United States Government Accountability Office

Report to Congressional Requesters

September 2023

FACIAL RECOGNITION SERVICES

Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties

Accessible Version

GAO-23-105607

GAO Highlights

Highlights of GAO-23-105607, a report to congressional requesters

September 2023

FACIAL RECOGNITION SERVICES

Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties

Why GAO Did This Study

Law enforcement may use facial recognition services provided by commercial and nonprofit entities to help solve crimes. For example, these services allow users to quickly search through billions of photos to help identify an unknown suspect in a crime scene photo.

GAO was asked to review federal law enforcement's use of facial recognition technology. This report examines, among other issues, the extent to which selected DHS and DOJ law enforcement agencies used facial recognition services to support criminal investigations; required staff to take training on facial recognition technology to use such services; and developed policies and guidance specific to facial recognition technology to help protect civil rights and civil liberties.

GAO selected seven law enforcement agencies within DHS and DOJ based on various factors, including the number of facial recognition technology systems used. GAO reviewed documents, such as training requirements and policies for using facial recognition services. GAO also analyzed training records and interviewed agency officials.

What GAO Recommends

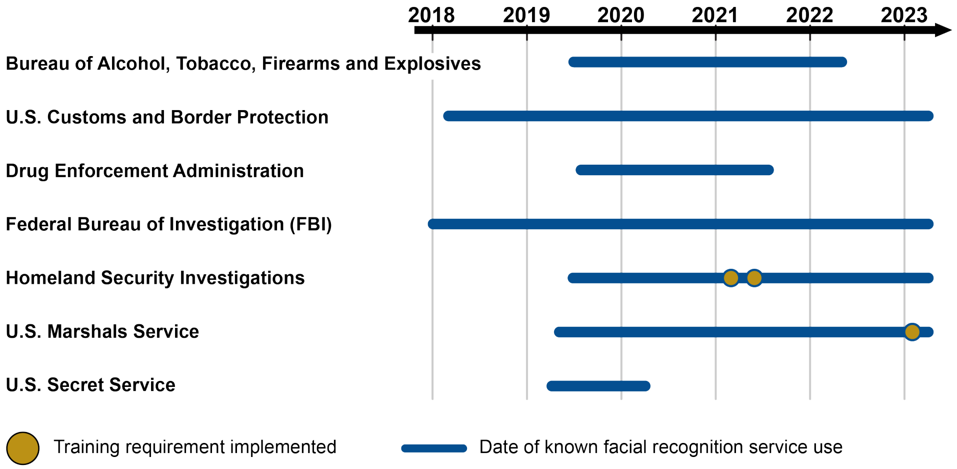
GAO is making 10 recommendations, including that FBI implement a training requirement and clarify the status of its training requirement to stakeholders. GAO also recommends that DOJ develop a plan to issue a facial recognition technology policy addressing safeguards for civil rights and civil liberties. Agencies concurred with all 10 recommendations.

View GAO-23-105607. For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov.

What GAO Found

Seven law enforcement agencies in the Departments of Homeland Security (DHS) and Justice (DOJ) reported using facial recognition services provided by commercial and nonprofit entities. The agencies reported using four services in total from October 2019 through March 2022 to support criminal investigations. All seven agencies initially used these services without requiring staff take facial recognition training. GAO found that six agencies had available data and cumulatively conducted about 60,000 searches when they did not have training requirements in place. As of April 2023, two agencies began to require training.

Facial Recognition Services, Use and Training for Selected Agencies, April 2023



Source: GAO analysis of agency information. | GAO-23-105607

Data for Facial Recognition Services, Use and Training for Selected Agencies, April 2023 (October 1, 2019 through March 31, 2022)

Timeline for use:

- ATF: earliest use in July 2019. Last use in May 2022.
- CBP: earliest use was March 2018. Continues to use as of April 2023.
- DEA: earliest use in August 2019. Last use in August 2021.
- FBI: earliest use in 2018. Continues to use as of April 2023.
- ICE: earliest use in June 2019. Continues to use as of April 2023.
- Marshals earliest use in May 2019. Continues to use as of April 2023.
- Secret Service: earliest use in April 2019. Last use in April 2020.

Timeline for training:

- ATF: earliest use in July 2019. Last use in May 2022. No training.

- CBP: earliest use in March 2018. Continues to use as of April 2023. No training.
- DEA: earliest use in August 2019. Last use in August 2021. No training.
- FBI earliest use in 2018. Continues to use as of April 2023. No training.
- ICE: earliest use in June 2019. Implemented training requirements in March and June 2021. Continues to use as of April 2023.
- Marshals: earliest use in May 2019. Implemented training requirement in February 2023. Continues to use service as of April 2023.
- Secret Service: earliest use in Clearview AI in April 2019. Last use in April 2020. No training.

Source: GAO analysis of agency information. | GAO-23-105607

Note: The figure shows when agencies used the four services covered by this review (services used from October 2019 through March 2022), and when, if at all, agencies implemented training requirements for facial recognition services. The figure provides use and training information as of April 2023. See figure 6 of the report for more detail.

FBI officials told key internal stakeholders that certain staff must take training to use one facial recognition service. However, in practice, FBI has only recommended it as a best practice. GAO found that few of these staff completed the training, and across the FBI, only 10 staff completed facial recognition training of 196 staff that accessed the service. FBI said they intend to implement a training requirement for all staff, but have not yet done so. Such a requirement would help FBI ensure its staff understand how to use these services. Also, clarifying the status of FBI's training requirement would allow stakeholders to fully evaluate use of the service against FBI ethical and privacy standards.

GAO also found that three of the seven agencies had policies or guidance specific to facial recognition technology that address civil rights and civil liberties. The other four agencies—three in DOJ and one in DHS—did not have such policies or guidance. DHS has plans to finalize a department-wide policy by December 2023. DOJ has taken steps to issue a department-wide policy, but has faced delays. Developing a plan with time frames and milestones would help DOJ ensure it issues a policy to support staff in safeguarding civil rights and civil liberties.

Contents

GAO Highlights ii

Why GAO Did This Study ii
What GAO Recommends ii
What GAO Found ii
Background 6
Federal Law Enforcement Agencies Used Four Facial Recognition Services to Support Criminal Investigations 12
Agencies with Available Data Reported Conducting About 60,000 Facial Recognition Searches Before Requiring Training 21
Three of Seven Agencies Took Some Steps to Address Selected Privacy Requirements 34
Most Agencies Did Not Have Policies Specific to Facial Recognition to Help Protect Civil Rights and Civil Liberties 41
Conclusions 46
Recommendations for Executive Action 48
Agency Comments and Our Evaluation 49

Appendix I: Objectives, Scope and Methodology 52

Appendix II: Extent to Which Selected Federal Law Enforcement Agencies Took Steps to Address Selected Privacy Requirements 59

Appendix III: Comments from the Department of Homeland Security 61

Text for Appendix III: Comments from the Department of Homeland Security 67

Appendix IV: GAO Contact and Staff Acknowledgements 73

GAO Contact 73
Staff Acknowledgments 73

Tables

Facial Recognition Services, Use and Training for Selected Agencies, April 2023 ii
Data for Facial Recognition Services, Use and Training for Selected Agencies, April 2023 (October 1, 2019 through March 31, 2022) ii
Text for Figure 1: Facial Recognition Technology Identification Search Process for Criminal Investigations 8

Table 1: Selected Privacy Requirements for Department of Homeland Security's (DHS) and Department of Justice's (DOJ) Use of Facial Recognition Services 10
Data for Figure 4: Selected Federal Law Enforcement Agencies' Reported Use of Facial Recognition Services (October 1, 2019 through March 31, 2022) 18
Table 2: Training Status of Homeland Security Investigations Staff That Conducted Facial Recognition Searches on Clearview AI from March 4, 2021 through March 31, 2022 28

Figures

Figure 1: Facial Recognition Technology Identification Search Process for Criminal Investigations 7
Figure 2: Facial Recognition Services Used by Selected Federal Law Enforcement Agencies to Support Criminal Investigations from October 2019 through March 2022 13
Text for Figure 2: Facial Recognition Services Used by Selected Federal Law Enforcement Agencies to Support Criminal Investigations from October 2019 through March 2022 14
Figure 3: Reported Number of Searches That Federal Agencies Conducted Using Facial Recognition Services, Based on Available Data from October 2019 through March 2022 16
Data for Figure 3: Reported Number of Searches That Federal Agencies Conducted Using Facial Recognition Services, Based on Available Data from October 2019 through March 2022 16
Figure 4: Selected Federal Law Enforcement Agencies' Reported Use of Facial Recognition Services 18
Figure 5: Homeland Security Investigations Agent Working to Identify Suspected Child Abusers and Victims 20
Figure 6: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023 23
Data for Figure 6: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023 (October 1, 2019 through March 31, 2022) 23
Figure 7: Extent to which Selected Agencies Addressed Selected Privacy Requirements while Using Facial Recognition Services, as of April 2023 36

Data for Figure 7: Extent to which Selected Agencies Addressed Selected Privacy Requirements while Using Facial Recognition Services, as of April 2023 37

Abbreviations

AI	artificial intelligence
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CBP	U.S. Customs and Border Protection
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
PIA	privacy impact assessment
PII	personally identifiable information

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 5, 2023

Congressional Requesters

Facial recognition technology is a tool that the federal law enforcement community may use to help solve crimes. For example, facial recognition technology can allow users to quickly search through billions of photos to help identify an unknown suspect in a crime scene photo. A criminal investigator can also use this technology to help identify a victim in a photo or video. Federal agencies can own facial recognition technology or leverage technology owned by state and local governments. Federal agencies can also use facial recognition services offered by commercial and nonprofit entities.[1] While facial recognition services may support criminal investigations, members of Congress have raised questions about the extent to which federal law enforcement agencies use such services.

We have previously examined aspects of federal law enforcement agencies' use of facial recognition technology. For example, in June 2021, we found that 14 federal agencies that employed law enforcement officers used facial recognition technology, such as commercial services, to support criminal investigations. However, we found that 13 of these agencies did not have complete, up-to-date information on which facial recognition systems staff were using. We recommended that the 13 agencies—including agencies within the Department of Homeland Security (DHS) and the Department of Justice (DOJ)—track the use of such systems and assess the associated risks.[2]

You asked us to review federal law enforcement's use of facial recognition technology and its effects on privacy, civil rights, and civil

[1] For the purposes of this report, the term facial recognition service includes services provided by nonprofit and commercial entities. Thus, the term facial recognition services does not include technology owned and operated by federal, state, and local government entities.

[2] As of July 2023, agencies have taken actions to fully or partially implement 11 of the 26 recommendations to track the use of facial recognition systems and assess the associated risks. See GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* GAO-21-518 (Washington, D.C.: June 2021).

liberties.[3] This report examines the extent to which selected DHS and DOJ law enforcement agencies have:

(1) used facial recognition services to support criminal investigations from October 2019 through March 2022;

(2) required staff to take training on facial recognition technology to use such services, and ensured compliance with requirements;

(3) taken steps to address selected privacy requirements for using facial recognition services; and,

(4) developed policies and guidance specific to facial recognition technology to help protect civil liberties and civil rights.

To address all four objectives, we selected seven agencies within DHS and DOJ that employ law enforcement officers (law enforcement agencies).[4] We limited our selection to DHS and DOJ agencies because these two departments employ the highest number of law enforcement officers within the federal government, and cumulatively employ more than 80 percent of all federal law enforcement officers.[5] From there, we identified DHS and DOJ law enforcement agencies that previously reported owning or using facial recognition technology systems in 2020.[6]

We then selected the seven agencies that reported owning or using the highest number of facial recognition systems to include in this review. Within the DHS, we selected U.S. Customs and Border Protection (CBP); U.S. Immigration and Customs Enforcement's (ICE) Homeland Security

[3] For the purposes of this review, we are defining "privacy" as individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information (PII), including data such as names, Social Security numbers, or photos. We are defining "civil rights" as due process protections and personal rights protected by the U.S. Constitution and federal laws, such as the Civil Rights Act of 1964; and "civil liberties" as the exercise of activities protected under the First Amendment.

[4] Consistent with our prior work, we define federal law enforcement officers as full-time employees with federal arrest authority who are authorized to carry firearms while on duty.

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

[6] GAO-21-518.

Investigations (HSI); and, the U.S. Secret Service.[7] Within the DOJ, we selected the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Drug Enforcement Administration (DEA); the Federal Bureau of Investigation (FBI); and, the U.S. Marshals Service. The seven law enforcement agencies we selected are not representative of all law enforcement agencies.

Our review included agencies that used facial recognition services in support of criminal investigations, including sharing information (e.g., leads). For example, one agency—CBP—told us that it does not lead criminal investigations but has used facial recognition services to develop and share information in support of other agencies' criminal investigations.[8] We focused exclusively on the use of facial recognition technology services offered by commercial and nonprofit entities (facial recognition services) to build upon our prior reports that reviewed technologies owned and operated by federal agencies.[9]

To address our first objective, we reviewed agency documentation and interviewed agency officials to identify commercial and nonprofit facial recognition services that agencies used from October 2019 through March 2022 to support criminal investigations.[10] We then obtained and analyzed available data to determine the total number of searches that agency staff conducted using these services from October 2019 through March 2022. We assessed the reliability of these data by interviewing knowledgeable agency officials and representatives from each service that agencies reported using during this time period. In addition, we

[7] HSI is one of the investigative agencies within DHS responsible for investigating transnational crime and threats. HSI conducts federal criminal investigations into the illegal cross-border movement of people, goods, money, technology, and other contraband throughout the United States.

[8] CBP officials told us that the agency used facial recognition services primarily for immigration enforcement and border security purposes.

[9] See for example, GAO-21-518; GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies,* GAO-21-526 (Washington, D.C.: Aug. 2021); GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO-20-568 (Washington, D.C.: Sep 2020); and, GAO, *FACE Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* GAO-16-267 (Washington, D.C.: May 2016, reissued Aug. 2016).

[10] We selected this timeframe to overlap with our prior work, and to extend to the most recent data available when we conducted our analysis. We previously reported on agencies' use of facial recognition technology from January 2015 through March 2020 (see GAO-21-518).

tested these data for outliers or obvious errors when possible. We determined that these data were sufficiently reliable for reporting on the minimum number of searches conducted by agencies during the period of our review.

