owner to govern use of the system.

Table 5: Federal Agency Tracking of Employee Use of Non-Federal Systems with Facial Recognition Technology

Federal Agency	Have Mechanism to Track What Non-Federal Systems Are Used by Employees
U.S. Immigration and Customs Enforcement	Yes
Bureau of Alcohol, Tobacco, Firearms and Explosives	No
Bureau of Diplomatic Security	No
U.S. Capitol Police	No
U.S. Customs and Border Protection	No
Drug Enforcement Administration	No
Federal Bureau of Investigation	No
U.S. Fish and Wildlife Service	No

²¹According to U.S. Immigration and Customs Enforcement officials, only employees within its Homeland Security Investigations will be subject to the procedures, as only employees within this component of the agency use facial recognition technology.

²²We asked agencies whether they had a mechanism to track *what systems* were used by employees, not whether agencies track *each individual use of a system* by employees.

Federal Agency	Have Mechanism to Track What Non-Federal Systems Are Used by Employees
Food and Drug Administration, Office of Criminal Investigations	No
Internal Revenue Service, Criminal Investigation Division	No
U.S. Marshals Service	No
U.S. Park Police	No
U.S. Postal Inspection Service	No
U.S. Secret Service	No

Source: GAO analysis of agency information. | GAO-21-518

Note: Federal agencies marked “No” may have known that employees used certain systems, but they do not have a mechanism to provide complete, up-to-date information of what systems are used by employees.

Standards for Internal Control in the Federal Government state that agencies should design and implement controls to help achieve agencies’ objectives, which, in this case, is to conduct investigative activities.²³

These standards also state that ongoing monitoring—such as regular oversight that would provide visibility into the non-federal systems used by employees—should be performed continually in the course of normal operations.

Internal control standards further underscore that management should identify, analyze, and respond to risks related to achieving the defined objectives. Additionally, we have previously reported that enterprise risk management can help federal agencies assess risks, such as those related to the use of non-federal systems.²⁴ For example, assembling a list of risks can help an agency identify threats that could limit its ability to achieve goals and objectives.

By implementing a mechanism to track what non-federal systems with facial recognition technology are used by employees, agencies will be able to have visibility into the systems that employees are relying on to assist with investigative activities.²⁵ Gathering this information on a continuous basis can serve as an important initial step to identifying risks associated with non-federal systems. When asked about the potential implementation of a mechanism to track what systems are used by

²³GAO-14-704G.

²⁴GAO-17-63.

²⁵This sentence describes the potential benefits of tracking what systems are used by employees, and not each individual use of a system by employees.

employees, seven of the 13 agencies told us that it was feasible or did not express any specific concerns. The other six agencies did not comment.

Assessing Risks Related to Non-Federal Systems

As 13 federal agencies do not have awareness of non-federal systems used by employees, they cannot fully assess the risks of using these systems. Numerous risks to federal agencies and the public can accompany the use of facial recognition technology. In particular, these risks can relate to privacy and the accuracy of a system.

Several privacy-related requirements govern the protection of personal information by federal agencies, including federal law enforcement's use of facial images. For example, the Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records (e.g. photos).²⁶ Additionally, according to OMB officials, the E-Government Act of 2002 and OMB Privacy policy requirements necessitate that when an agency procures information technology that processes personally identifiable information from outside services, such as a third-party vendor or state or local government, agencies must conduct an assessment of the privacy implications.²⁷

When agencies use facial recognition technology without first assessing the privacy implications and applicability of privacy requirements, there is a risk that they will not adhere to privacy-related laws, regulations, and policies. There is also a risk that non-federal system owners will share sensitive information (e.g. photo of a suspect) about an ongoing investigation with the public or others. In addition, privacy advocacy organizations, government agencies, academics, and some industry representatives have raised privacy and security concerns. For example, there is a risk that data sets with personal information could be subject to breaches, resulting in sensitive biometric data being revealed to

²⁶See 5 U.S.C. § 552a(4). Per OMB guidance and the Federal Acquisition Regulation, agency obligations to maintain privacy protections and adhere to the Privacy Act of 1974 obligations extend to information technology systems that are used or operated by contractors or other entities on behalf of the federal government or that collect or maintain federal information on behalf of the federal government. See Office of Management and Budget Memorandum (OMB) Circular A-130, Managing Information as a Strategic Resource (July 28, 2016); Federal Acquisition Regulation, Subpart 24.1 Protection of Individual Privacy.

²⁷See Pub. L. No. 107-347, 116 Stat. 2899 (2002).

unauthorized entities. Because a person's face is distinctive, permanent, and therefore irrevocable, a breach involving data derived from a face may have more serious consequences than the breach of other information, such as passwords, which can be changed.

The U.S. Immigration and Customs Enforcement assessed privacy risks associated with its use of facial recognition technology, including non-federal systems.²⁸ The assessment was reviewed by the Chief Privacy Officer for the Department of Homeland Security. In the assessment, the agency identified privacy risks and what, if any, actions it can take to mitigate these risks. For example, as part of its process, before using a non-federal systems the agency plans to ensure that:

- methods of transmission of a probe photo are properly encrypted,
- no probe photos submitted by U.S. Immigration and Customs Enforcement are retained by the system owner or shared with other parties, and
- appropriate safeguards for housing sensitive personally identifiable information exist.

Accuracy rates can help agencies determine how often facial recognition technology correctly or incorrectly declares that two or more images match. Matching errors can be caused by the quality of the facial recognition technology, and other factors such as the quality of photos used in the matching process. Although the accuracy of facial recognition technology has increased dramatically in recent years, risks still exist that searches will provide inaccurate results. For example, if a system is not sufficiently accurate, it could unnecessarily identify innocent people as investigative leads. The system could also miss investigative leads that could otherwise have been revealed. In December 2019, the National Institute of Standards and Technology reported that facial recognition algorithms it tested differed in accuracy widely by race, ethnicity, or

²⁸Department of Homeland Security, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services*, DHS/ICE/PIA-054 (May 13, 2020).

country of origin, as well as by gender and age.²⁹ In addition, some members of Congress, privacy groups, and others have expressed concerns that facial recognition technology's higher error rates for certain demographics could result in disparate treatment, profiling, or other adverse consequences for members of these populations.

The U.S. Immigration and Customs Enforcement, as part of the risk assessment described earlier, also considered the accuracy of non-federal systems. According to the assessment, the agency will leverage resources such as the National Institute of Standards and Technology's testing on the accuracy and bias of systems. Additionally, the agency said it will conduct non-scientific tests to gain insight into the veracity of a system.

However, as the other 13 federal agencies do not have awareness of non-federal systems used by employees, they cannot fully assess the risks (e.g., privacy and accuracy-related risks) of using these systems. As described earlier, we have previously reported that assembling a list of risks can help an agency identify threats to achieving its goals and objectives. In addition, prioritizing identified risks and selecting the most appropriate treatment strategy to manage the risks are important next steps.

Without assessing the risks of using non-federal systems, agencies are more susceptible to risks that negatively affect their ability to meet stated goals and objectives. For example, agencies cannot ensure appropriate privacy safeguards are in place to prevent the mishandling of personal information when using non-federal systems. In addition, agencies cannot ensure they are using systems sufficiently accurate for their purposes.³⁰ Failure to appropriately assess risks when using non-federal systems with facial recognition technology could ultimately result in a reputational

²⁹National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST Interagency or Internal Report 8280 (Dec. 19, 2019). The National Institute of Standards and Technology reported that it tested 189 mostly commercial algorithms from 99 developers and that performance differences varied by the algorithms tested, with some performing better than others. For a small number of the one-to-many algorithms, differences in false positives across demographic groups were undetectable. The extent of performance differences varied by the developer, type of error, and quality of the facial images.

³⁰This sentence describes the potential benefits of understanding and managing accuracy-related risks, which may or may not result in agencies testing the accuracy of individual systems used by employees.

catastrophe, hindering an agency's efforts to meet its core mission for years.

Conclusions

Facial recognition technology is a powerful tool used by the federal law enforcement community. Federal agencies that employ law enforcement officers rely on systems with facial recognition technology, and the potentially millions or billions of photos stored in these systems, to help generate investigative leads and solve crimes. However, 13 federal agencies cannot assess the risks of using non-federal systems because they are unaware of what systems are used by employees. By implementing a mechanism to track what non-federal systems are used by employees, agencies will have better visibility into the technologies they rely upon to conduct criminal investigations. In addition, by assessing the risks of using these systems, including privacy and accuracy-related risks, agencies will be better positioned to mitigate any risks to themselves and the public.