To address our second objective, we reviewed agency documentation, including policies, guidance, and memorandums to determine the extent to which agencies required staff to take training on facial recognition technology to use such services.[11] In addition, we interviewed officials and reviewed available training materials to understand the nature and purpose of such training.[12] To understand the extent to which trained and untrained staff used facial recognition services, we then obtained and analyzed available data on staff training and facial recognition searches that staff conducted.

We assessed the reliability of these data by interviewing knowledgeable agency officials and company representatives, reviewing existing information about the data systems, and testing these data for outliers or obvious errors when possible. We determined that these data were sufficiently reliable for reporting on the number of trained and untrained staff who used facial recognition services. Finally, we compared the agencies' efforts to ensure compliance with training requirements to agency policy, our human capital guidance, and *Standards for Internal Control in the Federal Government*.[13]

To address our third objective, we reviewed relevant departmental privacy policies and guidance, such as DHS and DOJ guidance on implementing

[11] We assessed the extent to which agencies had implemented training specifically required for using facial recognition services, and did not assess requirements for more general training that agency staff may receive, such as general privacy training. We considered a training requirement to be written instruction to staff mandating training as a condition of access to a facial recognition service.

[12] We did not evaluate the content of this training to ascertain its sufficiency or appropriateness because there are no national training standards for facial recognition technology, which we discuss later in this report.

[13] GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004), GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

aspects of the E-Government Act of 2002.[14] Based on our review of these policies and guidance, we identified four privacy requirements that generally apply to agencies when using facial recognition services.[15] To identify the extent to which agencies addressed selected privacy requirements for using facial recognition services, we analyzed agency documentation—such as initial privacy reviews, privacy impact assessments, sensitive information and privacy checklists, and contract documentation. We also interviewed cognizant agency officials. Finally, we compared agencies' efforts to address selected privacy requirements for using facial recognition services to principles in the *Standards for Internal Control in the Federal Government*.[16]

To address our fourth objective, we reviewed agency documentation and interviewed agency officials to understand the extent to which agencies had existing policies and guidance that addressed civil rights and civil liberties in the context of facial recognition technology. We also reviewed a congressional report and executive order related to facial recognition technology policies.[17] We then interviewed department officials to understand their efforts to develop and implement new department-wide guidance related to civil rights and civil liberties specific to facial recognition technology, and to address the congressional report and

[14] Department of Homeland Security, Privacy Office, *Privacy Impact Assessments: Privacy Office Official Guidance*, (Washington, D.C.: June 2010). Department of Justice, Office of Privacy and Civil Liberties, *Privacy Impact Assessments: Official Guidance*, (Washington, D.C.: Revised July 2015). The E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921 (2002).

[15] The specific requirements applicable to DHS's and DOJ's use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. The four key privacy requirements we selected are (1) conduct initial privacy review; (2) conduct privacy impact assessment; (3) assess privacy needs prior to acquisition, and (4) oversee privacy controls for contractor access to PII. In addition, not all listed privacy requirements may apply to an agency's use of a facial recognition service. For example, an agency may conclude in its initial privacy review that a privacy impact assessment is not required.

[16] GAO-14-704G.

[17] See H.R. Rep. No. 117-97 (2021) (accompanying Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022) and incorporated by reference in the explanatory statement for the Act, 168 Cong. Rec. H1772 (2022)); Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

executive order. We compared agencies’ efforts to develop such policies and guidance to leading project management practices.[18]

Appendix I provides additional information on our scope and methodology for all four objectives.

We conducted this performance audit from January 2022 through September 2023 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.

Background

Facial Recognition Technology for Criminal Investigations

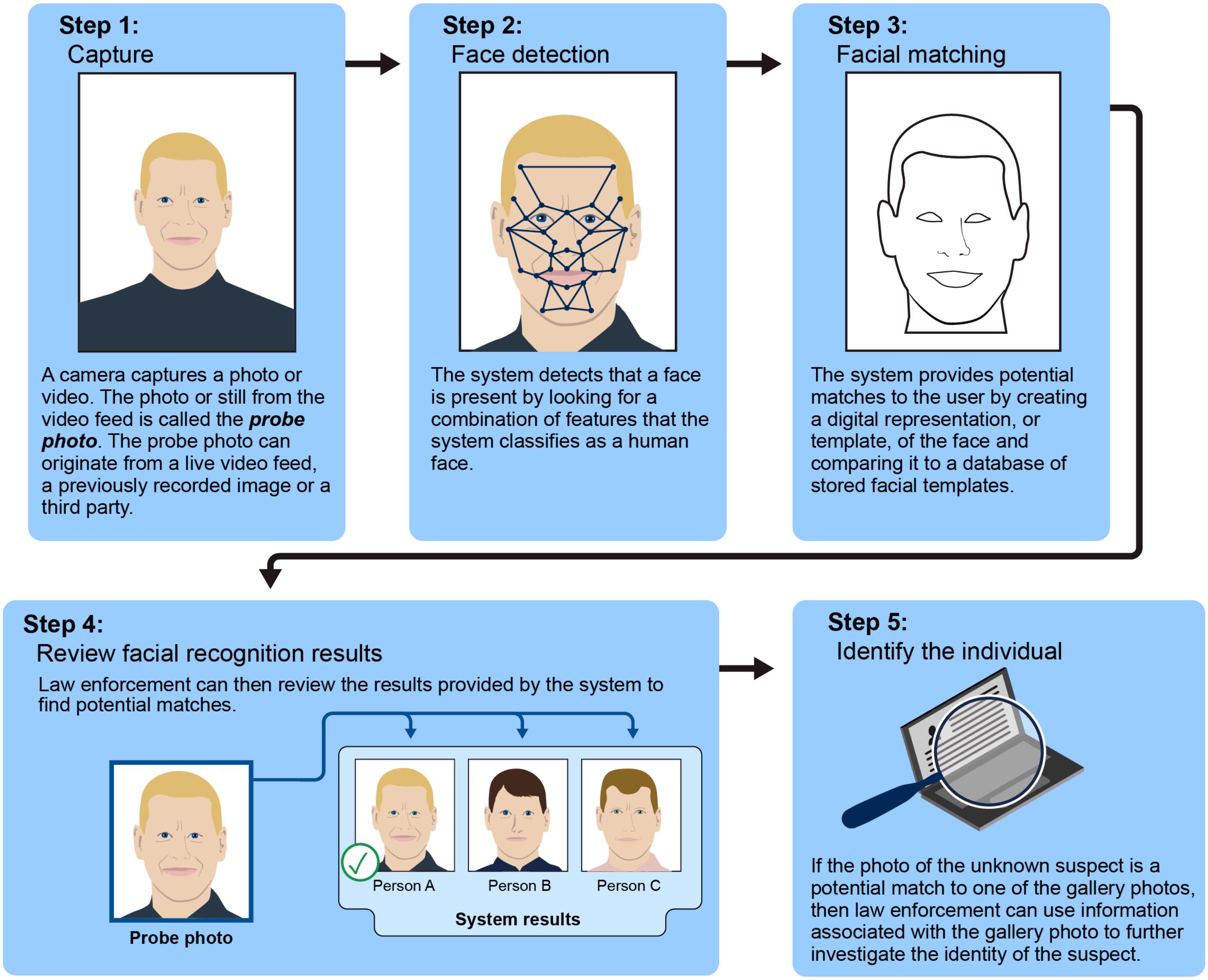
An identification search (or one-to-many search) is a type of facial recognition search used by the law enforcement community to support criminal investigations. Identification searches compare a photo of a single unknown individual against a gallery of photos to determine if there is a potential match (i.e., an investigative lead). For example, investigators may compare a photo of an unknown suspect from a crime scene against a facial recognition service’s gallery of photos.[19] If the photo of the unknown suspect is a potential match to one of the gallery photos, investigators can then use information associated with the gallery photo to investigate the identity of the suspect further. For example, a gallery photo may be linked to a public social media profile. Investigators can review details found in the profile, such as name and location, in conjunction with information gathered from other sources (e.g., information from witnesses, or evidence found at a crime scene) to potentially determine the identity of the suspect. Figure 1 shows how law

[18] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition* (2017). PMBOK is a trademark of Project Management Institute, Inc. The Project Management Institute is a not-for-profit association that, among other things, provides standards for managing various aspects of projects, programs, and portfolios.

[19] The photos in a facial recognition service’s gallery may be drawn from various sources, including public web sites.

enforcement may use a facial recognition identification search to support a criminal investigation.

Figure 1: Facial Recognition Technology Identification Search Process for Criminal Investigations



Step 1: Capture

A camera captures a photo or video. The photo or still from the video feed is called the ***probe photo***. The probe photo can originate from a live video feed, a previously recorded image or a third party.

Step 2: Face detection

The system detects that a face is present by looking for a combination of features that the system classifies as a human face.

Step 3: Facial matching

The system provides potential matches to the user by creating a digital representation, or template, of the face and comparing it to a database of stored facial templates.

Step 4: Review facial recognition results

Law enforcement can then review the results provided by the system to find potential matches.

Step 5: Identify the individual

If the photo of the unknown suspect is a potential match to one of the gallery photos, then law enforcement can use information associated with the gallery photo to further investigate the identity of the suspect.

Source: GAO analysis. | GAO-23-105607

Text for Figure 1: Facial Recognition Technology Identification Search Process for Criminal Investigations

Step 1: Capture

A camera captures a photo or video. The photo or still from the video feed is called the probe photo. The probe photo can originate from a live video feed, a previously recorded image or a third party.

Step 2: Face detection

The system detects that a face is present by looking for a combination of features that the system classifies as a human face.

Step 3: Facial matching

The system provides potential matches to the user by creating a digital representation, or template, of the face and comparing it to a database of stored facial templates.

Step 4: Review facial recognition results

Law enforcement can then review the results provided by the system to find potential matches.

Step 5: Identify the individual

If the photo of the unknown suspect is a potential match to one of the gallery photos, then law enforcement can use information associated with the gallery photo to further investigate the identity of the suspect.

Source: GAO analysis. | GAO-23-105607

Training Requirements to Use Facial Recognition Services in Criminal Investigations

There are no federal laws or regulations that require specific training for DHS or DOJ employees using facial recognition technology or services to support criminal investigations. A scientific working group that focuses on facial identification has developed training standards for using facial recognition technology, but federal agencies are not required to adopt these standards.[20] However, federal law enforcement agencies may establish their own training requirements for using facial recognition services, and we discuss the extent to which DHS and DOJ have done so later in this report.

Privacy Requirements for Using Facial Recognition Services

DHS and DOJ consider photos, such as those used for facial recognition services, as personally identifiable information (PII).[21] The departments' guidance directs agencies to take certain steps to help prevent the inappropriate collection, use, and release of PII when acquiring or using services that collect such information. The requirements applicable to DHS's and DOJ's use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. Table 1 provides an overview of selected privacy requirements.[22]

[20] The Facial Identification Scientific Working Group, which includes DHS and DOJ representatives, aims to develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features and to provide recommendations for research and development activities necessary to advance the state of the science in this field. The working group participates in an ongoing initiative by National Institute of Standards and Technology and DOJ to strengthen forensic science in the United States.

[21] Department of Homeland Security, Privacy Office, *Privacy and Civil Liberties Policy Guidance Memorandum*, (Washington, D.C.: June 20009). Department of Justice, Office of Privacy and Civil Liberties, *Initial Privacy Assessment Instructions and Template, Revised 2019.* For the purposes of this report, we are defining PII as any information that can be used to distinguish or trace an individual's identity, such as a photo, name, date and place of birth, and Social Security number; or that otherwise can be linked to an individual, in accordance with DHS, DOJ, and Office of Management and Budget Guidance.

[22] The privacy requirements that we selected for this review are from DHS and DOJ privacy guidance, including guidance on implementing the E-Government Act's Privacy Impact Assessment provision. There may be other privacy requirements that apply to federal agencies' use of services that collect PII that we do not discuss. E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921 (2002). The E-Government Act of 2002 addresses the protection of personal information in government information systems or information collections by requiring that agencies take certain steps to analyze how personal information is collected, stored, shared, and managed in a federal system.

Table 1: Selected Privacy Requirements for Department of Homeland Security's (DHS) and Department of Justice's (DOJ) Use of Facial Recognition Services

Conduct Initial Privacy Review	DHS and DOJ agencies are to complete initial privacy reviews when they intend to design, develop, or procure a project that will include personally identifiable information (PII), such as a facial recognition service. These reviews help agencies identify potential privacy issues related to the use of PII; assess whether additional privacy requirements apply; and ultimately, help ensure the agency's compliance with applicable privacy laws and policies. Based on its initial privacy review, an agency may determine that use of a service requires a more comprehensive privacy assessment, known as a privacy impact assessment (PIA).
Conduct Privacy Impact Assessment (PIA)	DHS and DOJ agencies are to complete PIAs before developing or procuring information technologies that collect, maintain, or disseminate PII. A PIA is an analysis of how PII is handled to (1) ensure compliance with applicable privacy requirements; (2) determine the privacy risks associated with an information system or activity; and, (3) evaluate ways the agency can mitigate potential privacy risks. For example, in a PIA, an agency may identify staff conducting inappropriate facial recognition searches as a potential privacy risk. The agency may then identify a related mitigation—such as requiring all staff take training on the appropriate use of facial recognition technology—that will help manage the potential privacy risk.
Assess Privacy Needs Prior to Acquisition	DHS and DOJ guidance directs agencies to consider privacy needs in decisions concerning the acquisition of services that handle PII. For example, the DHS Acquisition Manual requires that staff complete a checklist of considerations for sensitive information (including PII) for all acquisitions regardless of dollar value. Additionally, DOJ guidance states that privacy should be considered in the beginning stages of a proposed project, whether that project necessitates an external acquisition or not, to ensure that privacy protections are built into the system from the start.
Oversee Privacy Controls for Contractor Access to Personally Identifiable Information	DHS and DOJ agencies must include certain terms related to privacy in contracts when contractors will have access to PII. DHS acquisition regulations require that when contractors have access to sensitive information, including PII, DHS contracts are to include terms to safeguard PII.[a] For example, such DHS contracts are to include a clause requiring contractors with access to sensitive information to sign non-disclosure agreements, and direct how contractors are to handle PII. Similarly, DOJ requires contracts to include terms requiring contractors with access to PII take privacy training, sign non-disclosure agreements, and report data breaches, among other privacy requirements.

Source: GAO analysis of DHS and DOJ privacy guidance. | GAO-23-105607

Note: These selected privacy requirements are from DHS and DOJ privacy guidance, including guidance on implementing the E-Government Act's Privacy Impact Assessment provision. The specific requirements applicable to DHS's and DOJ's use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. Further, there are other privacy requirements that can apply to the departments' use of these services that are not included in this table and that were not included in our review.

[a] See Department of Homeland Security, *HSAR Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* (Washington, D.C., Mar. 2015); Homeland Security Acquisition Regulation § 3052.204-71(a).

Facial Recognition Technology, Civil Rights and Civil Liberties

The use of facial recognition technology for criminal investigations presents unique questions about civil rights and civil liberties. For example, civil liberties advocates have noted that the use of facial recognition at certain events—such as protests—could have a chilling effect on individuals' exercise of their First Amendment rights.[23] Additionally, facial recognition technology, like all artificial intelligence (AI) technology, contains the potential for error and thus the potential to misidentify individuals.[24] As a result, civil rights advocates have cautioned that an over-reliance on facial recognition technology in criminal investigations could lead to the arrest and prosecution of innocent people, and in particular innocent people of certain racial and ethnic backgrounds.[25]

Though not specific to facial recognition technology, both DOJ and DHS have longstanding guidance and policies that officials stated apply to the technology and can help safeguard civil liberties and civil rights during criminal investigations. For example, since 2003, DOJ has had guidance that limits the use of demographic characteristics by all federal law enforcement officers (including DHS law enforcement officers) during domestic law enforcement activities.[26] Additionally, in 2019, the DHS Secretary issued a memorandum to all employees emphasizing long-standing legal prohibitions on maintaining records that describe how U.S.

[23] See, e.g., *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight and Reform,* 116th Cong. (2019) (statement of Neema Singh Guliani, Senior Legislative Counsel, American Civil Liberties Union).

[24] Since 2018, the National Institute of Standards and Technology has tested facial recognition algorithms, and reported 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 algorithm developer, type of error, and quality of the facial images. National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST Interagency or Internal Report 8280 (Dec. 19, 2019).

[25] National Association of Criminal Defense Lawyers, *Letter to the White House Office of Science and Technology Policy*, January 15, 2022.

[26] Department of Justice, *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, Gender Identity and Disability* (Washington, D.C.: 2023). Among other things, the current version of guidance notes that federal law enforcement officers may not use race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in making routine or spontaneous law enforcement decisions. This guidance is limited to domestic law enforcement activities and does not apply to U.S. military, diplomatic, or non-Department of Justice intelligence agencies and their activities. In addition, this Guidance does not apply to interdiction activities at the border or its functional equivalent (e.g., airports, seaports, and other ports of entry) and related traveler and cargo vetting activities or to protective and inspection activities.

citizens and certain other individuals exercise their First Amendment rights.[27]

In addition, Congress and the President have directed certain federal departments to develop new policies to help ensure the protection of civil rights and civil liberties when using facial recognition technology. For example, a House committee report accompanying DOJ's fiscal year 2022 appropriations act directed DOJ to develop ethical policies for the use of facial recognition technology.[28]

Additionally, in May 2022, the President issued Executive Order 14074, which directed DOJ and DHS to take actions related to facial recognition technology.[29] The executive order directed DOJ to enter into a contract with the National Academy of Sciences by November 2022, for the purposes of conducting a study on facial recognition technology that includes an assessment of privacy, civil rights, and civil liberties concerns. The executive order also calls for DOJ, DHS, and the White House Office of Science and Technology Policy to lead an interagency effort to identify best practices for law enforcement agencies using facial recognition technology, and issue a report describing any resulting policy changes by November 2023.

Federal Law Enforcement Agencies Used Four Facial Recognition Services to Support Criminal Investigations

The seven federal law enforcement agencies in our review—ATF, CBP, DEA, FBI, HSI, the Marshals Service, and the Secret Service—reported

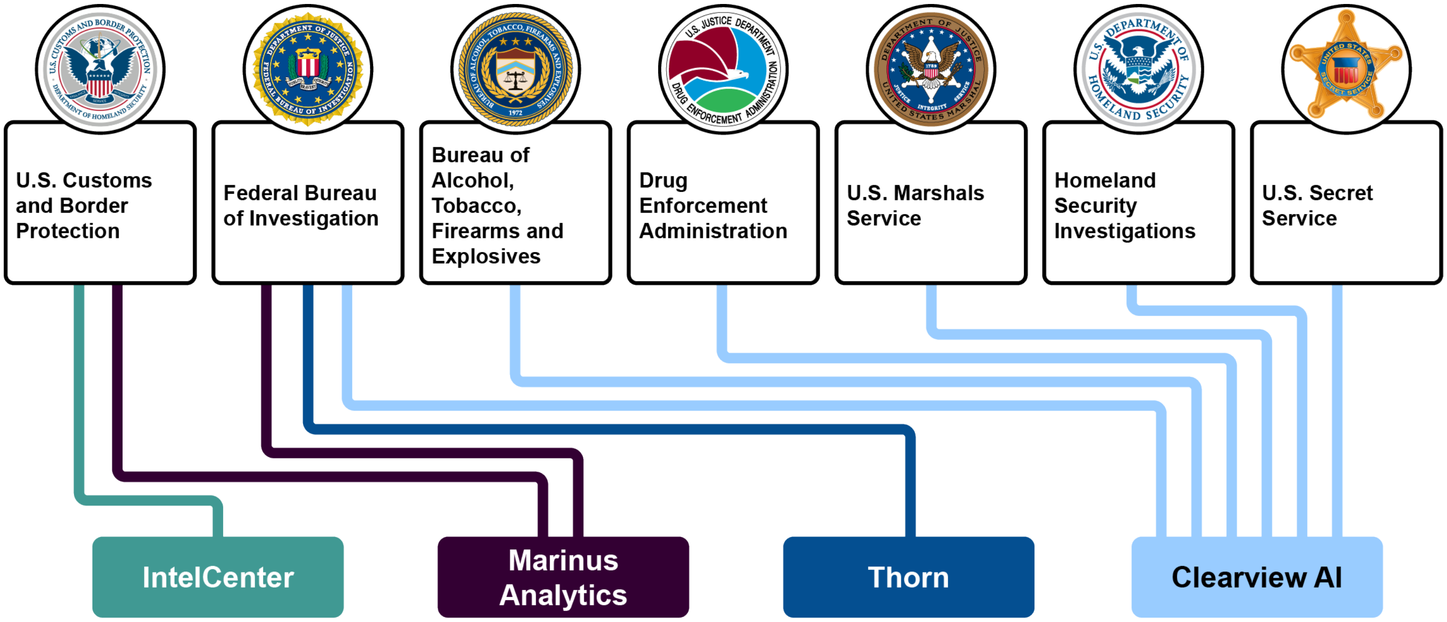
[27] Department of Homeland Security, Acting Secretary*, Information Regarding First Amendment Protected Activities*, (Washington, D.C.: May 17, 2019). This memorandum notes that under the Privacy Act of 1974, all DHS personnel are prohibited from maintaining records that describe how a U.S. citizen or legal permanent resident exercises his or her First Amendment rights, "unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

[28] See H.R. No. 117-97, at 60 (2021) (accompanying Pub. L. No. 117-103, 136 Stat. 49 (2022) and incorporated by reference in the explanatory statement for the Act, 168 Cong. Rec. H1772 (2022)). The committee report directed DOJ to develop ethical policies and required that DOJ report not later than 90 days after the enactment of the Consolidated Appropriations Act on the status of establishing such policies, but did not specify a deadline for the completion of these policies.

[29] Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

using four different facial recognition services in total to support criminal investigations from October 2019 through March 2022 (see figure 2). These services gather photos from various sources, such as social media and mugshot websites. In addition, some of these services support certain types of criminal investigations. For example, FBI told us it used Marinus Analytics's Traffic Jam service to support human trafficking investigations. Figure 2 provides more information about the four services used by the law enforcement agencies in our review.

Figure 2: Facial Recognition Services Used by Selected Federal Law Enforcement Agencies to Support Criminal Investigations from October 2019 through March 2022


U.S. Customs and Border Protection
Federal Bureau of Investigation
Bureau of Alcohol, Tobacco, Firearms and Explosives
Drug Enforcement Administration
U.S. Marshals Service
Homeland Security Investigations
U.S. Secret Service
IntelCenter
Marinus Analytics
Thorn
Clearview AI

IntelCenter's Terrorist Facial Recognition is a web-based service. The service allows users to search photos against a gallery of over 2.4 million faces extracted from open-source terrorist data, according to service representatives and web site materials.

Marinus Analytics's Traffic Jam is a web-based service that includes facial recognition capabilities. Traffic Jam uses images from the online commercial sex market to identify victims of human trafficking both in the United States and abroad, according to service representatives and web site materials.

Thorn's Spotlight is a web-based service that includes facial recognition capabilities. Spotlight uses images from the online commercial sex market to find exploited children and identify their traffickers to support sex trafficking investigations, according to service representatives and web site materials.

Clearview AI is a web-based facial recognition service using 30+ billion facial images sourced from publicly-available websites, including news media, mugshot, and social media websites, among others, according to service representatives and web site materials.

Source: GAO analysis of facial recognition service information. | GAO-23-105607

Text for Figure 2: Facial Recognition Services Used by Selected Federal Law Enforcement Agencies to Support Criminal Investigations from October 2019 through March 2022

System	IntelCenter	Marinus Analytics	Thorn	Clearview AI
System description	IntelCenter's Terrorist Facial Recognition is a web-based service. The service allows users to search photos against a gallery of over 2.4 million faces extracted from open-source terrorist data, according to service representatives and web site materials.	Marinus Analytics's Traffic Jam is a web-based service that includes facial recognition capabilities. Traffic Jam uses images from the online commercial sex market to identify victims of human trafficking both in the United States and abroad, according to service representatives and web site materials.	Thorn's Spotlight is a web-based service that includes facial recognition capabilities. Spotlight uses images from the online commercial sex market to find exploited children and identify their traffickers to support sex trafficking investigations, according to service representatives and web site materials.	Clearview AI is a web-based facial recognition service using 30+ billion facial images sourced from publicly-available websites, including news media, mugshot, and social media websites, among others, according to service representatives and web site materials.
U.S. Customs and Border Protection	Used	Used	Not used	Not used
Federal Bureau of Investigation	Not used	Used	Used	Used
Bureau of Alcohol, Tobacco, Firearms and Explosives	Not used	Not used	Not used	Used
Drug Enforcement Administration	Not used	Not used	Not used	Used
U.S. Marshals Service	Not used	Not used	Not used	Used
Homeland Security Investigations	Not used	Not used	Not used	Used
U.S. Secret Service	Not used	Not used	Not used	Used

Source: GAO analysis of facial recognition service information. | GAO-23-105607

DHS and DOJ officials stated that, as of April 2023, these law enforcement agencies had limited their use of facial recognition services in criminal investigations to conducting identification searches to generate investigative leads, or to help identify potential victims in specific investigations such as human trafficking cases. Additionally, HSI officials told us that within ICE, only HSI has used Clearview AI to support criminal investigations, and that ICE has not used this service in immigration law enforcement or removal operations.

CBP officials told us the agency does not lead criminal investigations but may develop and share information in support of other agencies' criminal investigations. For example, CBP officials stated that they have used facial recognition services to identify potential terrorists, transnational criminals, and individuals who pose a higher risk of violating U.S. law. If CBP identifies something criminal in nature, officials stated that they would refer the information to other law enforcement agencies to conduct criminal investigations, such as HSI.

Six agencies with available data reported conducting approximately 63,000 searches using facial recognition services from October 2019 through March 2022 in aggregate—an average of 69 searches per day.[30] We refer to the number of searches as approximately 63,000 because the aggregate number of searches that the six agencies reported is an undercount.[31] Specifically, the FBI could not fully account for searches it conducted using two services, Marinus Analytics and Thorn.[32] Additionally, the seventh agency (CBP) did not have available data on the number of searches it performed using either of two services staff used.[33] Figure 3 provides information on the number of searches agencies reported conducting during this time period, to the extent this information was available.

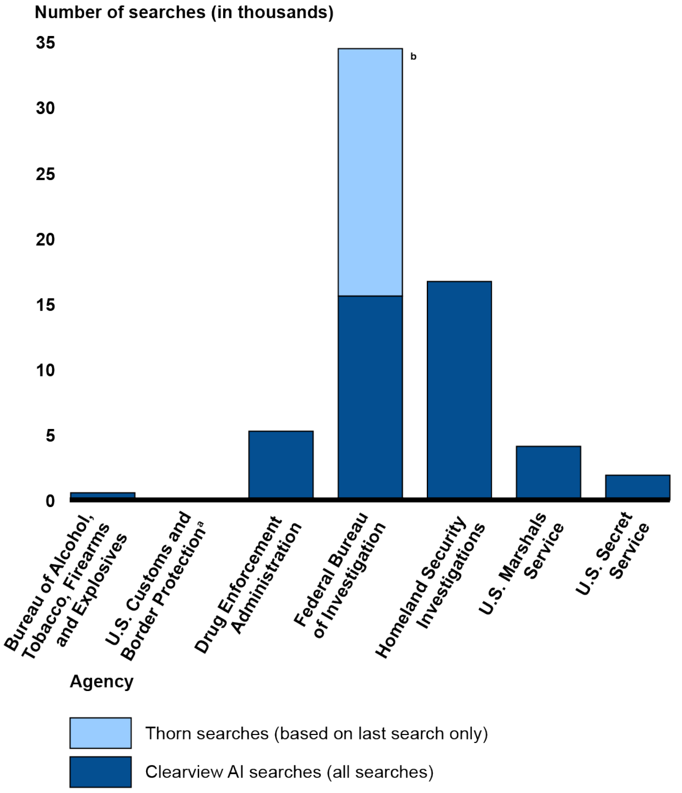
[30] For this analysis, we defined a search as any instance of comparing a probe photo to a facial recognition service's gallery of photos. Additionally, when an agency searched the same probe photo multiple times but at different points in time, we included each individual search in our count. For instance, if an agency conducted three searches on the same probe photo at different times or dates, we included all three searches in our count.

[31] It is difficult to determine the overall extent to which agencies use facial recognition services, in part, because of variation in how facial recognition services and agencies using those services track the number of searches conducted by agency staff. Additionally, in 2021, we found that some agencies did not track what facial recognition systems staff used and therefore agencies may not have a complete list of facial recognition searches on untracked systems (see GAO-21-518).

[32] Specifically, neither the FBI nor Marinus Analytics tracked the number of searches staff conducted during this time. Additionally, Thorn, only tracked the last time the agency searched using a specific probe photo, and not each time the agency searched using that same probe photo. Marinus Analytics representatives told us that the service did not track the number of facial recognition searches, but it would be able to establish the capability to track searches upon the request of a client organization.