Recommendations for Executive Action

We are making the following 26 recommendations:

The Director of the Bureau of Alcohol, Tobacco, Firearms and Explosives should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 1)

The Director of the Bureau of Alcohol, Tobacco, Firearms and Explosives should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 2)

The Administrator for the Drug Enforcement Administration should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 3)

The Administrator for the Drug Enforcement Administration should, after implementing a mechanism to track non-federal systems, assess the risks

of using such systems, including privacy and accuracy-related risks. (Recommendation 4)

The Director of the FBI should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 5)

The Director of the FBI should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 6)

The Director of the U.S. Marshals Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 7)

The Director of the U.S. Marshals Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 8)

The Commissioner of CBP should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 9)

The Commissioner of CBP should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 10)

The Director of the Secret Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 11)

The Director of the Secret Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 12)

The Director of the U.S. Fish and Wildlife Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 13)

The Director of the U.S. Fish and Wildlife Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 14)

The Chief of the U.S. Park Police should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 15)

The Chief of the U.S. Park Police should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 16)

The Assistant Secretary of the Bureau of Diplomatic Security should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 17)

The Assistant Secretary of the Bureau of Diplomatic Security should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 18)

The Assistant Commissioner of the Food and Drug Administration's Office of Criminal Investigations should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 19)

The Assistant Commissioner of the Food and Drug Administration's Office of Criminal Investigations should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 20)

The Chief of the Internal Revenue Service's Criminal Investigation Division should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 21)

The Chief of the Internal Revenue Service's Criminal Investigation Division should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 22)

The Chief Postal Inspector of the U.S. Postal Inspection Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 23)

The Chief Postal Inspector of the U.S. Postal Inspection Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 24)

The Chief of Police, U.S. Capitol Police, should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities. (Recommendation 25)

The Chief of Police, U.S. Capitol Police, should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks. (Recommendation 26)

Agency Comments and Our Evaluation

We provided a draft of this product for comment to the 21 federal departments and other entities (i.e., entities) that responded to our survey.³¹ We made recommendations to eight of the 21 entities, and these eight entities generally concurred with our recommendations.³² Seven of the eight entities provided written comments, which are reproduced in appendices IV through X and summarized below.³³

³¹Although we surveyed 42 federal agencies, we generally provide draft products for comment to the respective department (e.g., Department of Homeland Security) rather than the individual agencies (e.g., U.S. Customs and Border Protection) within a department. See the list of 21 departments and other entities (e.g., Amtrak) that received the draft product at table 6 in appendix I.

³²We made recommendations to 13 of the 42 federal agencies that we surveyed. These 13 agencies are located within eight federal departments and entities (i.e., entities), and as discussed, these eight entities generally concurred with our recommendations.

³³As discussed earlier, this report is a public version of a sensitive report that we issued in April 2021. Five of the seven entities asked that we reprint their comments from the sensitive report, which are reproduced in appendices VI through X.

- U.S. Department of Health and Human Services concurred with our recommendations.
- Department of Homeland Security concurred with our recommendations and provided technical comments, which we incorporated as appropriate.
- Department of the Interior concurred with our recommendations.
- Department of Justice's Federal Bureau of Investigation concurred with our recommendations and provided technical comments, which we incorporated as appropriate.
- Department of State concurred with our recommendations and provided technical comments, which we incorporated as appropriate.
- Department of the Treasury concurred with our recommendations, stating that the Internal Revenue Service's Criminal Investigation Division has mechanisms in place capable of tracking non-federal systems used by employees. However, during our review, the Criminal Investigation Division told us it does not track what systems are used by employees because it is not the owner of these technologies. Moreover, as noted in our report, the Criminal Investigation Division used facial recognition technology owned by other governmental entities at the federal and state, local, tribal, or territorial level. We therefore continue to believe that the Criminal Investigation Division should, as part of implementing these recommendations, ensure mechanisms are in place to appropriately track what non-federal systems (e.g., systems owned by other federal and state agencies) are used to support its investigative activities.
- U.S. Postal Service concurred, in part, with our recommendation to develop a mechanism to track what non-federal systems employees use. Specifically, the agency told us that the U.S. Postal Inspection Service currently tracks employee use of certain non-federal systems. Thus, the agency said it only needs to develop a mechanism to track other non-federal systems that employees use. Our report acknowledges that agencies may have had awareness of certain non-federal systems used by employees. However, U.S. Postal Inspection Service does not have a mechanism to provide complete, up-to-date information about what non-federal systems are used by employees. As a result, we continue to believe our recommendation, as written, is valid. In addition, the U.S. Postal Service concurred with our recommendation to assess the risks associated with non-federal systems.

Two of the eight entities that received recommendations emailed their comments. Specifically, the U.S. Capitol Police concurred with our recommendations and provided technical comments, which we incorporated as appropriate. In addition, the Department of Justice concurred with our recommendations and provided technical comments, which we incorporated as appropriate. Of note, the Department of Justice provided written and emailed comments.

We did not make recommendations to 13 of the 21 entities. Two of the 13 entities provided technical comments, which we incorporated as appropriate. Specifically, the Department of Commerce provided technical comments from the National Institute of Standards and Technology, and the National Aeronautics and Space Administration provided technical comments. The remaining 11 entities informed us that they had no comments.

We also provided a draft of this product for comment to two entities that did not receive our survey—the Office of Management and Budget and Clearview AI. The Office of Management and Budget informed us they had no comments, and Clearview AI provided technical comments, which we incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the relevant federal departments and entities.³⁴ 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 me 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 XI.

³⁴Specifically, we will send copies to the 21 federal departments and other entities included in table 6 at appendix I. In addition, we will send a copy to the Office of Management and Budget.

Letter

A handwritten signature in black ink, reading "Gretta L. Goodwin". The signature is written in a cursive style with a large, stylized initial "G".

Gretta L. Goodwin
Director
Homeland Security and Justice

List of Requesters

The Honorable Jerrold Nadler
Chairman
Committee on the Judiciary
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives

The Honorable Cory A. Booker
United States Senate

The Honorable Christopher A. Coons
United States Senate

The Honorable Edward J. Markey
United States Senate

The Honorable Ron Wyden
United States Senate

Appendix I: Objectives, Scope, and Methodology

This report examines (1) what federal agencies that employ law enforcement officers own and use facial recognition technology, (2) the type of activities these federal agencies use facial recognition technology to support, and (3) the extent that these federal agencies track employee use of facial recognition technology owned by non-federal entities, including state, local, tribal, territorial, and non-government entities.

This report is a public version of a sensitive report that we issued in April 2021.¹ Some federal agencies deemed information in our April report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information about agency ownership and use of facial recognition technology. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To address all three objectives, we surveyed 42 federal agencies that employ law enforcement officers. Consistent with our prior work, we define federal law enforcement officers as full-time employees with federal arrest authority and who are authorized to carry firearms while on duty. To identify which agencies employ federal law enforcement officers, we reviewed the Bureau of Justice Statistics' 2016 Census of Federal Law Enforcement Officers.² The 2016 census identified the number of law enforcement officers employed by federal entities, with the exception of officers in the U.S. Armed Forces, officers stationed in foreign countries, and officers at the Central Intelligence Agency or Transportation Security Administration's Federal Air Marshal Service.

Our scope included 42 of the 86 federal entities identified in the 2016 census as employing law enforcement officers (see table 6). The 2016 Census included Offices of Inspectors General; however, we excluded these agencies. We contacted the Council of the Inspectors General on Integrity and Efficiency, who stated that they were unaware of any Offices

¹GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-243SU (Washington, D.C.: April 28, 2021).

²Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016 – Statistical Tables*, NCJ 251922 (Washington, D.C.: October 2019).

Appendix I: Objectives, Scope, and Methodology

of Inspectors General that use facial recognition technology. However, we did include the Transportation Security Administration because it employs federal law enforcement officers, and was excluded from the 2016 census report for sensitivity reasons.