[33] CBP officials were unable to provide information on the number of facial recognition searches staff conducted during this time because neither the agency nor the services tracked this information.

Figure 3: Reported Number of Searches That Federal Agencies Conducted Using Facial Recognition Services, Based on Available Data from October 2019 through March 2022



Source: GAO analysis of data provided by agencies and facial recognition services. | GAO-23-105607

Data for Figure 3: Reported Number of Searches That Federal Agencies Conducted Using Facial Recognition Services, Based on Available Data from October 2019 through March 2022

Federal Agency	Clearview AI searches (all searches)	Thorn searches (based on last search only)
Bureau of Alcohol, Tobacco, Firearms and Explosives	0.549	NA
U.S. Customs and Border Protection	0	NA
Drug Enforcement Administration	5.25	NA
Federal Bureau of Investigation	15.567	18.9
Homeland Security Investigations	16.678	NA
U.S. Marshals Service	4.093	NA
U.S. Secret Service	1.886	NA

GAO Highlights

Source: GAO analysis of data provided by agencies and facial recognition services. | GAO-23-105607

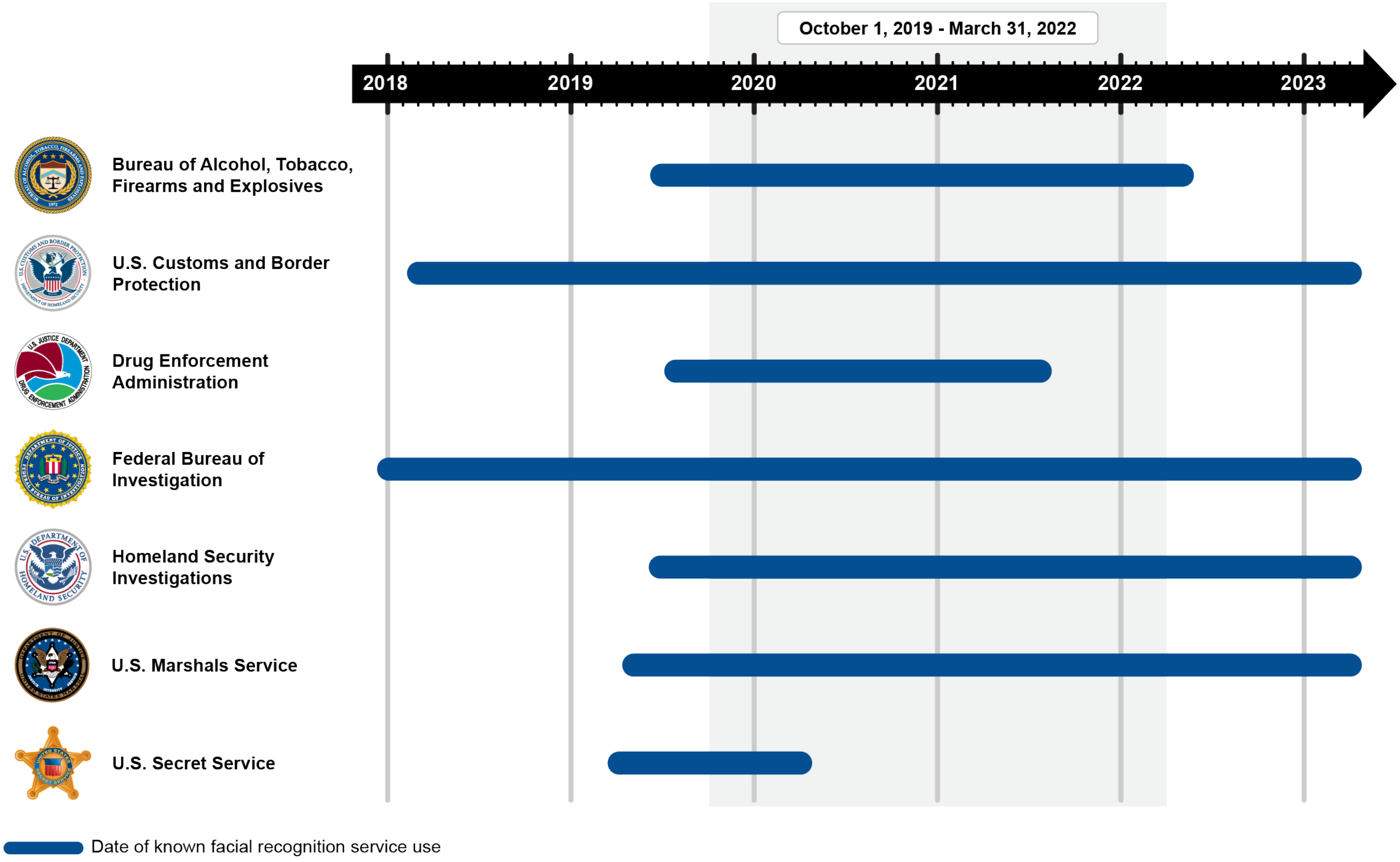
Note: For this analysis, we defined a search as any instance of comparing a probe photo to a commercial or nonprofit facial recognition service's gallery of photos. Additionally, when an agency searched the same probe photo multiple times but at different points in time, we included each individual search in our count. For instance, if an agency conducted three searches on the same probe photo at different times or dates, we included all three searches in our count. The number of searches conducted in this time period may be incomplete. For example, in 2021, we found that some agencies did not track what facial recognition systems staff used and therefore agencies may not have a complete list of facial recognition searches on untracked systems (see GAO-21-518).

[a]CBP officials were unable to provide information on the number of facial recognition searches staff conducted on the two services it used during this time—IntelCenter and Marinus Analytics—because neither the agency nor the services tracked this information. CBP officials acknowledged that staff used two services with facial recognition capabilities.

[b]The number of searches that FBI reported conducting in this time period is an undercount. This is because the FBI could not fully account for searches it conducted using two services, Marinus Analytics and Thorn. Specifically, the figure does not include searches for Marinus Analytics because neither the FBI nor Marinus Analytics tracked the number of searches staff conducted on the service. Additionally, Thorn only tracked the last time the agency searched using a specific probe photo, and not each time the agency searched using that same probe photo.

Our review included facial recognition services that agencies used from October 2019 through March 2022, but some agencies began using these services before this period, and continued to use them after. For example, CBP began using IntelCenter services in 2018 and continued to use this service as of April 2023. Further, as of April 2023, four of the seven agencies in our review continued to use facial recognition services, including FBI, CBP, HSI, and the Marshals Service. However, as of April 2023, ATF, DEA, and the Secret Service reported that they had halted their use of such services. See figure 4.

Figure 4: Selected Federal Law Enforcement Agencies' Reported Use of Facial Recognition Services



Source: GAO analysis of agency information. | GAO-23-105607

Data for Figure 4: Selected Federal Law Enforcement Agencies' Reported Use of Facial Recognition Services (October 1, 2019 through March 31, 2022)

Timeline for use:

- ATF: earliest use in July 2019. Last use in May 2022.
- CBP: earliest use was March 2018. Continues to use as of April 2023.
- DEA: earliest use in August 2019. Last use in August 2021.
- FBI: earliest use in 2018. Continues to use as of April 2023.
- ICE: earliest use in June 2019. Continues to use as of April 2023.
- Marshals earliest use in May 2019. Continues to use as of April 2023.
- Secret Service: earliest use in April 2019. Last use in April 2020.

GAO Highlights

Source: GAO analysis of agency information. | GAO-23-105607

Note: Our review only included commercial and nonprofit facial recognition services that agencies reported using from October 1, 2019 to March 31, 2022 (see gray shading in figure). Agencies reported using four services during this time period. The timeline ranges from January 2018 through April 2023 because agencies may have used these four services prior to October 1, 2019 and continued to use the services after March 31, 2022.

For agencies that continued to use selected services after March 31, 2022, we collected data through April 12, 2023, the most recent data available at the time of our review. Additionally, in 2021, we found that some agencies did not track what systems staff used, and not all agencies have taken actions to address this issue (see GAO-21-518). Further, the timeline does not include agencies' use of government-owned facial recognition services, or commercial and nonprofit services that agencies stopped using prior to October 1, 2019, or began using after March 31, 2022.

According to agency training materials and officials, law enforcement agencies have used facial recognition services during criminal investigations to help identify relevant individuals, including both suspects and victims. See figure 5.[34]

[34] ATF officials noted that as of April 2023, ATF staff were not directly accessing facial recognition services. However, these officials noted that ATF routinely partners with state and local law enforcement agencies who may use such services during a joint investigation. We discuss agencies' ongoing use of the technology in greater detail later in this report.

Figure 5: Homeland Security Investigations Agent Working to Identify Suspected Child Abusers and Victims

Source: Josh Denmark/ U.S. Immigration and Customs Enforcement. | GAO-23-105607

For example:

- ICE training material indicates that HSI staff worked on a task force that used facial recognition services to help identify an individual suspected of involvement in the production of child sexual abuse materials. Specifically, according to HSI training documents, HSI investigators in the Cyber Crimes Center first extracted an image of the suspect's face from the child sexual abuse materials. Task force investigators then uploaded this photo to a facial recognition service. One of the potential matches for this photo was linked to an image on a public social media profile. Using this information, in conjunction with other investigative efforts, task force investigators were able to identify, locate, and arrest the suspect. According to the U.S. Attorney's Office, this individual pled guilty to federal charges of sexual exploitation of children and possession of child pornography and was sentenced to 35 years in prison.[35]

- ATF officials provided another example of the use of facial recognition services. According to the officials, an ATF task force investigated the suspected arson of a Pennsylvania State Police vehicle in Philadelphia. ATF investigators obtained video footage of a suspect, and uploaded images from this footage to a facial recognition service. One of the potential matches included a link to a public social media profile, which showed the individual was in Philadelphia on the day of the suspected arson. The profile also included the individual's cell phone number. ATF investigators obtained a search warrant to review location information from the individual's cellphone. Based on the location data, ATF investigators determined the suspect was at the location of the crime when it occurred. According to ATF officials, the individual was ultimately arrested, confessed to arson, and was sentenced to 364 days in jail.

Agencies with Available Data Reported Conducting About 60,000 Facial Recognition Searches Before Requiring Training

All seven agencies in our scope initially used facial recognition services without requiring staff to take training on topics such as how facial recognition technology works, what photos are appropriate to use, and how to interpret results. Some agencies required general privacy training for all staff, and made optional facial recognition training available to staff, both of which may have benefited staff using facial recognition services. However, we found that cumulatively, agencies with available data reported conducting about 60,000 searches—nearly all of the roughly 63,000 total searches—without requiring that staff take training on facial recognition technology to use these services.[36] While some agencies have since implemented training requirements, others have not assessed whether training would be beneficial. Additionally, although the FBI determined that training is needed, the agency has not yet implemented a

[35] Department of Justice, U.S. Attorney's Office for the District of Nevada, "Argentine Citizen Sentenced To 35 Years In Prison For Child Sexual Exploitation And Distribution Of Child Pornography Over The Dark Web," (Las Vegas, NV: Sept. 16, 2020).

[36] As discussed earlier in this report, there are limitations associated with the number of searches agencies reported conducting.

training requirement, and did not provide clear documentation to stakeholders about the status of its training requirement. Finally, in our review of FBI records, we found that only about 5 percent of FBI staff that accessed one facial recognition service had taken training.[37]

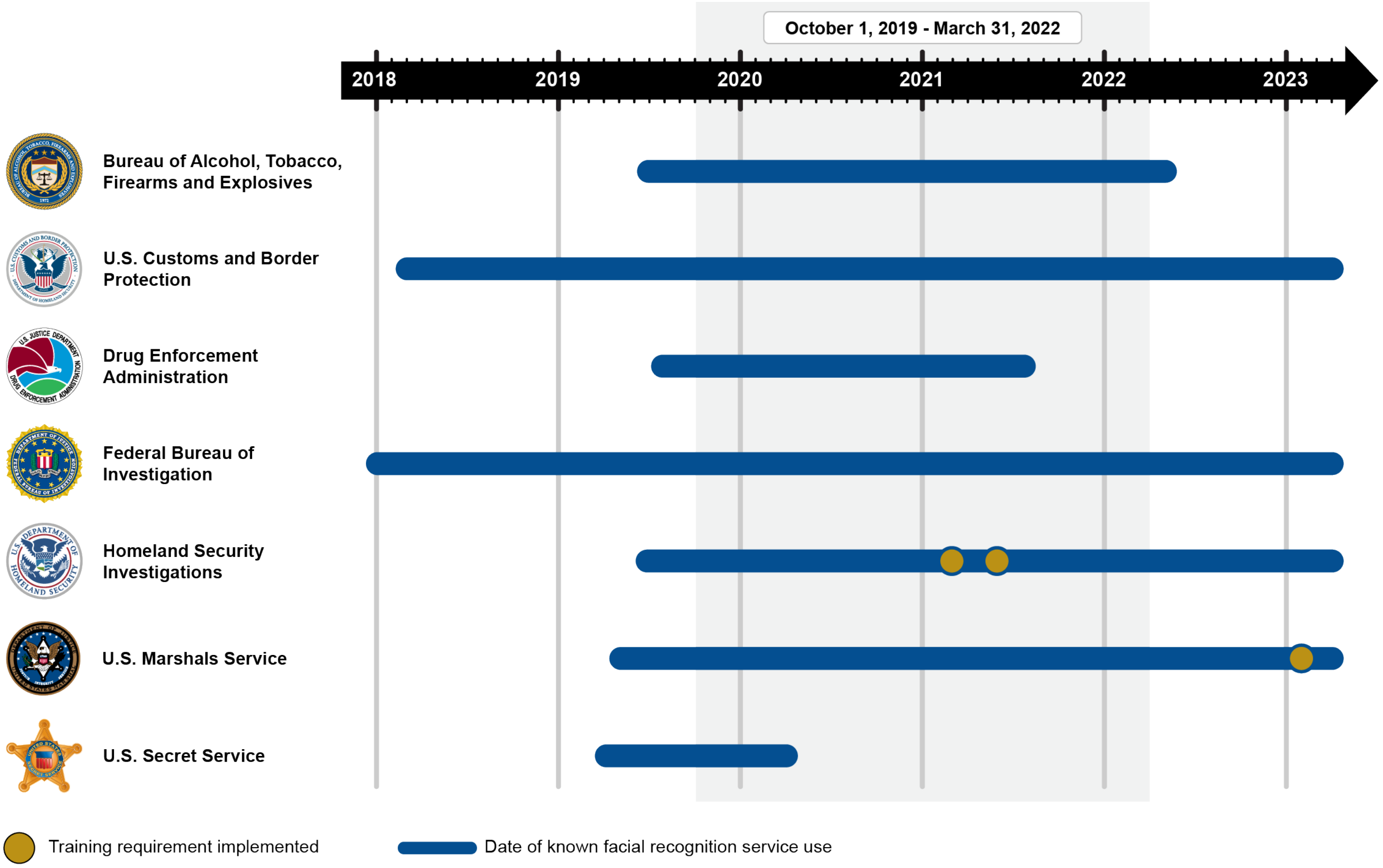
Two of Seven Agencies Have Implemented Training Requirements Specific to Facial Recognition Services

From October 2019 through March 2022, seven agencies used facial recognition services to support criminal investigations. During this time period, one agency—HSI—required staff to take facial recognition training prior to using services, while the other six agencies did not have requirements in place. In February 2023, the Marshals Service also implemented training requirements for staff. Among the remaining agencies that did not have training requirements, CBP and FBI continued to use the services and three agencies—ATF, DEA, and the Secret Service—as of April 2023 had halted their use of these services.[38] Figure 6 illustrates when agencies implemented training requirements, and when they began using the four facial recognition services mentioned earlier in this report.

[37] The three remaining agencies in our review—ATF, DEA, and the Secret Service—did not require staff to complete training but had halted their use of facial recognition services at the time of our review (i.e., as of April 2023).

[38] ATF, DEA and Secret Service officials told us that their headquarters officials were unaware that staff were using these services because staff were using free trial accounts. They said they directed staff to discontinue use of these services after discovery. We discuss this in greater detail later in this report.

Figure 6: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023



Source: GAO analysis of agency information. | GAO-23-105607

Data for Figure 6: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023 (October 1, 2019 through March 31, 2022)

Timeline for use:

- ATF: earliest use in July 2019. Last use in May 2022.
- CBP: earliest use was March 2018. Continues to use as of April 2023.
- DEA: earliest use in August 2019. Last use in August 2021.
- FBI: earliest use in 2018. Continues to use as of April 2023.
- ICE: earliest use in June 2019. Continues to use as of April 2023.
- Marshals earliest use in May 2019. Continues to use as of April 2023.

- Secret Service: earliest use in April 2019. Last use in April 2020.

Timeline for training:

- ATF: earliest use in July 2019. Last use in May 2022. No training.
- CBP: earliest use in March 2018. Continues to use as of April 2023. No training.
- DEA: earliest use in August 2019. Last use in August 2021. No training.
- FBI earliest use in 2018. Continues to use as of April 2023. No training.
- ICE: earliest use in June 2019. Implemented training requirements in March and June 2021. Continues to use as of April 2023.
- Marshals: earliest use in May 2019. Implemented training requirement in February 2023. Continues to use service as of April 2023.
- Secret Service: earliest use in Clearview AI in April 2019. Last use in April 2020. No training.

Source: GAO analysis of agency information. | GAO-23-105607

Note: This timeline represents agencies' use of commercial and nonprofit facial recognition services and training requirements to use such services between October 1, 2019 through March 31, 2022 (see gray shading in figure). The timeline ranges from January 2018 to April 2023 because agencies may have used these four services prior October 1, 2019 and continued to use these services after March 31, 2022. For agencies that continued to use selected services after our scope ends, we collected data as of April 12, 2023, the most recent data available at the time of our review. We assessed the extent to which agencies had implemented training specifically required for using facial recognition services, and did not assess requirements for more general training that agency staff may receive, such as general privacy training.

HSI. In 2021, HSI implemented two training requirements that staff must complete prior to using Clearview AI. HSI began requiring the first course, *ICE Use of Facial Recognition Services*, in March 2021.[39] This course, which is about three and a half hours in length, covers ICE policies for using third party facial recognition services and best practices for using such services. According to HSI officials, this training also provides information on the capabilities and limitations of facial recognition technology more generally as well as safeguards to help reduce errors and misuse. In addition, the training covers HSI staff responsibilities for protecting individuals' privacy, civil rights and civil liberties when using these services. For example, according to course materials we reviewed, the training covers ICE's policies designed to help avoid discrimination and ICE's policy limiting the collection of probe photos in certain contexts, such as participation at events protected by the First Amendment (e.g., protests).[40]

In addition, officials stated that HSI began requiring that staff using Clearview AI take a second course in July 2021. The *Clearview AI Facial Recognition Tool* course is a one-hour virtual training that provides information on how to use Clearview AI, including how to submit a probe photo and how to record the use of facial recognition searches in HSI tracking sheets and case files.[41]

[39] ICE established this requirement when the agency issued its *Use of and Access to Third Party Facial Recognition Services* memo in January 2021. The memo states that all staff must take and electronically certify that they completed the training course prior to using facial recognition services. U.S. Immigration and Customs Enforcement, Acting Executive Associate Director, *Use of and Access to Third-Party Facial Recognition Services,* Memorandum to All Homeland Security Investigations Personnel (Washington, D.C.: January 15, 2021). HSI officials stated they began enforcing this requirement two months later, in March 2021, when ICE made staff aware of the training requirement.

[40] In particular, the training notes that ICE may not collect probe photos based solely on an individual's religious, political, social views or activities, race, ethnicity, citizenship, place of origin, age, disability, gender identity, or sexual orientation. Additionally, the training re-iterates ICE's policy that staff may not collect probe photos based solely on an individual's participation in a noncriminal organization or event protected by the First Amendment.

[41] For example, HSI staff are to log certain information on the use of any commercial service in agency tracking sheets. This information includes the name of the service used, the date it was searched, the case number associated with the search, the number of probe photos submitted, and the results of the search, among other things. In addition, staff are to record the results of all facial recognition searches in the relevant case file and the associated report of investigation. U.S. Immigration and Customs Enforcement, *Clearview AI Facial Recognition Tool* (Washington, D.C.: July 9 2021).

Marshals Service. The Marshals Service recommended staff complete training as a best practice, but has since made such training required. According to officials, in February 2021, the Marshals Service began recommending staff complete training to use facial recognition services, but did not require staff to do so. In February 2023, the Marshals Service implemented a training requirement for staff using facial recognition services.[42] Specifically, staff must complete Clearview AI's virtual training session prior to initially using the service, and complete Clearview AI's refresher training annually.[43]

Marshals Service officials stated that this training, which is about four hours in length, provides an overview of the functions of Clearview AI. For example, officials stated that the training provides information on how to navigate and interpret possible matches on the service.[44] Further, officials stated that as part of the training, the service runs example searches and reviews the results with staff to help them understand how to interpret search results appropriately.

The Marshals Service has also taken steps to limit the number of staff that use the service. Specifically, the Marshals Service reached out to Clearview AI to suspend accounts of staff that were no longer using or did not have a need for using the service. This reduced the number of staff with active accounts from 103 to three. Based on our review of training

[42] In February 2023, the Marshals Service implemented training requirements and a process to help ensure compliance with these requirements. Given that the Marshals Service implemented these requirements as our audit was underway, we did not assess the agency's compliance process.

[43] The Marshals Service implemented training requirements by issuing a memorandum in February 2023. The memorandum states that all staff that use Clearview AI must complete Clearview AI's initial virtual training session prior to using the service and complete the service's virtual refresher session annually. The memorandum also requires that staff take agency-provided general privacy training. Among other things, officials stated that this training provides a general overview of privacy and civil liberties, their historical abuses, and staff obligations to protect privacy and civil liberties. U.S. Marshals Service, *Clearview AI Training Requirements* (Washington, D.C. Feb. 6 2023).

[44] Marshals Service officials stated that this includes training on how to interpret the degree of confidence the Clearview tool assigns to a potential match.

records, as of February 2023, all three staff that had access to Clearview AI completed the required training.[45]

FBI. As of April 2023, FBI did not require staff to complete training to use any of the three facial recognition services it uses—Clearview AI, Thorn or Marinus Analytics. FBI officials stated that although the agency did not require staff to complete training prior to using facial recognition services, they intend to develop such a requirement. We discuss this later in our report. Although not a requirement, FBI officials said they recommend (as a best practice) that some staff complete FBI's *Face Comparison and Identification Training* when using Clearview AI. The recommended training course, which is 24 hours in length, provides staff with information on how to interpret the output of facial recognition services, how to analyze different facial features (such as ears, eyes, and mouths), and how changes to facial features (such as aging) could affect results.[46] However, the recommendation does not apply to other FBI units using Clearview AI, or to staff using Thorn or Marinus Analytics. According to FBI officials, the agency has been using the facial recognition capabilities of Thorn and Marinus Analytics since 2018, when the capabilities were added to both services.

CBP. CBP does not require staff to take facial recognition training to access the two services it uses: IntelCenter and Marinus Analytics' Traffic Jam. According to officials, this is in part because they believe staff rarely use the facial recognition capabilities of either service, and instead predominantly use other features available through these services.[47] Additionally, CBP officials stated that the agency requires all staff to complete privacy training, and that staff could have taken facial comparison training as part of training for identifying fraudulent documents.

[45] We reviewed training records that showed all three staff completed the required trainings. Marshals Service officials stated all agency staff that would like probe photos searched against the Clearview AI gallery in support of an investigation must now work with one of the three trained staff. These three staff will conduct the searches and review results on behalf of the requestor, according to the agency officials.

[46] Federal Bureau of Investigation, *Face Comparison and Identification Training* (Washington, D.C.: Revised Dec. 2020).

[47] CBP officials stated that staff primarily use IntelCenter for its news alerts, and primarily use Marinus Analytics for its feature that aggregates online advertisements to help CBP gather information on certain criminal investigations. However, as we discuss later in the report, CBP does not track the extent to which the agency uses these services.

ATF, DEA, and Secret Service. ATF, DEA, and the Secret Service used Clearview AI during the period of our review, but did not require staff to complete training. Combined, these agencies conducted roughly 7,700 searches during the period of our review. Officials with all three agencies told us that, as of April 2023, they had halted their use of these services.

Most HSI Staff Completed Training, but HSI Could Better Monitor Whether Staff Take Training

Within ICE, HSI established a process to help ensure staff complete required training prior to using facial recognition services. We found that most staff completed this training before using facial recognition services. However, some staff did not complete the training. We reviewed training records from March 4, 2021—when HSI implemented its first training requirement—through March 31, 2022. We found that 106 HSI staff used Clearview AI, and 15 of those staff did not complete the required training prior to conducting searches (see table 2).[48]

Table 2: Training Status of Homeland Security Investigations Staff That Conducted Facial Recognition Searches on Clearview AI from March 4, 2021 through March 31, 2022

Training Status	Number of Staff	Number of Searches Conducted by Staff	Percentage of Total Searches Conducted by Staff
Trained Staff	91	2,120	79%
Untrained Staff	15	569	21%
Total	**106**	**2,689**	**100%**

Source: GAO analysis of agency data. | GAO-23-105607

Note: We considered staff trained if they completed all required training prior to conducting searches, and untrained if they had not completed all training requirements prior to conducting searches. Of the 15 untrained staff, 11 completed the agency's training requirements (though after conducting searches without such training), and four had not completed the training requirements as of March 31, 2022.

HSI officials told us that the official responsible for administering Clearview AI accounts is to review proof that staff complete the required training, and then provide the fully trained staff access to the service. HSI officials stated that they were unaware of any staff using Clearview AI without having completed the necessary training requirements. In January 2023, officials also told us HSI did not conduct periodic reviews to ensure

[48] We analyzed training records from March 4, 2021 through March 31, 2022 to determine the number of trained and untrained staff. Specifically, we reviewed the date each individual completed training. We considered staff trained if they completed all required training prior to conducting searches, and untrained if they had not completed all training requirements prior to conducting searches.

that staff using Clearview AI had met training requirements. In addition, HSI officials stated that the agency had not evaluated the current approval process to ensure it is working as intended.

As previously described, ICE issued a memorandum that established a training requirement for staff using facial recognition services. *Standards for Internal Control in the Federal Government* states that management should design and implement controls to help achieve agencies' objectives, which, in this case, is to ensure only trained staff use facial recognition services. Further, the internal control standards state that management should periodically monitor the internal control system and evaluate results to help ensure controls are working as intended.[49]

Since we conducted our initial audit work, HSI officials have taken steps to improve staff adherence to training requirements. Specifically, HSI officials told us that the agency conducted a one-time review of all staff using Clearview AI to determine whether staff received required training and whether staff should still have access to the service. As a result of this one-time review, HSI officials reported that they were able to ensure that all staff using Clearview AI as of July 2023 had completed training. Officials also stated that they intend to conduct additional reviews, but had not established or implemented a process for periodically monitoring whether staff have completed training requirements.

ICE has highlighted the importance of its training to help reduce errors and inappropriate use of facial recognition technology by staff. For example, the *ICE Use of Facial Recognition Services* training course teaches staff about common issues in probe photos (e.g., photos with poor resolution or with part of the face obstructed) that could cause errors when using them, and how to reduce these errors. The agency has developed a process to help ensure staff take the required training, and we found that many staff followed this process. However, HSI has not established or implemented a process to periodically review whether all staff with access to facial recognition services received required training. For example, as noted earlier, our review found that 15 staff had conducted over 500 searches before completing the required training. HSI officials took the positive step of conducting a one-time review of staff training and access to Clearview AI. However, without establishing and implementing a process to periodically monitor whether staff using facial

[49] GAO-14-704G.

recognition services have completed training, HSI faces a continued risk that untrained staff may use facial recognition services.

Key FBI Stakeholders Were Not Given Clear Documentation on Training Requirements

Federal government officials and others have emphasized the importance of training to help prevent potential abuse of facial recognition technology and increase public confidence in the technology. For example, the FBI has emphasized the importance of facial recognition training, and FBI officials told key internal stakeholders, including the AI Ethics Council and the Privacy and Civil Liberties Unit, that certain staff must take training to use one facial recognition service (Clearview AI).[50] However, FBI officials told us that while the agency recommends that staff in one unit take training to use a facial recognition service, it does not require any staff that use facial recognition services to take training, and we found that few staff did so. Additionally, FBI officials told us they intend to implement a training requirement, but the agency has not yet done so.