Table 6: 42 Federal Agencies Selected in GAO’s Work

Federal Agency	Department
Forest Service	Agriculture
Bureau of Industry and Security	Commerce
National Oceanic and Atmospheric Administration, Office of Law Enforcement	Commerce
Office of Security	Commerce
Secretary’s Protective Detail	Commerce
Pentagon Force Protection Agency	Defense
National Nuclear Security Administration	Energy
Food and Drug Administration, Office of Criminal Investigations	Health and Human Services
National Institutes of Health, Division of Police	Health and Human Services
U.S. Customs and Border Protection	Homeland Security
Federal Emergency Management Agency, Mount Weather Police	Homeland Security
Federal Protective Service	Homeland Security
U.S. Immigration and Customs Enforcement	Homeland Security
Office of the Chief Security Officer	Homeland Security
U.S. Secret Service	Homeland Security
Transportation Security Administration	Homeland Security
Bureau of Indian Affairs, Office of Justice Services	Interior
Bureau of Land Management	Interior
Bureau of Reclamation	Interior
U.S. Fish and Wildlife Service	Interior
U.S. Park Police	Interior
National Park Service Rangers	Interior
Bureau of Alcohol, Tobacco, Firearms and Explosives	Justice
Drug Enforcement Administration	Justice
Federal Bureau of Investigation	Justice
Federal Bureau of Prisons	Justice
U.S. Marshals Service	Justice
Division of Protective Operations	Labor
Bureau of Diplomatic Security	State
Bureau of Engraving and Printing Police	Treasury
Internal Revenue Service, Criminal Investigation Division	Treasury

Appendix I: Objectives, Scope, and Methodology

Federal Agency	Department
U.S. Mint Police	Treasury
Police Service	Veterans Affairs
Amtrak Police Department	Not Applicable
Environmental Protection Agency, Criminal Investigation Division	Not Applicable
National Aeronautics and Space Administration, Office of Protective Services	Not Applicable
U.S. Postal Inspection Service	Not Applicable
Smithsonian Institution, Office of Protection Services	Not Applicable
Tennessee Valley Authority Police	Not Applicable
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	Not Applicable
U.S. Capitol Police	Not Applicable
Government Publishing Office, Uniform Police Branch	Not Applicable

Legend: – Not Applicable

Source: GAO information. | GAO-21-518

To answer our first and second objectives, we administered a survey questionnaire to each of these 42 federal agencies. We administered the questionnaire by email from April through November 2020. Because we surveyed and obtained responses from all 42 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 questionnaire survey may introduce other errors. For example, difficulties in how a particular question is interpreted by respondents, in the sources of information that are available to respondents, or in how we processed and analyzed the responses we received can influence the accuracy of the survey results. We took steps in the development of the questionnaire, the data collection, and the data analysis to minimize these potential errors, and to help ensure the accuracy of the answers that were obtained. We conducted pre-tests with three agencies in different departments to test the survey’s applicability to a variety of facial recognition technology use cases, and revised the questionnaire based on the pre-tests.

When agencies submitted survey responses, we conducted an initial review for completeness, discrepancies, or logical errors within the responses, or discrepancies based on our prior knowledge (e.g., based on our review of a privacy impact assessment). We asked agencies to re-submit or clarify responses if necessary. We also confirmed our understanding of agency-provided information in semi-structured, open-ended follow-up interviews and information requests to the 20 agencies that reported they owned or used facial recognition technology. To help corroborate the information agencies provided in the questionnaire, we

conducted a search of government contracting information, agency websites, and privacy documentation. When we discovered discrepancies, we followed up with the agency as appropriate.

We sent the questionnaire to audit liaisons or their designees for dissemination to relevant subject matter experts. We instructed these liaisons to provide a response on behalf of their organization, which would include all the agency's offices, employees, and contractors. The questionnaire defined facial recognition technology as a type of automated or semi-automated biometric technology that uses images for verification, identification, and/or investigative purposes. The questionnaire noted that facial recognition technology can be used for a variety of applications, such as verifying the identity claimed by an individual, identifying if an unknown individual exists in a gallery of known people, or comparing an unknown person to a gallery of known people to develop an investigative lead. In addition, we stated that a system with facial recognition technology may include a facial recognition algorithm, hardware, software, and a photo database. We asked agencies to include all uses of facial recognition technology in their response except for facial recognition technology that was solely used to authenticate the identity of the agency's employees and contractors to log into computers and phones.

The questionnaire asked whether at any point during January 2015 through March 2020, an agency owned a system with facial recognition technology, including systems in the process of being developed.³ We used this time frame because March 2020 was the most recent full month for which information was available when we issued our questionnaire. Also, using a 5-year period allowed us to identify technology that was recently developed but not put in operation, and identify trends in facial recognition search data. We also asked whether at any point from April 2018 through March 2020, an agency's offices, employees, or contractors (1) accessed a system owned or operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf.⁴ All 42 agencies responded to questions about the use of another entity's systems; however, some

³In our questionnaire, we stated that the term "own" includes systems that were procured or developed by the respective entity.

⁴For the purposes of this report, by saying an agency "used" another entity's system, we mean that an agency's offices, employees, and contractors (1) accessed a system owned or operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf.

indicated that they could not guarantee the accuracy of the answers because they did not track this information. In some instances, employees and contractors had to work from their memory on the usage of another entity's systems. Agencies expressed this concern when we pretested the questionnaire, thus, we gathered this information from April 2018 (a 2-year period) instead of January 2015 (a 5-year period).

Agencies that owned a system completed an attachment with additional questions, such as the reason the agency used the system and the operational status of the system. In addition, we asked about the number of searches conducted on the system from 2015 through 2019, and number of photos included within the system as of March 31, 2020. We asked agency officials about the source of the data, whether the data were approximations or exact, whether definitions were consistently used in producing the data, and if there were any other data limitations that we should consider when reporting the information.

We requested additional information, through interviews and written requests, from agencies that reported in their questionnaire that they owned or used facial recognition technology. For example, if an agency reported having a system in operation, we requested privacy impact assessments and system descriptions. The information was used to help develop the system description and status throughout the report, including the detailed system appendices. In addition, we requested that 17 federal agencies provide information regarding whether they had used facial recognition technology on images of the civil unrest, riots, or protests from May through August 2020—the most recent full month for which information was available when we sent our questions. We also asked these 17 federal agencies whether they conducted facial recognition searches from January 6 through January 22, 2021 on images of the riot and civil unrest that occurred at the U.S. Capitol complex on January 6, 2021. We requested this information from 17 agencies that reported, via our questionnaire described above, they (1) had a system with facial recognition technology that was in operation, or (2) had used another entities' system. One exception was the Federal Bureau of Prisons, which we excluded because its system is used by employees to enter secure rooms.

To answer our third objective, we reviewed statutes and regulations, such as the Privacy Act of 1974. In addition, we interviewed or requested information from officials from 14 agencies that reported using (1) non-federal systems, and (2) facial recognition technology to support criminal investigations. We determined that the control activities component of

internal control was significant to this objective, along with the underlying principles that management should design control activities to achieve its objective and respond to risks. Specifically, we asked officials from the 14 agencies about their processes for gathering information on what non-federal systems are used by employees, and compared this information against our risk management framework and key aspects of *Standards for Internal Control in the Federal Government* (Principles 7, 10, and 16).⁵

We also interviewed and requested information from three additional federal agencies: Department of State's Bureau of Consular Affairs, Department of Homeland Security's Office of Biometric and Identity Management, and Department of Defense's Defense Forensic Science Center. We selected these agencies because multiple federal agencies we surveyed reported using these agencies' systems. We also met with other stakeholders to discuss law enforcement use of facial recognition technology, including other government entities, privacy advocacy groups, and non-government facial recognition technology providers. For example, we met with the Department of Commerce's National Institute of Standards and Technology, Georgetown Law Center on Privacy and Technology, and the International Biometrics and Identity Association.

While we did not comprehensively assess the reliability of data provided by agencies and other stakeholders, we took the steps described earlier and considered limitations identified by the agencies. We determined that data elements we assessed were sufficiently reliable for the purposes of this report.

The performance audit upon which this report is based was conducted from August 2019 to April 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 based on our audit objectives. We subsequently worked with the relevant entities from April 2021 to June 2021 to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

⁵See [GAO-14-704G](#) and [GAO-17-63](#).