In February 2022, program officials provided documentation to the FBI AI Ethics Council to review the use of Clearview AI by a specific FBI unit.[51] The documentation stated that staff in the unit must take training to use

[50] See, e.g., *The Use Of Facial Recognition Technology By Government Entities and the Need for Oversight of Government Use of this Technology Upon Civilians: Hearing before H. Comm. on Oversight and Reform*, 116th Cong. (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation). In this testimony, FBI stated that every facial recognition search—including facial recognition results received from partners—is reviewed and evaluated by trained FBI examiners to ensure the results are consistent with FBI standards. FBI officials told us that this testimony focused on FBI's Criminal Justice Information Services use of facial recognition services, which does not include Clearview AI.

[51] According to FBI officials, the agency's AI Ethics Council helps the FBI identify, review, and assess new and existing AI deployed and operating in support of agency missions. FBI's Privacy and Civil Liberties Unit within the Office of General Counsel is responsible for, among other things, providing legal advice and counsel on compliance with federal law protecting individual privacy, and best practices to achieve an appropriate balance between protecting civil liberties and facilitating FBI activities. Officials stated that the AI Ethics Council evaluated whether FBI's AI use cases and systems comply with ethical principles in accordance with Executive Order 13960. Exec. Order No. 13960, § 3(a)-(i), 85 Fed. Reg. 78,939 (Dec 3, 2022).

Clearview AI.[52] In particular, the AI Ethics Council Intake Questionnaire—used by the Council to help it holistically evaluate an AI use case against ethical principles—notes that these staff must receive training to ensure they understand how to use AI systems, like facial recognition services, and the limitations of such systems. In response to this questionnaire, FBI program officials reported that staff in this one unit take the agency's *Face Comparison and Identification Training* course, in addition to training provided by the service. Additionally, the initial privacy review, completed by program officials and submitted to FBI's Privacy and Civil Liberties Unit, similarly states that training is required for staff in this one unit using Clearview AI. However, FBI communicated to staff in this unit that training to use Clearview AI is a best practice, rather than a requirement. Additionally, FBI officials told us that the agency did not have a training requirement for any staff using any facial recognition service.

Standards for Internal Control in the Federal Government states that agencies should internally communicate the necessary quality information to achieve its objectives.[53] The AI Ethics Council found one unit's use of Clearview AI to be ethical in part based on documentation that staff in this unit were required to take training to use the service, when no such requirement exists. Similarly, the Privacy and Civil Liberties Unit approved an initial privacy review for Clearview AI that erroneously stated that training requirements were in place. However, as of April 2023, FBI officials had not provided clear documentation to these key internal stakeholders on the status of the training requirement. By clarifying the status of the agency's training requirement for staff using Clearview AI to the AI Ethics Council and the Privacy and Civil Liberties Unit, the FBI would allow these stakeholders to fully evaluate whether the use of this service complies with FBI ethical and privacy standards.

FBI officials recommended training as a best practice for staff in one unit of the FBI; however, multiple units used facial recognition services without either a requirement or recommendation of training. As we discussed earlier, according to records we analyzed, only 10 of 196 staff from

[52] FBI officials told us that this documentation only relates to staff in one operational unit of the FBI. However, we found that staff on other FBI units used the service, which we discuss later in this section.

[53] GAO-14-704G.

across FBI who accessed Clearview AI had completed training.[54] Further, we found that the 186 untrained staff included staff in the FBI unit where training was recommended as well as other FBI units.

FBI officials told us that training would be beneficial for staff and that they intend to make training a requirement for all staff using facial recognition services. However, FBI staff have used facial recognition services included in our review since 2018 and have conducted tens of thousands of searches. In addition, staff continue to use the services without a training requirement in place. *Standards for Internal Control in the Federal Government* state that management should design control activities to achieve objectives and respond to risks.[55] Implementing a training requirement for staff using facial recognition services could help prevent potential abuses and increase the public's confidence in the agency's use of the technology. Additionally, doing so would help ensure that all staff that use these services understand how to use facial recognition services and their limitations.

CBP Has Not Assessed Whether Staff Would Benefit from Training for Facial Recognition Services

CBP provides staff access to two facial recognition services—IntelCenter and Marinus Analytics. However, CBP does not require staff to complete training on facial recognition technology to access these services, does not know the extent staff use such services for facial recognition searches, or whether training on facial recognition would benefit staff.

CBP officials told us they do not require staff to complete facial recognition training as a condition of receiving access to IntelCenter or Marinus Analytics, because they believe that staff rarely use the facial recognition capabilities of either service. Instead, agency officials stated that staff predominantly use other aspects of these services. For example, officials said staff mainly use IntelCenter for the news alerts,

[54] We obtained and analyzed available data on training and FBI Clearview AI accounts to determine the number of trained and untrained staff. Specifically, we reviewed training records for each staff person that completed facial recognition training, and compared that to a list of staff that accessed the facial recognition service. We considered staff trained if they accessed the service and completed the training, and untrained if they accessed the service but did not complete training at all. Further details on our analysis are in Appendix I. FBI officials stated that since we conducted our analysis, additional FBI users of the service had completed training.

[55] GAO-14-704G.

and mainly use Marinus Analytics for its feature that aggregates online advertisements to help CBP gather information on certain criminal investigations. However, CBP officials also acknowledged that staff use the facial recognition capabilities of the services to develop and share information in support of other agencies' criminal investigations. For example, CBP used the facial recognition capability of IntelCenter as part of a joint federal law enforcement task force.

Additionally, the agency does not have information on the number of staff that used the facial recognition capabilities available in either service, or how many facial recognition searches staff conducted from October 2019 through March 2022.[56] According to officials, neither the agency nor the services tracked this information. As a result, CBP could not determine the extent that staff used these facial recognition services.[57]

Although there is no specific training required for staff to access either service, CBP told us it requires all staff throughout the agency to complete certain training courses that could benefit users of facial recognition services. For example, CBP requires all staff to complete courses on protecting personal information and records management.[58] Further, CBP officials told us that staff could have taken face comparison training as part of their general training upon entering the agency. CBP officials also told us it has optional training resources available to staff with accounts.[59] However, CBP officials told us the agency has not assessed whether staff have the appropriate skills and competencies to use facial recognition services, and whether they would benefit from training beyond the general training required for all CBP staff.

According to our human capital guidance, agencies should assess the skills and competencies a workforce needs to address agency objectives,

[56] Representatives from both services told us that developing a feature to allow agencies to monitor how many staff use the facial recognition capability would be possible.

[57] In addition, we confirmed with representatives from each service that they could not provide this information either.

[58] CBP officials stated that some staff must also take agency training on integrity awareness and ethics. Further, CBP officials stated that staff could have taken training specific to use of other services, and a three-hour photo comparison training.

[59] For example, Marinus Analytics provides trainings to assist with law enforcement investigations on human trafficking using information from adult services websites, among other topics. Additionally, according to company representatives from IntelCenter, they offer training to help users understand its facial recognition capability, but do not require it.

and identify gaps in those skills and competencies, including gaps that training and development strategies can help address.[60] This guidance further notes that valid and reliable data are the starting point for such assessments. Similarly, *Standards for Internal Control in the Federal Government* states that management should ensure that information it uses to achieve its objectives is appropriate, current, complete, and accurate.[61]

Assessing whether training would benefit staff using facial recognition services to develop and share information in support of other agencies' criminal investigations could help CBP obtain assurance that its staff have the skills and competencies to address agency objectives. In addition, CBP could better support such an assessment by determining the extent to which staff use facial recognition services to develop and share information in support of other agencies' criminal investigations (such as number of CBP staff that use the services, and how often they do so).

Three of Seven Agencies Took Some Steps to Address Selected Privacy Requirements

We found that three of the seven agencies in our review addressed some privacy requirements related to facial recognition services, which helped them identify privacy risks and develop related mitigation strategies. However, we also found several instances where these agencies did not address privacy requirements. For example, two of these agencies did not complete privacy impact assessments for facial recognition services they used, or only completed them after years' of using the service. Additionally the remaining four agencies did not fully address any privacy requirements. In addition, we found that most agencies had yet to make determinations about whether certain privacy requirements apply to their use of a facial recognition service.

As discussed earlier, DHS and DOJ have requirements generally applicable to the use of facial recognition services to help prevent the inappropriate collection, use, and release of PII including: (1) conducting an initial privacy review prior to acquiring the service; (2) conducting a

[60] GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004).

[61] GAO-14-704G.

privacy impact assessment (PIA) prior to acquiring the service; (3) assessing privacy needs prior to acquisition; and (4) overseeing privacy controls for contractor access to PII. We reviewed the extent to which the seven agencies followed these four privacy requirements before sending photos of individuals to facial recognition services.[62] Figure 7 (below) and appendix II provide a detailed summary of the extent to which agencies addressed these four privacy requirements.

[62] Our review focused on the facial recognition services used by the seven agencies from October 1, 2019 through March 31, 2022. As discussed previously, both DHS and DOJ guidance identify photos of people as PII, potentially subject to privacy requirements. In addition, not all listed privacy requirements may apply to an agency's use of a facial recognition service. For example, an agency may conclude in its initial privacy review that a privacy impact assessment is not required.

Figure 7: Extent to which Selected Agencies Addressed Selected Privacy Requirements while Using Facial Recognition Services, as of April 2023

	Selected privacy requirement			
	Conduct initial privacy review	Conduct privacy impact assessment	Assess privacy needs prior to acquisition	Oversee privacy controls for contractor access to personally identifiable information
U.S. Customs and Border Protection Provider: IntelCenter	🟩	🟩	□	▨
U.S. Customs and Border Protection Provider: Marinus Analytics	🟩	□	🟩	□
Homeland Security Investigations Provider: Clearview AI	🟩	🟩	🟩	□
U.S. Secret Service Provider: Clearview AI	□	▨	▨	▨
Bureau of Alcohol, Tobacco, Firearms and Explosives Provider: Clearview AI	□	▨	▨	▨
Drug Enforcement Administration Provider: Clearview AI	□	▨	▨	▨
Federal Bureau of Investigation Provider: Clearview AI	🟩	□	▨	▨
Federal Bureau of Investigation Provider: Marinus Analytics	🟩	□	▨	▨
Federal Bureau of Investigation Provider: Thorn	□	▨	▨	▨
U.S. Marshals Service Provider: Clearview AI	□	▨	▨	▨

🟦 Agency addressed requirement

🟩 Agency addressed requirement, but not fully

▨ Agency did not determine whether requirement applied

□ Agency did not address requirement

Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

Data for Figure 7: Extent to which Selected Agencies Addressed Selected Privacy Requirements while Using Facial Recognition Services, as of April 2023

	Selected privacy requirement			
	Conduct initial privacy review	**Conduct privacy impact assessment**	**Assess privacy needs prior to acquisition**	**Oversee privacy controls for contractor access to personally identifiable information**
U.S. Customs and Border Protection **Provider: IntelCenter**	Agency addressed requirement, but not fully	Agency addressed requirement, but not fully	Agency did not address requirement	Agency did not determine whether requirement applied
U.S. Customs and Border Protection **Provider: Marinus Analytics**	Agency addressed requirement, but not fully	Agency did not address requirement	Agency addressed requirement, but not fully	Agency did not address requirement
Homeland Security Investigations **Provider: Clearview AI**	Agency addressed requirement, but not fully	Agency addressed requirement, but not fully	Agency addressed requirement, but not fully	Agency did not address requirement
U.S. Secret Service **Provider: Clearview AI**	Agency did not address requirement	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied
Bureau of Alcohol, Tobacco, Firearms and Explosives **Provider: Clearview AI**	Agency did not address requirement	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied
Drug Enforcement Administration **Provider: Clearview AI**	Agency did not address requirement	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied
Federal Bureau of Investigation **Provider: Clearview AI**	Agency addressed requirement, but not fully	Agency did not address requirement	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied
Federal Bureau of Investigation **Provider: Marinus Analytics**	Agency addressed requirement, but not fully	Agency did not address requirement	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied
Federal Bureau of Investigation **Provider: Thorn**	Agency did not address requirement	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied
U.S. Marshals Service **Provider: Clearview AI**	Agency did not address requirement	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied	Agency did not determine whether requirement applied

Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

Note: For each agency, we reviewed the use of facial recognition services from October 2019 through March 2022. In addition, we determined the extent to which these agencies had addressed the four selected requirements as of April 2023. We considered an agency to have completed a selected privacy requirement if it completed the requirement in accordance with departmental policy. We were unable to evaluate the extent to which agencies executed certain privacy requirements if the agency had not yet determined whether such requirements applied when we conducted our audit work.

Appendix I provides more information on how we evaluated privacy requirements and appendix II provides additional information on whether each agency met the four selected privacy requirements.

As shown in the figure above, three of the seven agencies in our review—CBP, HSI, and FBI—undertook efforts to address some of the requirements we reviewed. Specifically, CBP and HSI each completed an initial privacy review and associated PIA for facial recognition services they used. In addition, FBI finalized initial privacy reviews for two services it uses. By carrying out these activities, these agencies identified some privacy risks, and developed mitigation strategies to address those risks. For example, in its PIA, HSI identified as a potential privacy risk that HSI staff may submit probe photos to a facial recognition service that are not directly relevant to an ongoing criminal case.[63] HSI identified a mitigation strategy that included training HSI staff on the appropriate uses of the technology, requiring staff to document the source of probe photos and the use of facial recognition services in investigative case files, and requiring supervisory review of investigative case files.

In addition, the remaining four agencies in our review—ATF, DEA, the Marshals Service and the Secret Service—did not address the requirement to conduct an initial privacy review and did not determine the applicability of other privacy requirements we reviewed.

As shown in figure 7 above, we found that agencies:

- **Did not address a requirement.** None of seven agencies in our review completed all privacy requirements. For example, both CBP and FBI have determined a need for a PIA for facial recognition services they used; but, despite years of using these services, neither agency had completed the PIAs as of April 2023.
- **Did not determine the applicability of a requirement.** Six agencies—all but HSI—did not determine whether certain privacy requirements applied to their use of facial recognition services. For example, five of the six agencies did not complete initial privacy reviews for services they used—reviews intended to assess whether additional privacy requirements are applicable to the agency's use of a service. Without completing these reviews, the agencies were unable to determine the applicability of the remaining privacy requirements.
- **Addressed a requirement, but not fully or in a timely manner.** Three agencies took actions toward addressing a requirement (CBP, HSI, and FBI); however, we found that the agencies did not address

[63] U.S. Immigration and Customs Enforcement, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services (DHS/ICE/PIA- 054)*, (Washington, D.C.: May 13, 2020).

these requirements in accordance with departmental policy and guidance. For example, CBP completed the initial privacy review for IntelCenter's services prior to use, in accordance with DHS policy, but did not include a discussion of the service's facial recognition capabilities. Additionally, the initial privacy review indicated that CBP would only download IntelCenter data but we confirmed with both CBP officials and IntelCenter representatives that users must upload photos of individuals to the service to use the facial recognition capabilities. In addition, DHS and DOJ guidance calls for agencies to complete initial privacy reviews and PIAs prior to acquiring and using services that handle PII. We found that only CBP completed these reviews prior to acquiring and using one of its two facial recognition services. HSI and FBI addressed some privacy requirements for certain services they used, but addressed these requirements after they had already begun to use the services.

The four DHS and DOJ agencies that continued to use facial recognition services as of April 2023, had begun to take some, but not all, of the necessary steps to address outstanding privacy requirements. For example, according to CBP officials, CBP intends to publish the Marinus Analytics' PIA before the end of fiscal year 2023. In addition, FBI officials told us that they submitted a PIA for the services it uses to DOJ's Chief Privacy and Civil Liberties Officer for final approval in April 2023. Additionally, the three agencies that used free trials of facial recognition services—ATF, DEA, and the Secret Service—told us they have all taken actions to prohibit staff use of free trials, and had halted their use of these services as of April 2023.

Across the seven agencies we reviewed, program officials told us they did not fully address the privacy requirements, in part, because they (1) did not initially recognize the photos used as PII, (2) did not realize staff transmitted photos to facial recognition services, or (3) did not fully coordinate with privacy officials while acquiring these services. For example, CBP program officials stated they did not consider transmitted photos to facial recognition service providers as PII. ATF headquarters officials stated they were initially unaware ATF staff sent photos to Clearview AI. Additionally, HSI acquisition officials did not incorporate privacy officials' perspectives when making acquisition decisions with potential privacy implications. Privacy officials we met with stated that they were unaware that some privacy compliance documentation was not fully complete, and stated that they relied on program officials to understand the extent to which PII is used in facial recognition services.

Multiple agency and department offices share the responsibility for ensuring agencies address privacy requirements. For example, program officials are to notify privacy officials when they seek to procure potentially privacy-sensitive technology and work with them to complete initial privacy reviews and privacy impact assessments. Acquisition officials are to coordinate with privacy officials to ensure that required privacy terms are included in contracts, and ultimately implemented. In addition, DHS and DOJ each have department officials responsible for helping their respective agencies and staff comply with laws and policies for protecting privacy, including the requirements we reviewed. Further, DHS and DOJ guidance states that program, privacy, and acquisition officials should coordinate prior to using privacy sensitive technology.[64] DHS and DOJ officials also emphasized that program officials should coordinate with relevant offices on privacy concerns, even when it may not be initially clear whether PII is directly involved.

Standards for Internal Control in the Federal Government state that management should evaluate and remediate deficiencies.[65] While most of the agencies continuing to use facial recognition services have begun to take steps to address the outstanding privacy requirements we identified in Figure 7, many of these efforts are incomplete. Additionally, agencies have not updated privacy documentation (initial privacy reviews, privacy impact assessments) that do not include full or correct information on the extent to which contractors may have access to PII. At a broader level, DHS and DOJ privacy offices have yet to work with other relevant offices (e.g., acquisition offices) to determine why agencies did not adhere to their respective privacy compliance processes for facial recognition services.[66]

Both DOJ and DHS have noted the importance of adhering to privacy requirements. For example, DOJ has noted that timely completion of privacy impact assessments ensures that privacy protections are built into systems from the start, and not after the fact when they could be far more

[64] Department of Homeland Security, *Privacy Impact Assessment: The Privacy Office Official Guidance* (Washington, D.C.: June 2010). Department of Justice, Office of Privacy and Civil Liberties, *Initial Privacy Assessment Instructions and Template* (Washington, D.C.: Revised May 2022).

[65] GAO-14-704G.

[66] Appendix II provides detailed information of the extent to which each of the seven agencies included in our review addressed selected privacy requirements.

costly or affect the viability of the project.[67] Further, DOJ noted that timely completion of these assessments help promote trust between the public and the federal government by increasing transparency of the department's systems and missions. More broadly, DHS has noted that as stewards of data on the citizens it serves it must strive to ensure privacy protection and awareness remain fundamental to its operations.[68]

By taking actions to ensure that agencies continuing to use facial recognition services address outstanding privacy requirements for facial recognition services, and updating existing privacy documentation as appropriate, DHS and DOJ can better ensure that PII shared with facial recognition services (such as probe photos), are not inappropriately disclosed or compromised. Further, DHS and DOJ Privacy Officers could help ensure agencies better comply with privacy requirements in the future by collaborating with agency program, acquisition, and privacy officials to evaluate why agencies did not adhere to their respective privacy compliance processes for facial recognition services—taking into account the results in this report. Conducting such an evaluation and remediating any deficiencies identified through the process could help DHS and DOJ increase transparency of the departments' use of facial recognition services.

Most Agencies Did Not Have Policies Specific to Facial Recognition to Help Protect Civil Rights and Civil Liberties

Of the seven agencies in our review, three had policies specific to facial recognition technology intended to help protect civil liberties and civil rights, and four did not. In addition, DHS has plans to issue new department-wide guidance that, according to the department, will help ensure the protection of civil rights and civil liberties while staff use facial recognition technology. Finally, DOJ officials told us that they also intend to issue a department-wide policy, and have taken steps to do so. However, DOJ has also faced delays in its efforts, and officials told us

[67] Department of Justice, Office of Privacy and Civil Liberties, *Privacy Impact Assessments:* Official *Guidance,* (Washington, D.C.: Revised July 2015).

[68] Department of Homeland Security, Privacy Impact Assessments: The Privacy Office Official Guidance, (Washington, D.C.: June 2010).

they did not have a plan with time frames and milestones to issue such a policy.

Officials with HSI, the Marshals Service, and the Secret Service all identified policies or guidance that helped staff ensure the protection of certain civil rights and civil liberties. HSI's policy, first established in January 2021, includes requirements such as limiting the use of such technology to certain criminal investigations.[69] Specifically, this memorandum states that HSI will use a facial recognition service only for authorized law enforcement purposes relevant and necessary to an ongoing investigation relating to HSI's statutory authorities; or as part of an established HSI program or task force whose use of facial recognition is assessed for its impacts on privacy, civil rights, and civil liberties. Additionally, HSI's policy places explicit limits on the collection of probe photos taken while individuals are exercising their First Amendment rights (such as at protests), among other things.

In addition, the Marshals Service has guidance to staff that limits the use of facial recognition technology to ongoing criminal investigations. For example, the Marshals Service guidance states that all searches conducted in Clearview AI must have a direct nexus to an active fugitive investigation or other authorized criminal investigation, and that possible matches will require further research and investigation.

Finally, the Secret Service had halted its use of facial recognition services in April 2020. However, in April 2023 the Secret Service issued a directive which provides general guidance on using facial recognition services. For example, the directive limits the use of facial recognition services to subjects and victims in established Secret Service investigations under laws the Secret Service has the authority to enforce. In addition, this policy only permits the use of facial recognition services that are pre-approved by the agency's Criminal Investigative Division.

The remaining four agencies (FBI, CBP, ATF, and DEA) did not have guidance or policies specific to facial recognition technology that addressed civil rights and civil liberties. However, officials with FBI and CBP told us staff must abide by more general guidance that helps ensure the protection of civil rights and civil liberties during investigatory activities, including when using facial recognition technology. For

[69] U.S. Immigration and Customs Enforcement, Acting Executive Associate Director, *Use of and Access to Third-Party Facial Recognition Services,* Memorandum to All Homeland Security Investigations Personnel (Washington, D.C.: January 15, 2021).

example, FBI officials noted that the Attorney General's Guidelines for Domestic FBI Operations and the FBI's Domestic Investigations and Operations Guidelines provide overarching guidance for all FBI activities, including addressing civil rights and civil liberties during investigatory activities.[70] Additionally, CBP officials identified a DHS memorandum on protecting First Amendment rights as a source of guidance for staff using facial recognition technology.[71] Among other things, this memorandum notes that DHS personnel are only permitted to collect, maintain, or use information protected by the First Amendment in certain circumstances.[72]

ATF and DEA had halted their use of facial recognition services at the time of our review. However, these officials noted the agency has general departmental and agency guidance to help ensure the protection of civil rights and civil liberties applicable to all criminal investigatory activities.[73]

Additionally, DHS officials reported that beginning in May 2022, the DHS Chief Information Officer initiated a working group to develop a department-wide policy to establish responsibilities and requirements for the authorized, responsible, and ethical use of face recognition technology, including protections for individual rights. For example, DHS officials told us that they anticipated the policy would (1) address safeguarding privacy, civil rights, civil liberties, (2) identify authorized uses of facial recognition technology, and (3) provide guidelines to help ensure individuals are not targeted based on protected characteristics or protected activities (e.g., First Amendment activities). In May 2023, DHS officials provided us a project plan highlighting anticipated milestones to

[70] Additionally, FBI officials noted that one unit in the FBI had identified best practices for their staff to use one facial recognition service, which included practices to help protect civil rights. FBI officials also told us they were working on developing agency-wide policy specific to the use of facial recognition technology.

[71] Department of Homeland Security, Acting Secretary, *Information Regarding First Amendment* Protected *Activities,* (Washington, D.C.: May 17, 2019).

[72] In particular, this memorandum notes that DHS personnel are not permitted to collect, maintain, or use information protected by the First Amendment unless (1) an individual has expressly granted their consent for DHS to collect, maintain, and use that information; (2) maintaining such information is expressly authorized by a federal statute or (3) the information is relevant to a criminal, civil, or administrative activity relating to a law DHS enforces or administers.

[73] Because our review focused on the extent to which agencies had developed policies and guidance specific to facial recognition technology to help protect civil liberties and civil rights, we did not evaluate general guidance agencies have to protect civil rights and civil liberties.

finalize the policy, including that they anticipated issuing this policy by June 2023. In August 2023, DHS officials stated that DHS Office of General Counsel was reviewing the policy but that they expected the policy to be completed by the end of December 2023. It will be important that DHS has focused attention on completing and implementing the policy by the newly established timeframe.

DOJ has also begun to develop a department-wide facial recognition policy addressing civil rights and civil liberties. In February 2022, DOJ formed a working group charged with determining a need for, and developing, policy on law enforcement's use of facial recognition technology.[74] DOJ officials stated that this working group was drafting a department-wide facial recognition policy that would include safeguards for civil rights and civil liberties. Officials also stated that they intended to use this policy to address the related congressional report from March 2022.[75] DOJ officials told us that they did not have a project plan with time frames and milestones for issuing this policy. Previously, in November 2022, they stated they expected to implement the policy in the following months, and in March 2023, DOJ officials stated they expected to finalize the policy shortly.

In April 2023, DOJ officials told us that although they had developed a draft policy, they had changed course, and intended to wait for the study and interagency effort required by Executive Order 14074 to complete before issuing the policy.[76] As discussed earlier, Executive Order 14074, issued in May 2022, directed DOJ to contract with the National Academy of Sciences to study facial recognition technology and assess related privacy, civil rights, and civil liberties concerns. Additionally, the executive order calls for DOJ and others to lead an interagency effort to identify best practices for using facial recognition technology, and describe any resulting policy changes for federal law enforcement.

DOJ officials stated that they have begun to take some steps to address the facial recognition directives found in Executive Order 14074. For

[74] DOJ officials also said the department formed the working group in part due to our reports since 2016 that have highlighted potential risks and benefits of facial recognition technology.

[75] See H.R. No. 117-97 (2021) (accompanying Pub. L. No. 117-103, 136 Stat. 49 (2022) and incorporated by reference in the explanatory statement for the Act, 168 Cong. Rec. H1772 (2022)). As previously discussed, Congress directed DOJ to develop ethical policies for the use of facial recognition technology.

[76] Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

example, DOJ officials told us that representatives from DOJ, DHS, the White House's Domestic Policy Council, and the Office of Science and Technology Policy held three meetings from October 2022 through February 2023 to address the executive order requirements.

However, some efforts called for in the executive order have been delayed. DOJ officials told us that they had identified funding to address the requirement to develop a study on facial recognition technology, but had not yet awarded the funding to the National Academy of Sciences.[77] The executive order called on DOJ to enter into the contract by November 2022, and it had not done so as of April 2023. Additionally, the executive order called on the interagency effort to issue a report—using the results of the National Academy of Sciences study—by November 2023. However, as of April 2023, the funding for the study had not yet been awarded, the study had not yet begun, and it is unclear what impact this may have on DOJ's ability to issue their facial recognition policy in a timely manner.

Leading project management practices include that organizations direct and manage project work by developing a project management plan and a project schedule, which notes work activities, their durations, resources, and planned start and finish dates.[78]

DOJ officials have stated that they intend to wait for the completion of the study and interagency effort before issuing department policy on facial recognition technology, which will allow them to leverage information gained during that process. However, without a department-wide facial recognition policy, we found that selected DOJ law enforcement agencies continued to use facial recognition technology. DOJ also lacks an implementation plan to ensure it issues its policy upon completion of the Executive Order activities, and has faced delays in those activities.

DOJ officials stated that the department has existing general guidance and policies that apply to the use of facial recognition technology; however, there may also be unique issues raised by the technology that DOJ has not yet addressed through existing policy. For example, in

[77] Specifically, DOJ stated that the department would fund the study through a grant from the National Institute of Justice's fiscal year 2023 appropriations. As of April 2023, the National Institute of Justice was undertaking administrative tasks prior to awarding funding for the study.

[78] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition* (2017).

September 2022, DOJ officials told us that they were considering including in their policy guidance on whether a potential match result from a facial recognition system alone would constitute sufficient basis to apply for a search warrant.

Leveraging information gained through the interagency process may help DOJ improve policy on how to safeguard civil rights and civil liberties while using facial recognition technology. However, given uncertainties about when this process will complete, DOJ risks a delay in meeting its own goal of providing a policy to law enforcement on the use of facial recognition technology—a goal that predates the actions required by Executive Order 14074. Developing a plan with time frames and milestones would better position DOJ to issue its policy in a more timely manner upon completion of the executive order activities, thereby supporting staff in safeguarding civil rights and civil liberties while using facial recognition technology.