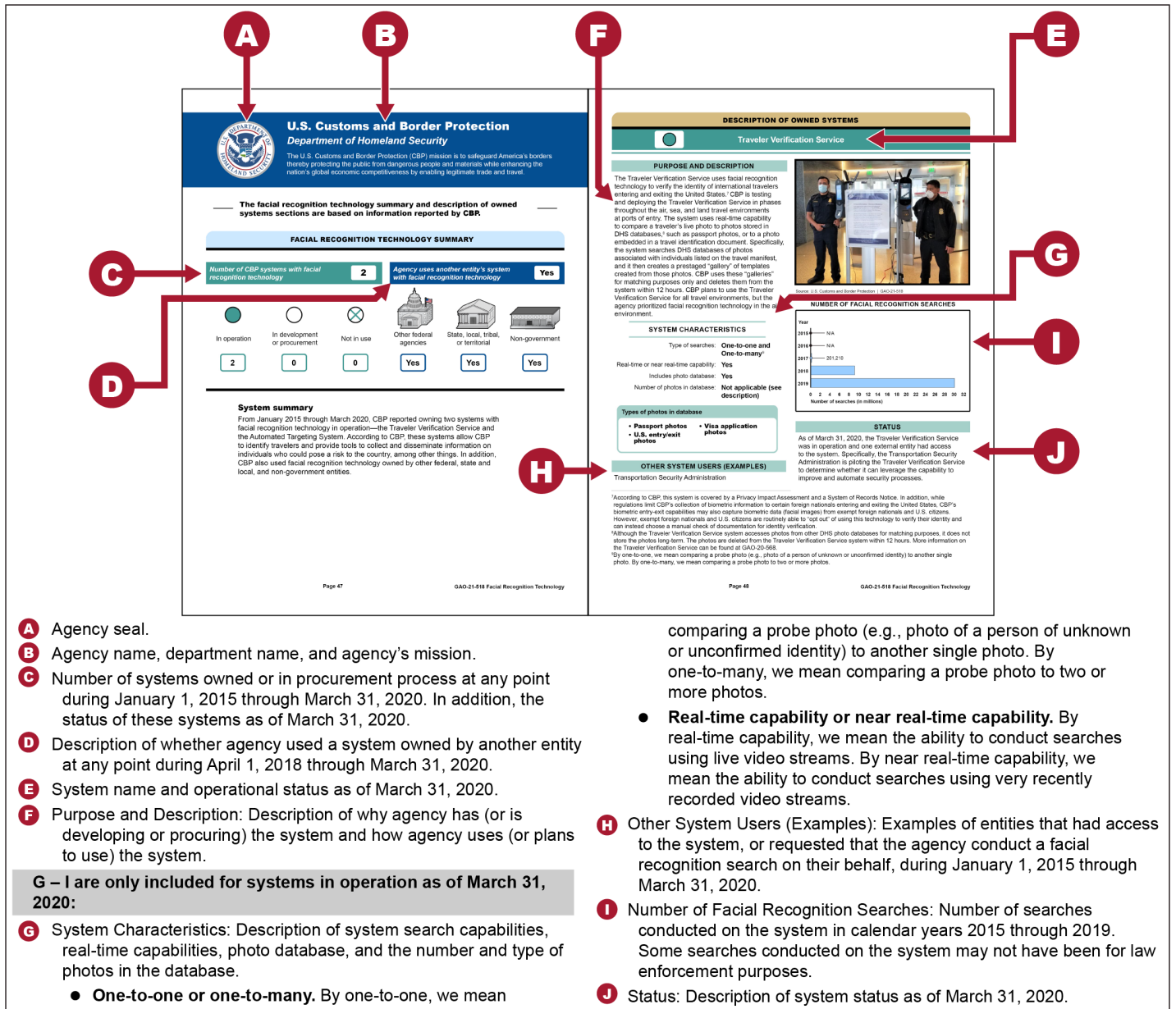
Appendix II: Systems with Facial Recognition Technology Owned by Federal Agencies that Employ Law Enforcement Officers

Eight of the 42 surveyed agencies reported owning systems with facial recognition technology. Eight summaries are presented below—that is, one for each of the eight agencies.¹ Each summary includes a description of the agency’s mission, an overview of the agency’s ownership and use of other entities’ systems, and detailed descriptions of each system owned by the agency. Information in these summaries was provided by the respective agency. See figure 4 for an illustration of the layout of the summaries, including a description of each section in the summaries.

¹This appendix omits information about systems with facial recognition technology deemed sensitive by the respective federal agency.

Appendix II: Systems with Facial Recognition Technology Owned by Federal Agencies that Employ Law Enforcement Officers

Figure 4: Illustration of a Facial Recognition Technology Summary



Source: GAO. | GAO-21-518

Appendix III: Other Federal Systems with Facial Recognition Technology

This appendix includes facial recognition technology summaries for three federal agencies: the Department of State's Bureau of Consular Affairs, Department of Defense's Defense Forensic Science Center, and the Department of Homeland Security's Office of Biometric Identity Management. These agencies were not included in our survey. However, we are presenting summary descriptions because they have facial recognition technology that multiple surveyed agencies reported using. Information in the summaries were provided by the respective agency. The summaries use a similar format to those included in appendix II. See figure 4 in appendix II for an illustration of the layout of the summaries, including a description of each section in the summaries.

Appendix IV: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

May 12, 2021

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

Dear Ms. Goodwin:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, *"Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks"* (Job code 105161/GAO-21-518).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Rose M.
Sullivan -S

Digitally signed by Rose
M. Sullivan -S
Date: 2021.05.25
16:08:24 -04'00'

Rose Sullivan
Acting Assistant Secretary for Legislation
Principal Deputy Assistant Secretary for Legislation

Attachment

**Appendix IV: Comments from the Department
of Health and Human Services**

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD BETTER ASSESS PRIVACY AND OTHER RISKS (GAO-21-518)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 19

The Assistant Commissioner of the Food and Drug Administration's Office of Criminal Investigations should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

HHS Response

FDA concurs with this GAO recommendation, and the Food and Drug Administration's Office of Criminal Investigations (OCI) intends to implement a mechanism to track what federal and non-federal (including state, local, tribal, territorial, and non-governmental) facial recognition technology (FRT) systems are used by OCI agents to support investigative activities. OCI intends that such tracking mechanism will include the name of the FRT system, owner of the FRT system, and how use of the FRT system supported OCI's mission.

Recommendation 20

The Assistant Commissioner of the Food and Drug Administration's Office of Criminal Investigations should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

HHS Response

FDA concurs with GAO's recommendation to assess the risks of using non-federal FRT systems that are identified through OCI's tracking mechanism. OCI will assemble a list of potential risks posed by the use of non-federal FRT systems, including risks related to privacy issues as well as system accuracy-related risks. OCI will use this list to help FDA identify threats to achieving investigative goals and objectives, and if appropriate, assist FDA in the adoption of treatment strategies to manage priority risks.

Agency Comment Letter

Text of Appendix IV: Comments from the Department of Health and Human Services

Page 1

May 12, 2021

Gretta Goodwin
Director, Health Care
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Goodwin:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks" (Job code 105161/GAO-21-518).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Rose Sullivan
Acting Assistant Secretary for Legislation
Principal Deputy Assistant Secretary for Legislation

Attachment

Page 2

**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN
SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT
REPORT ENTITLED — FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW
ENFORCEMENT AGENCIES SHOULD BETTER ASSESS PRIVACY AND OTHER
RISKS (GAO-21-518)**

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 19

The Assistant Commissioner of the Food and Drug Administration's Office of Criminal Investigations should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

HHS Response

FDA concurs with this GAO recommendation, and the Food and Drug Administration's Office of Criminal Investigations (OCI) intends to implement a mechanism to track what federal and non-federal (including state, local, tribal, territorial, and non-governmental) facial recognition technology (FRT) systems are used by OCI agents to support investigative activities. OCI intends that such tracking mechanism will include the name of the FRT system, owner of the FRT system, and how use of the FRT system supported OCI's mission.

Recommendation 20

The Assistant Commissioner of the Food and Drug Administration's Office of Criminal Investigations should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

HHS Response

FDA concurs with GAO's recommendation to assess the risks of using non-federal FRT systems that are identified through OCI's tracking mechanism. OCI will assemble a list of potential risks posed by the use of non-federal FRT systems, including risks related to privacy issues as well as system accuracy-related risks. OCI will use this list to help FDA identify threats to achieving investigative goals and objectives, and if appropriate, assist FDA in the adoption of treatment strategies to manage priority risks.

Appendix V: Comments from the Department of Homeland Security

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



May 11, 2021

Gretta L. Goodwin
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-21-518, "FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks"

Dear Ms. Goodwin:

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

The Department is pleased to note GAO's recognition that the U.S. Immigration and Customs Enforcement assessed privacy risks associated with its use of facial recognition technology, including non-federal systems, and that the agency identified privacy risks and possible actions to mitigate those risks. As the Department expands the use of facial recognition technology in its missions, DHS is committed to improved tracking of the use of non-Federal systems for mission purposes, as well as assessing the privacy and accuracy risks of utilizing such systems.


The draft report contained 24 recommendations, including four for DHS with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

**Appendix V: Comments from the Department
of Homeland Security**

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

Sincerely,

JIM H
CRUMPACKER

 Digitally signed by JIM H CRUMPACKER
Date: 2021.05.11 16:37:37 -04'00'

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

Attachment

**Attachment: Management Response to Recommendations
Contained in GAO-21-518**

GAO recommended that the Commissioner of U.S. Customs and Border Protection (CBP):

Recommendation 9: Implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Response: Concur. Pursuant to CBP’s Privacy Directive 2120-010, “Privacy Policy, Compliance, and Implementation,” dated January 2, 2015, all CBP personnel are responsible for notifying the CBP Privacy Office regarding the implementation, or proposed implementation, of technologies that involve personally identifiable information (PII) or that may otherwise impact the privacy of individuals. While directive 2120-010 broadly defines PII, it does not explicitly indicate that facial recognition technologies are potentially privacy invasive tools. The Directive also requires that all programs using tools, systems, and technologies—or implementing a program, pilot, or rulemaking—must, in coordination with the CBP Privacy Office, complete a Privacy Threshold Analysis to determine whether PII is involved.

By the end of 2021, the CBP Privacy Office will update CBP’s Privacy Directive to more explicitly identify the applicability of these reporting and coordination requirements with regard to the use of facial recognition technologies, regardless of whether they are owned or operated by CBP. Upon approval and implementation by the Commissioner of CBP, the Directive will be distributed to the CBP workforce. Additionally, the CBP Privacy Office will create and circulate messaging specific to the use and implementation of facial recognition technologies to the entirety of CBP’s workforce. This increase in awareness should foster more active participation in CBP’s already robust Privacy Compliance process, reinforcing its function as a mechanism for the tracking of CBP systems, programs, and pilot efforts. Estimated Completion Date (ECD): December 31, 2021.

Recommendation 10: After implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Response: Concur. CBP’s Privacy Compliance process is substantial, and includes reviews of IT systems, technologies, rulemakings, programs, pilot projects, and other activities to determine what, if any, PII is collected, used, or shared. This assessment allows CBP to determine whether additional policy, technological, or physical safeguards are necessary to ensure that data is protected from unauthorized use or disclosure. Increased awareness and understanding of the requirement to coordinate with the CBP Privacy Office, brought on by updating and publishing the Privacy Directive, will present

new opportunities for the review of use cases and tools associated with facial recognition technologies that the Privacy Office may not have been previously aware. However, the CBP Privacy Office will also conduct training and outreach for individuals who have the ability to procure access to these types of vendors and technologies, via a government purchase card, outside of the typical IT acquisition review process. ECD: December 31, 2021.

GAO recommended that the Director of the United States Secret Service (USSS):

Recommendation 11: Implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Response: Concur. The USSS Office of Investigations recognizes the importance of establishing visibility regarding the investigative tools utilized by agency personnel during the course of official investigative activities. Consequently, the Investigative Support Division and the Criminal Investigative Division are jointly working to enhance the functionality of the internal agency case management system to collect this information. Once established, the functional augmentation of the internal case management system will serve as a tracking mechanism for usage of non-federal facial recognition technologies. As such, the system will require USSS personnel to record the usage, or request for the usage, of non-federal facial recognition technology systems as an official investigative activity within the internal case management system. Specifically, the internal case management system will provide a mechanism to collect information about the use of facial recognition technologies used in support of investigative activities to include the: (1) owner and/or operator of the facial recognition technology system; (2) facial recognition technology system utilized; and (3) date the search was conducted. ECD: December 31, 2021.

Recommendation 12: After implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Response: Concur. Upon completion of the functional augmentation within the internal case management system, as well as implementation of the mechanism to capture usage of non-federal facial recognition technology systems, the USSS Office of Investigations will be better postured to assess the risks of using such systems. This improved visibility into the non-federal facial recognition technology used by agency personnel will enable the Office of Investigations to: (1) actively query usage of such systems; (2) ensure best practices for usage; and (3) assess the risks associated with privacy and/or accuracy deficiencies. Furthermore, the Office of Investigations will use the information garnered from this continual assessment to provide guidance to agency personnel as to appropriate usage of, or restrictions to the usage of, non-federal facial recognition technology systems. ECD: December 31, 2021.

Agency Comment Letter

Text of Appendix V: Comments from the Department of Homeland Security

Page 1

May 11, 2021

Gretta L. Goodwin
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548
U.S. Department of Homeland Security
Washington, DC 20528

Re: Management Response to Draft Report GAO-21-518, "FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks"

Dear Ms. Goodwin:

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

The Department is pleased to note GAO's recognition that the U.S. Immigration and Customs Enforcement assessed privacy risks associated with its use of facial recognition technology, including non-federal systems, and that the agency identified privacy risks and possible actions to mitigate those risks. As the Department expands the use of facial recognition technology in its missions, DHS is committed to improved tracking of the use of non-Federal systems for mission purposes, as well as assessing the privacy and accuracy risks of utilizing such systems.

The draft report contained 24 recommendations, including four for DHS with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Page 2

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

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Page 3

**Attachment: Management Response to Recommendations Contained in GAO-
21-518
GAO recommended that the Commissioner of U.S. Customs and Border
Protection (CBP):**

Recommendation 9:

Implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Response: Concur. Pursuant to CBP's Privacy Directive 2120-010, "Privacy Policy, Compliance, and Implementation," dated January 2, 2015, all CBP personnel are responsible for notifying the CBP Privacy Office regarding the implementation, or proposed implementation, of technologies that involve personally identifiable information (PII) or that may otherwise impact the privacy of individuals. While directive 2120-010 broadly defines PII, it does not explicitly indicate that facial recognition technologies are potentially privacy invasive tools. The Directive also requires that all programs using tools, systems, and technologies—or implementing a program, pilot, or rulemaking—must, in coordination with the CBP Privacy Office, complete a Privacy Threshold Analysis to determine whether PII is involved.

By the end of 2021, the CBP Privacy Office will update CBP's Privacy Directive to more explicitly identify the applicability of these reporting and coordination requirements with regard to the use of facial recognition technologies, regardless of whether they are owned or operated by CBP. Upon approval and implementation by the Commissioner of CBP, the Directive will be distributed to the CBP workforce.

Additionally, the CBP Privacy Office will create and circulate messaging specific to the use and implementation of

facial recognition technologies to the entirety of CBP's workforce. This increase in awareness should foster more active participation in CBP's already robust Privacy Compliance process, reinforcing its function as a mechanism for the tracking of CBP systems, programs, and pilot efforts. Estimated Completion Date (ECD): December 31, 2021.

Recommendation 10:

After implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Response: Concur. CBP's Privacy Compliance process is substantial, and includes reviews of IT systems, technologies, rulemakings, programs, pilot projects, and other activities to determine what, if any, PII is collected, used, or shared. This assessment allows CBP to determine whether additional policy, technological, or physical safeguards are necessary to ensure that data is protected from unauthorized use or disclosure.

Increased awareness and understanding of the requirement to coordinate with the CBP Privacy Office, brought on by updating and publishing the Privacy Directive, will present new opportunities for the review of use cases and tools associated with facial recognition technologies that the Privacy Office may not have been previously aware. However, the CBP Privacy Office will also conduct training and outreach for individuals who have the ability to procure access to these types of vendors and technologies, via a government purchase card, outside of the typical IT acquisition review process. ECD: December 31, 2021.

Page 4

GAO recommended that the Director of the United States Secret Service (USSS):

Recommendation 11:

Implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Response: Concur. The USSS Office of Investigations recognizes the importance of establishing visibility regarding the investigative tools utilized by agency personnel during the course of official investigative activities. Consequently, the Investigative Support Division and the Criminal Investigative Division are jointly working to

enhance the functionality of the internal agency case management system to collect this information. Once established, the functional augmentation of the internal case management system will serve as a tracking mechanism for usage of non-federal facial recognition technologies. As such, the system will require USSS personnel to record the usage, or request for the usage, of non-federal facial recognition technology systems as an official investigative activity within the internal case management system.

Specifically, the internal case management system will provide a mechanism to collect information about the use of facial recognition technologies used in support of investigative activities to include the: (1) owner and/or operator of the facial recognition technology system; (2) facial recognition technology system utilized; and (3) date the search was conducted. ECD: December 31, 2021.

Recommendation 12:

After implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Response: Concur. Upon completion of the functional augmentation within the internal case management system, as well as implementation of the mechanism to capture usage of non-federal facial recognition technology systems, the USSS Office of Investigations will be better postured to assess the risks of using such systems. This improved visibility into the non-federal facial recognition technology used by agency personnel will enable the Office of Investigations to: (1) actively query usage of such systems; (2) ensure best practices for usage; and (3) assess the risks associated with privacy and/or accuracy deficiencies. Furthermore, the Office of Investigations will use the information garnered from this continual assessment to provide guidance to agency personnel as to appropriate usage of, or restrictions to the usage of, non-federal facial recognition technology systems. ECD: December 31, 2021.

Appendix VI: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

Gretta L. Goodwin
Director, Justice and Law Enforcement Issues
Homeland Security and Justice Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Goodwin,

Thank you for providing the Department of the Interior (Department) an opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (GAO-21-243SU). We appreciate GAO's review and feedback related to the federal law enforcement use of facial recognition technology.

The GAO issued four recommendations to the Department as part of its overall findings to improve these processes. The report contains two recommendations each for the U.S. Fish and Wildlife Service (FWS) and National Park Service (NPS). Below is a summary of actions taken or planned to implement the recommendations.

Recommendation 13: "The Director of the U.S. Fish and Wildlife Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities."

Response: Concur. The Assistant Director, Office of Law Enforcement, entered into a licensing agreement with Clearview Facial Recognition Technology (FRT) on July 1, 2020, to provide all facial recognition requests for the FWS law enforcement needs. The FWS has limited use to two licensed users. Clearview's reporting capabilities include tracking of all inquiries by license and case number. Clearview is the only FRT authorized for use in the FWS. Use of FRT during an investigation is entered into the case file in the Law Enforcement Management Information System (LEMIS). The Assistant Director will issue a Chief's Directive outlining the process for law enforcement personnel to request the use of facial recognition by the licensed users in cases requiring facial recognition.

Responsible Official: Assistant Director, Office of Law Enforcement

Target Date: March 1, 2022

**Appendix VI: Comments from the Department
of the Interior**

Recommendation 14: “The Director of the U.S. Fish and Wildlife Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.”

Response: Concur. The Assistant Director, Office of Law Enforcement, will issue a Chief’s Directive, in coordination with the Department’s Office of the Chief Information Officer, as appropriate, requiring a risk assessment of any facial recognition technology the FWS may use, to include an assessment of privacy and accuracy risks.

Responsible Official: Assistant Director, Office of Law Enforcement

Target Date: March 1, 2022

Recommendation 15: “The Chief of the U.S. Park Police should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.”

Response: Concur. The Chief, U.S. Park Police, will establish a policy outlining a tracking mechanism for the use of non-federal systems with facial recognition technology used by its employees to support investigative activities.

Responsible Official: Chief, U.S. Park Police

Target Date: December 31, 2021

Recommendation 16: “The Chief of the U.S. Park Police should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.”

Response: Concur. The Chief, U.S. Park Police (USPP), will issue a policy, in coordination with the Department’s Office of the Chief Information Officer, as appropriate, requiring a risk assessment of any facial recognition technology the USPP may use, to include an assessment of privacy and accuracy risks.

Responsible Official: Chief, U.S. Park Police

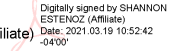
Target Date: March 1, 2022

**Appendix VI: Comments from the Department
of the Interior**

If you have any questions or need additional information, please contact the Internal Control and Audit Follow-up Division of the Office of Financial Management at DOI_PFM_ICAF@ios.doi.gov.

Sincerely,

SHANNON
ESTENOZ (Affiliate)



Digitally signed by SHANNON
ESTENOZ (Affiliate)
Date: 2021.03.19 10:52:42
-0400

Shannon Estenoz
Principal Deputy Assistant Secretary for
Fish and Wildlife and Parks
Exercising the Delegated Authority of the Assistant
Secretary for Fish and Wildlife and Parks

Agency Comment Letter

Text of Appendix VI: Comments from the Department of the Interior

Page 1

Gretta L. Goodwin
Director, Justice and Law Enforcement Issues
Homeland Security and Justice Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Goodwin,

Thank you for providing the Department of the Interior (Department) an opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (GAO-21-243SU). We appreciate GAO's review and feedback related to the federal law enforcement use of facial recognition technology.

The GAO issued four recommendations to the Department as part of its overall findings to improve these processes. The report contains two recommendations each for the U.S. Fish and Wildlife Service (FWS) and National Park Service (NPS). Below is a summary of actions taken or planned to implement the recommendations.

Recommendation 13: "The Director of the U.S. Fish and Wildlife Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities."

Response: Concur. The Assistant Director, Office of Law Enforcement, entered into a licensing agreement with Clearview Facial Recognition Technology (FRT) on July 1, 2020, to provide all facial recognition requests for the FWS law enforcement needs. The FWS has limited use to two licensed users. Clearview's reporting capabilities include tracking of all inquiries by license and case number. Clearview is the only FRT authorized for use in the FWS. Use of FRT during an investigation is entered into the case file in the Law Enforcement Management Information System (LEMIS). The Assistant Director will issue a Chiefs Directive outlining the process for law enforcement personnel to request the use of facial recognition by the licensed users in cases requiring facial recognition.

Responsible Official: Assistant Director, Office of Law Enforcement

Target Date: March 1, 2022

Page 2

Recommendation 14:

"The Director of the U.S. Fish and Wildlife Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks."

Response: Concur. The Assistant Director, Office of Law Enforcement, will issue a Chiefs Directive, in coordination with the Department's Office of the Chief Information Officer, as appropriate, requiring a risk assessment of any facial recognition technology the FWS may use, to include an assessment of privacy and accuracy risks.

Responsible Official: Assistant Director, Office of Law Enforcement

Target Date: March 1, 2022

Recommendation 15:

"The Chief of the U.S. Park Police should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities."

Response: Concur. The Chief, U.S. Park Police, will establish a policy outlining a tracking mechanism for the use of non-federal systems with facial recognition technology used by its employees to support investigative activities.

Responsible Official: Chief, U.S. Park Police

Target Date: December 31, 2021

Recommendation 16:

"The Chief of the U.S. Park Police should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks."

Response: Concur. The Chief, U.S. Park Police (USPP), will issue a policy, in coordination with the Department's Office of the Chief Information Officer, as appropriate, requiring a risk assessment of any facial recognition technology the USPP may use, to include an assessment of privacy and accuracy risks.

Responsible Official: Chief, U.S. Park Police

Target Date: March 1, 2022

Page 3

If you have any questions or need additional information, please contact the Internal Control and Audit Follow-up Division of the Office of Financial Management at DOI_PFM_ICAF@ios.doi.gov.

Sincerely,

Shannon Estenoz
Principal Deputy Assistant Secretary for
Fish and Wildlife and Parks
Exercising the Delegated Authority of the Assistant
Secretary for Fish and Wildlife and Parks

Appendix VII: Comments from the Department of State



United States Department of State
Comptroller
Washington, DC 20520

MAR 10 2021

Thomas Melito
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, “FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks” GAO Job Code 103705.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

A handwritten signature in blue ink that reads "Jeffrey C. Mounts".

Jeffrey C. Mounts

Enclosure:
As stated

cc: GAO – Gretta Goodwin
DS – Todd J. Brown
OIG - Norman Brown

Department of State Comments on GAO Draft Report

**FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement
Agencies Should Better Assess Privacy and Other Risks**
(GAO-21-243SU, GAO Code 103705)

Thank you for the opportunity to comment on your draft report entitled “*Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks.*” The report includes two recommendations for the Department of State. The Department concurs with these recommendations.

Recommendation 17: The Assistant Secretary for Diplomatic Security (DS) should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Response: The Department of State agrees. The Department, through the Bureau of Diplomatic Security (DS), supports the need for tracking and managing access to “non-federal systems with facial recognition technology” and the use of these systems in support of DS criminal investigations.

Prior to this study and concurrent with it, DS has been developing internal controls and standard operating procedures to ensure that access to any “non-federal systems with facial recognition technology” by DS special agents and analysts is properly vetted and that accounts are managed centrally through Bureau system account management processes. These procedures and functions are in the final drafting phase and are intended to be implemented this fiscal year globally.

Recommendation 18: The Assistant Secretary for DS should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Response: The Department of State agrees. As part of the implementation of the controls referred to in response to Recommendation 17, DS intends to establish an internal review panel to evaluate and review any “non-federal systems with facial recognition technology” that might be used. The panel would be intended to centralize contracting reviews and evaluate the provider’s privacy assessments and practices, as well as the internal processes for data collection, in order to assess the risks of using such a system. DS also intends to centralize control over the contracts and funding to ensure users are not inadvertently encouraged by

**Appendix VII: Comments from the Department
of State**

- 2 -

providers to utilize “non-federal systems with facial recognition technology” that lack approval and oversight.

The Department thanks the GAO for this constructive audit and will promptly implement the above recommendations.

Agency Comment Letter

Text of Appendix VII: Comments from the Department of State

Page 1

Thomas Melito
Managing Director

International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks" GAO Job Code 103705.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

Jeffrey C. Mounts

Enclosure:
As stated

cc: GAO – Gretta Goodwin
DS – Todd J. Brown
OIG - Norman Brown

Page 2

**Department of State Comments on GAO Draft Report
FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement Agencies**

**Should Better Assess Privacy and Other Risks
(GAO-21-243SU, GAO Code 103705)**

Thank you for the opportunity to comment on your draft report entitled "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks." The report includes two recommendations for the Department of State. The Department concurs with these recommendations.

Recommendation 17:

The Assistant Secretary for Diplomatic Security (DS) should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Response: The Department of State agrees. The Department, through the Bureau of Diplomatic Security (DS), supports the need for tracking and managing access to "non-federal systems with facial recognition technology" and the use of these systems in support of DS criminal investigations.

Prior to this study and concurrent with it, DS has been developing internal controls and standard operating procedures to ensure that access to any "non-federal systems with facial recognition technology" by DS special agents and analysts is properly vetted and that accounts are managed centrally through Bureau system account management processes. These procedures and functions are in the final drafting phase and are intended to be implemented this fiscal year globally.

Recommendation 18:

The Assistant Secretary for DS should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Response: The Department of State agrees. As part of the implementation of the controls referred to in response to Recommendation 17, DS intends to establish an internal review panel to evaluate and review any "non-federal systems with facial recognition technology" that might be used. The panel would be intended to centralize contracting reviews and evaluate the provider's privacy assessments and practices, as well as the internal processes for data collection, in order to assess the risks of using such a system. DS also intends to centralize control over the contracts and funding to ensure users are not inadvertently encouraged by providers to utilize "non-federal systems with facial recognition technology" that lack approval and oversight.

Page 3

The Department thanks the GAO for this constructive audit and will promptly implement the above recommendations.

Appendix VIII: Comments from the Department of the Treasury



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

March 10, 2021

James R. McTigue, Jr
Director, Tax Issues/Strategic Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. McTigue:

Thank you for the opportunity to review the draft report of the Government Accountability Office entitled "*Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*" (GAO-21-243SU). The focus of the report is to review how federal law enforcement agencies utilize facial recognition technology to assist in criminal investigations. We agree with the report and its findings.

This report includes two recommendations to each of twelve Agencies. These recommendations are designed to assist the Agencies in tracking what non-federal systems are used by employees, and to assess the risks of using these systems. With that as background, enclosed are comments on the draft report's recommendations directed to the IRS.

We appreciate having the opportunity to review and comment on the draft report. Responses to your specific recommendations are enclosed. If you have questions, please contact me, or a member of your staff may contact Guy Ficco, Executive Director of Operations, at 202-317-3804.

Sincerely,

Sunita B. Lough

Digitally signed by Sunita B. Lough
Date: 2021.03.10 17:13:23 -05'00'

Sunita Lough
Deputy Commissioner for Services and Enforcement

Enclosure

Enclosure

Comments on the GAO Recommendations Directed to the IRS

Recommendation 1:

The Chief of the Internal Revenue Service's Criminal Investigative Division should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Comment:

The IRS agrees that the Chief of the Internal Revenue Service's Criminal Investigative Division (CI) should implement a mechanism to track non-federal facial recognition technology systems used by employees to support investigative activities. To that end, requests that would involve the use of a facial recognition technology system, if carried out by IRS CI's National Forensic Laboratory (NFL), would be tracked using an electronic Laboratory Information Management System (LIMS). LIMS is used for creating, collecting, and storing all case-related information, to include database searches and the results of those searches, as well as equipment and technology used in analysis and to obtain reportable results. Furthermore, CI's Technology Operations and Investigative Services (TOIS) uses cyber security tools to monitor software and systems accessed on the CI network. Therefore, the IRS has mechanisms in place capable of tracking non-federal facial recognition technology systems used by the IRS in support of investigative activities.

It should be noted that CI does not currently have the ability to directly access or connect to federal or non-federal systems with facial recognition technology capabilities.

Recommendation 2:

The Chief of the Internal Revenue Service's Criminal Investigative Division should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Comment:

The IRS agrees that the Chief of the Internal Revenue Service's Criminal Investigative Division should assess the risks of using non-federal facial recognition technology systems, including privacy and accuracy related risks. To that end, IRS subject matter experts serve as members of professional organizations and groups such as the Facial Recognition Interagency Working Group. Active participation allows the IRS to continually assess risks of and best practices for using non-federal facial recognition technology systems. Also, documents such as the Bureau of Justice Assistance Face Recognition Policy Development Template are available to provide a framework under which a face recognition program can be operated and in a manner that complies with applicable laws, minimizes risks, and establishes accountability and oversight.

2

Although IRS does not currently possess or is not connected to facial recognition technology systems, IRS subject matter experts are already working with members of the relevant professional community to assess potential risks, privacy, and accuracy issues pertaining to the use of facial recognition technology.

Agency Comment Letter

Text of Appendix VIII: Comments from the Department of the Treasury

Page 1

March 10, 2021

James R. McTigue, Jr
Director, Tax Issues/Strategic Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. McTigue:

Thank you for the opportunity to review the draft report of the Government Accountability Office entitled "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks" (GAO-21-243SU). The focus of the report is to review how federal law enforcement agencies utilize facial recognition technology to assist in criminal investigations. We agree with the report and its findings.

This report includes two recommendations to each of twelve Agencies. These recommendations are designed to assist the Agencies in tracking what non-federal systems are used by employees, and to assess the risks of using these systems. With that as background, enclosed are comments on the draft report's recommendations directed to the IRS.

We appreciate having the opportunity to review and comment on the draft report. Responses to your specific recommendations are enclosed. If you have questions, please contact me, or a member of your staff may contact Guy Ficco, Executive Director of Operations, at 202-317-3804.

Sincerely,

Sunita Lough
Deputy Commissioner for Services and Enforcement

Enclosure

Page 2

Comments on the GAO Recommendations Directed to the IRS

Recommendation 1:

The Chief of the Internal Revenue Service's Criminal Investigative Division should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Comment:

The IRS agrees that the Chief of the Internal Revenue Service's Criminal Investigative Division (CI) should implement a mechanism to track non-federal facial recognition technology systems used by employees to support investigative activities. To that end, requests that would involve the use of a facial recognition technology system, if carried out by IRS CI's National Forensic Laboratory (NFL), would be tracked using an electronic Laboratory Information Management System (LIMS). LIMS is used for creating, collecting, and storing all case-related information, to include database searches and the results of those searches, as well as equipment and technology used in analysis and to obtain reportable results. Furthermore, CI's Technology Operations and Investigative Services (TOIS) uses cyber security tools to monitor software and systems accessed on the CI network. Therefore, the IRS has mechanisms in place capable of tracking non-federal facial recognition technology systems used by the IRS in support of investigative activities.

It should be noted that CI does not currently have the ability to directly access or connect to federal or non-federal systems with facial recognition technology capabilities.

Recommendation 2:

The Chief of the Internal Revenue Service's Criminal Investigative Division should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Comment:

The IRS agrees that the Chief of the Internal Revenue Service's Criminal Investigative Division should assess the risks of using non-federal facial recognition technology systems, including privacy and accuracy related risks. To that end, IRS subject matter experts serve as members of professional organizations and groups such as the Facial Recognition Interagency Working Group. Active participation

allows the IRS to continually assess risks of and best practices for using non-federal facial recognition technology systems. Also, documents such as the Bureau of Justice Assistance Face Recognition Policy Development Template are available to provide a framework under which a face recognition program can be operated and in a manner that complies with applicable laws, minimizes risks, and establishes accountability and oversight.

Page 3

Although IRS does not currently possess or is not connected to facial recognition technology systems, IRS subject matter experts are already working with members of the relevant professional community to assess potential risks, privacy, and accuracy issues pertaining to the use of facial recognition technology.

Appendix IX: Comments from the Federal Bureau of Investigation



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 19, 2021

Ms. Gretta L. Goodwin
Director
Homeland Security and Justice
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Goodwin:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO's) draft report entitled FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks (GAO-21-243SU). The FBI agrees with the two recommendations addressed to the FBI Director. The FBI's planned actions to address the recommendations are addressed below:

Recommendation: The Director of the FBI should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

FBI's Response:

The FBI recognizes the importance of tracking the use of facial recognition technology by FBI employees, contractors, and Task Force Officers and currently follows numerous policies governing the use of such technology, including, but not limited to, the Domestic Investigations and Operations Guide (DIOG) and the Next Generation Identification Policy and Implementation Guide. The FBI will review and, if necessary, update existing policy to ensure this GAO recommendation is addressed.

Recommendation: The Director of the FBI should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

FBI's Response:

The FBI recognizes the importance of assessing privacy and accuracy related risks associated with FBI use of non-federal systems with facial recognition technology and is committed to assessing such risks in accordance with applicable law and policy. The FBI will

**Appendix IX: Comments from the Federal
Bureau of Investigation**

review and, if necessary, update existing policy to ensure this GAO recommendation is addressed.

Again, thank you for the opportunity to comment on this report. We look forward to GAO closing the recommendations that the FBI has agreed to address.

Sincerely,



Darrin E. Jones
Executive Assistant Director
Science and Technology Branch

Agency Comment Letter

Text of Appendix IX: Comments from the Federal Bureau of Investigation

Page 1

March 19, 2021

Ms. Gretta L. Goodwin
Director
Homeland Security and Justice
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Goodwin:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO's) draft report entitled FACIAL RECOGNITION TECHNOLOGY: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks (GAO-21-243SU). The FBI agrees with the two recommendations addressed to the FBI Director. The FBI's planned actions to address the recommendations are addressed below:

Recommendation:

The Director of the FBI should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

FBI's Response:

The FBI recognizes the importance of tracking the use of facial recognition technology by FBI employees, contractors, and Task Force Officers and currently follows numerous policies governing the use of such technology, including, but not limited to, the Domestic Investigations and Operations Guide (DIOG) and the Next Generation Identification Policy and Implementation Guide. The FBI will review and, if necessary, update existing policy to ensure this GAO recommendation is addressed.

Recommendation:

The Director of the FBI should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Page 2

FBI's Response:

The FBI recognizes the importance of assessing privacy and accuracy related risks associated with FBI use of non-federal systems with facial recognition technology and is committed to assessing such risks in accordance with applicable law and policy. The FBI will review and, if necessary, update existing policy to ensure this GAO recommendation is addressed.

Again, thank you for the opportunity to comment on this report. We look forward to GAO closing the recommendations that the FBI has agreed to address.

Sincerely,

Executive Assistant Director
Science and Technology Branch

Appendix X: Comments from the United States Postal Service



March 5, 2021

Greta L. Goodwin
Director, Homeland Security and Justice
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

SUBJECT: Draft report review of *Facial Technology Recognition: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (GAO-21-243SU) – March 2021

Dear Ms. Goodwin:

Thank you for the opportunity to review and comment on the United States Government Accountability Office (GAO) draft report titled *Facial Technology Recognition: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*. Our responses to the GAO's Recommendations for Executive Action are set forth below.

Specific Responses

With regard to your specific recommendations, we provide the following responses:

Recommendation 23

The Chief Postal Inspector of the U.S. Postal Inspection Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Management's Response –

Management agrees in part with this recommendation. The U.S. Postal Inspection Service currently does track employee usage of agency-procured and provided non-federal systems with facial recognition technology. We will develop a mechanism to track other non-federal systems with facial recognition technology that our employees use to support investigative activities.

Expected completion date: September 30, 2021.

Recommendation 24

The Chief Postal Inspector of the U.S. Postal Inspection Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-5665
WWW.USPS.GOV

**Appendix X: Comments from the United States
Postal Service**

- 2 -

Management's Response –

Management agrees with this recommendation. Risk assessments are continuous for any system(s), or usage of systems, that our agency procures, to include agency-procured and provided non-federal systems with facial recognition technology. Upon developing a mechanism to track other non-federal systems with facial recognition technology that our employees use to support investigative activities, we will assess the risks associated to such usage.

Expected completion date: March 31, 2022.

The Postal Service appreciates the opportunity to respond to GAO's draft report and Recommendations for Executive Action.

Sincerely,



Gary Barksdale
Chief Postal Inspector

cc: Sally K. Haring, Manager, Corporate Audit and Responses

Agency Comment Letter

Text of Appendix X: Comments from the United States Postal Service

Page 1

March 5, 2021

Greta L. Goodwin
Director, Homeland Security and Justice
United States Government Accountability Office 441 G
Street, NW
Washington, DC 20548-0001

SUBJECT: Draft report review of Facial Technology Recognition: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks (GAO-21-243SU) - March 2021

Dear Ms. Goodwin:

Thank you for the opportunity to review and comment on the United States Government Accountability Office (GAO) draft report titled "Facial Technology Recognition: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks." Our responses to the GAO's Recommendations for Executive Action are set forth below.

Specific Responses

With regard to your specific recommendations, we provide the following responses:

Recommendation 23

The Chief Postal Inspector of the U.S. Postal Inspection Service should implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities.

Management's Response -

Management agrees in part with this recommendation. The U.S. Postal Inspection Service currently does track employee usage of agency-procured and provided non-

federal systems with facial recognition technology. We will develop a mechanism to track other non-federal systems with facial recognition technology that our employees use to support investigative activities.

Expected completion date: September 30, 2021.

Recommendation 24

The Chief Postal Inspector of the U.S. Postal Inspection Service should, after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy related risks.

Page 2

Management's Response -

Management agrees with this recommendation. Risk assessments are continuous for any system(s), or usage of systems, that our agency procures, to include agency-procured and provided non-federal systems with facial recognition technology. Upon developing a mechanism to track other non-federal systems with facial recognition technology that our employees use to support investigative activities, we will assess the risks associated to such usage.

Expected completion date: March 31, 2022.

The Postal Service appreciates the opportunity to respond to GAO's draft report and Recommendations for Executive Action.

Sincerely,

Gary Barksdale
Chief Postal Inspector

cc: Sally K. Haring, Manager, Corporate Audit and Responses

Appendix XI: GAO Contact and Staff Acknowledgments

GAO Contact

Gretta L. Goodwin, (202) 512-8777 or goodwing@gao.gov

Staff Acknowledgments

In addition to the contact named above, Joseph P. Cruz (Assistant Director), Jeffrey Fiore (Analyst-in-Charge), Andrea Bivens, Emily Flores, Lily Folkerts, Aaron Safer-Lichtenstein and Dawn Locke made key contributions to this report. Also contributing to this report were Amy Apostol, Jennifer Beddor, Benjamin Crossley, Caitlin Cusati, Richard Hung, Thomas Lombardi, Heidi Nielson, Carl Ramirez, and Kevin Reeves.

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/fraudnet/fraudnet.htm>

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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, Acting 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.