Conclusions

Facial recognition services offered by commercial and nonprofit entities are tools that DHS and DOJ used to support criminal investigations. While these services may support such investigations, federal government officials and others have also emphasized the importance of training to help prevent potential abuses and increase the public's confidence in the technology. While some agencies have developed training requirements, we found that HSI, FBI, and CBP could take additional steps to help ensure that staff are sufficiently trained.

HSI has a process to ensure staff take required training, but our analysis found that some staff did not complete these requirements. HSI has taken the positive step of undertaking a one-time review of staff adherence to training requirements. However, without establishing and implementing a process to periodically monitor whether staff using facial recognition services complete training requirements, HSI faces a continued risk that untrained staff may use facial recognition services.

The FBI does not require any staff to take training to use facial recognition services, but told key internal stakeholders that training is required for certain staff. Clarifying the status of its training requirement for staff using Clearview AI to the AI Ethics Council and the Privacy and Civil Liberties Unit would better enable the FBI to fully evaluate whether the use of these services follows FBI ethical and privacy standards. In addition, FBI officials said they intend to make training a requirement for all staff using facial recognition services, but have not yet done so. Implementing a training requirement for all staff using facial recognition services to support criminal investigations would better position FBI to help ensure staff understand how to use these services and their limitations.

CBP provides staff access to facial recognition services but does not have information on the number of staff that use the facial recognition services or how often. Further, CBP has not assessed whether staff using facial recognition services to develop and share information in support of other agencies' criminal investigations could benefit from training on facial recognition technology. Such an assessment can help provide CBP assurance that staff have skills and competencies needed to address agency objectives. In addition, determining the extent that staff use facial recognition services to develop and share information in support of other agencies' criminal investigations would provide key information to help CBP conduct the assessment.

All seven agencies in our review sent photos to facial recognition services without fully addressing privacy requirements. Addressing the outstanding privacy requirements identified in this report, and updating existing privacy documentation, would better enable DHS and DOJ to determine whether appropriate privacy safeguards are in place for agencies that continue to use facial recognition services. Further, ensuring privacy, program, and acquisition officials collaborate on an evaluation of components' adherence to the department's privacy compliance process for facial recognition services could help ensure DHS and DOJ better address privacy requirements in the future, thereby increasing transparency in the departments' use of facial recognition services.

Finally, DOJ has taken steps to develop a department-wide facial recognition policy that includes a focus on civil rights and civil liberties, but has not issued it, and some DOJ law enforcement agencies continue to use this technology without specific guidance. DOJ lacks a plan with time frames and milestones for issuing its facial recognition technology policy. Developing such a plan would better position DOJ to safeguard civil rights and civil liberties while using facial recognition technology.

Recommendations for Executive Action

We are making a total of 10 recommendations, including one to ICE, two to FBI, two to CBP, three to DOJ, and two to DHS:

The Director of ICE should establish and implement a process to periodically monitor whether HSI staff using facial recognition services to support criminal investigations have completed training requirements. (Recommendation 1)

The Director of the FBI should clarify the status of its training requirement for staff using Clearview AI to FBI's AI Ethics Council and the Privacy and Civil Liberties Unit. (Recommendation 2)

The Director of the FBI should implement a training requirement for staff using facial recognition services to support criminal investigations. (Recommendation 3)

The Commissioner of CBP should determine the extent that staff use facial recognition services to develop and share information in support of other agencies' criminal investigations (such as number of CBP staff that use the services and how often they do so). (Recommendation 4)

The Commissioner of CBP should assess whether training would benefit staff using facial recognition services to develop and share information in support of other agencies' criminal investigations, incorporating information on the extent to which staff use such services. (Recommendation 5)

The Attorney General should ensure the Chief Privacy and Civil Liberties Officer works with DOJ components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate. (Recommendation 6)

The Attorney General should ensure the Chief Privacy and Civil Liberties Officer collaborates with component program, acquisition, and privacy officials to evaluate components' adherence to the department's privacy compliance process for facial recognition services—taking into account the results of this report—and to remediate any deficiencies identified during their evaluation. (Recommendation 7)

The Secretary of Homeland Security should ensure the Chief Privacy Officer works with DHS components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate. (Recommendation 8)

The Secretary of Homeland Security should ensure the Chief Privacy Officer collaborates with component program, acquisition, and privacy officials to evaluate components' adherence to the department's privacy compliance process for facial recognition services—taking into account the results of this report—and to remediate any deficiencies identified during their evaluation. (Recommendation 9)

The Attorney General should develop a plan with time frames and milestones for issuing its facial recognition technology policy that addresses safeguards for civil rights and civil liberties. (Recommendation 10)

Agency Comments and Our Evaluation

We provided a draft of this report to DOJ and DHS for review and comment. DOJ concurred with our recommendations and provided technical comments, which we incorporated as appropriate.

DHS provided formal, written comments, which are reproduced in appendix III. In its comments, DHS concurred with our recommendations and described actions taken and planned to address them. Additionally, DHS provided technical comments, which we incorporated as appropriate. In its technical comments, DHS pointed out that our draft recommendations 4 and 5 did not specify that the recommendations were about the extent that CBP staff use facial recognition services to develop and share information in support of other agencies' criminal investigations. We adjusted the language of these recommendations accordingly.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until one week from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Attorney General, and the Secretary of the Department of Homeland Security. In addition, this 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 IV.

Gretta L Goodwin

Gretta L. Goodwin
Director, Homeland Security and Justice

List of Requesters

The Honorable Richard J. Durbin,
Chair
Committee on the Judiciary
United States Senate

The Honorable Jerrold Nadler
Ranking Member
Committee on the Judiciary
House of Representatives

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
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 the extent to which selected Department of Homeland Security (DHS) and Department of Justice (DOJ) law enforcement agencies have:

(1) used facial recognition services to support criminal investigations from October 2019 through March 2022;

(2) required staff to take training on facial recognition technology to use such services, and ensured compliance with requirements;

(3) taken steps to address selected privacy requirements for using facial recognition services; and,

(4) developed policies and guidance specific to facial recognition technology to help protect civil liberties and civil rights.

To address all four objectives, we selected seven agencies within DHS and DOJ that employ law enforcement officers (i.e., law enforcement agencies).[1] We limited our selection to DHS and DOJ agencies because these two departments employ the highest number of law enforcement officers within the federal government, and cumulatively employ more than 80 percent of all federal law enforcement officers.[2] From there, we identified DHS and DOJ law enforcement agencies that previously reported owning or using facial recognition technology systems in 2020.[3]

We selected seven agencies that reported owning or using the highest number of systems to include in this review. Within DHS, we selected U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), and the U.S. Secret Service. Within the DOJ, we selected the Bureau of

[1] Consistent with our prior work, we define federal law enforcement officers as full-time employees with federal arrest authority who are authorized to carry firearms while on duty.

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

[3] GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* GAO-21-518 (Washington, D.C.: June 2021).

Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the U.S. Marshals Service. The seven law enforcement agencies we selected are not representative of all law enforcement agencies.

Our review included agencies that used facial recognition services in support of criminal investigations, including sharing information (e.g., leads). For example, one agency—CBP—told us that it does not lead criminal investigations but has used facial recognition services to develop and share information in support of other agencies' criminal investigations.[4] We focused exclusively on the use of facial recognition technology services offered by commercial and nonprofit entities (facial recognition services) to build upon our prior reports that reviewed technologies owned and operated by federal agencies.[5]

To address our first objective, we reviewed agency documentation and interviewed agency officials to identify commercial and nonprofit facial recognition services that agencies used from October 2019 through March 2022 to support criminal investigations. We then obtained and analyzed available data to determine the total number of searches that agency staff conducted using these services from October 2019 through March 2022.

We selected this timeframe to overlap with our prior work, and extend to the most recent data available at the time of our analysis. We included reported searches conducted through March 31, 2022, as it was the most recent data available when we conducted our analysis. We previously reported on agencies' use of facial recognition technology from January 2015 through March 2020.[6] We assessed the reliability of these data by interviewing knowledgeable agency officials and representatives from each service that agencies reported using during this time period. In addition, we tested these data for outliers or obvious errors when

[4] CBP officials told us that the agency used facial recognition services primarily of immigration enforcement and border security purposes.

[5] See for example, GAO-21-518; GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies,*GAO-21-526 (Washington, D.C.: Aug. 2021); GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO-20-568 (Washington, D.C.: Sep 2020); and, GAO, *FACE Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* GAO-16-267 (Washington, D.C.: May 2016, reissued Aug. 2016).

[6] See GAO-21-518.

possible. The data on the number of searches agencies reported is an undercount. For example, the FBI could not fully account for searches it conducted using two services, Marinus Analytics and Thorn.[7] Additionally, CBP officials were unable to provide information on the number of searches staff conducted during this time because neither the agency nor the services tracked this information. Therefore, we determined that these data were sufficiently reliable for reporting on the minimum number of searches conducted by agencies during the period of our review.

To address our second objective, we reviewed agency documentation, including policies, guidance, and memorandums, to determine the extent to which agencies required staff to take training on facial recognition technology to use such services.[8] For agencies with training requirements, we interviewed relevant officials to learn more about the requirements, and how the agency ensures compliance with these requirements. In addition, for these agencies, we reviewed agency documentation such as memorandums of agency policy and training materials.[9] In addition, because FBI recommended training as a best practice for one unit in the agency, we also reviewed relevant FBI documents.[10]

[7] Specifically, neither the FBI nor Marinus Analytics tracked the number of searches staff conducted during this time. Additionally, Thorn, only tracked the last time the agency searched using a specific probe photo, and not each time the agency searched using that same probe photo.

[8] We assessed the extent to which agencies had implemented training specifically required for using facial recognition services, and did not assess requirements for more general training that agency staff may receive, such as general privacy training. We considered a training requirement to be written instruction to staff mandating training as a condition of access to a facial recognition service.

[9] U.S. Immigration and Customs Enforcement, Acting Executive Associate Director, *Use of and Access to Third-Party Facial Recognition Services* (Washington, D.C.: Jan. 15 2021); U.S. Immigration and Customs Enforcement, *Clearview AI Facial Recognition Tool Training* (Washington, D.C.: July 9 2021); U.S. Marshals Service, *Clearview AI Training Requirements* (Washington, D.C.: Feb. 6 2023). We did not evaluate the content of training to ascertain its sufficiency or appropriateness because there are no national training standards for facial recognition technology.

[10] Federal Bureau of Investigation, *Face Comparison and Identification Training* (Washington, D.C.: Revised Dec. 2020).

We then evaluated the extent agencies ensured compliance with requirements or recommended best practices.[11] Specifically, we compared training records maintained by the agency to a list of staff that used facial recognition services.[12] We considered staff trained if they completed all required or recommended training in place prior to conducting searches, and untrained if they had not completed all training requirements or recommended training prior to conducting searches. Due to limited data available for the FBI, we considered staff trained if they completed training and accessed the service, and untrained if they did not complete training but accessed the service.[13] We compared the agencies' efforts to ensure compliance with training requirements against agency policies requiring training and *Standards for Internal Control in the Federal Government*, including standards for designing and implementing controls activities, establishing and operating monitoring activities, and internally communicating quality information.[14]

If an agency did not require staff to take training but continued to use facial recognition services at the time of our review, we interviewed officials to understand the agency's rationale. We compared agencies' efforts against our human capital guidance and *Standards for Internal Control in the Federal Government*, including the standard for ensuring that information the agency uses to achieve its objectives is appropriate,

[11] One agency—the Marshals Service did not implement its training requirement until February 2023. Given the short amount of time that has passed since the agency implemented its requirements, we did not assess the agency's compliance process for this training requirement.

[12] To compare HSI training records to Clearview AI search records, we matched record-level training data (staff first and last names and email addresses) to record-level Clearview AI search records (staff first and last names, and each date they conducted a search in our time frame).

[13] To compare FBI training records to search records, we matched record-level training data as of September 30, 2022 (staff first and last names) to summary-level Clearview AI records of staff that accessed the service (staff first and last names) as of August 2022.

[14] Specifically, Principle 10 states that management should design control activities to achieve objectives and respond to risks. Principle 12 states that management should implement control activities through policies. Principle 14 states management should internally communicate the necessary quality information to achieve the entity's objectives. Principle 16 states that management should establish and operate monitoring activities to monitor the internal control system and evaluate results. GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

current, complete, and accurate.[15] In addition, we interviewed officials about their intention to implement a training requirement for all staff and compared agencies' efforts against *Standards for Internal Control in the Federal Government*, including the standard that management should design control activities to achieve objectives and respond to risks.[16] We did not assess training requirements for agencies that reported they were not using facial recognition services at the time we conducted our audit work.

For all of the data we used in this objective, we assessed the reliability of the data by interviewing knowledgeable agency officials and company representatives, reviewing existing information about the data systems, and testing these data for outliers or obvious errors. We determined that these data were sufficiently reliable for reporting on the number of trained and untrained staff using facial recognition services during the period of our review.

To address our third objective, we reviewed departmental privacy guidance and agency documentation, such as the DHS and DOJ guidance on implementing aspects of the E-Government Act of 2002.[17] We also reviewed DHS and DOJ acquisitions regulations and policies. Based on our review of these documents, we selected four privacy requirements generally applicable to systems and services that collect personally identifiable information (PII).[18] The four privacy requirements we selected include conducting an initial privacy review, conducting a

[15] GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004). Specifically, Principle 13 states that management should use quality information to achieve its objectives. GAO-14-704G.

[16] Specifically, Principle 10 states that management should design control activities to achieve objectives and respond to risks. GAO-14-704G.

[17] Department of Homeland Security, Privacy Office. *Privacy Impact Assessments: Privacy Office Official Guidance*. (Washington, D.C., June 2010). Department of Justice, Office of Privacy and Civil Liberties. *Privacy Impact Assessments: Official Guidance*. (Washington, D.C.: Revised July 2015). The E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921 (2002).

[18] The specific requirements applicable to DHS's and DOJ's use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. In addition, there may be other privacy requirements that apply to federal agencies' use of services that collect PII that we did not include in our review.

privacy impact assessment (PIA), assessing privacy needs prior to acquisition, and overseeing privacy controls for contractor access to PII.

We then determined whether agencies addressed the four selected privacy requirements for each facial recognition service used from October 2019 through March 2022. For each requirement, we gathered relevant agency documentation and compared them to agency guidance and policies. Specifically, we reviewed available initial privacy reviews, PIAs, privacy checklists for acquisition, and contract documentation.[19] We also interviewed cognizant agency officials and representatives from facial recognition services to understand the extent to which PII may be transmitted during a facial recognition search.

We considered an agency to have addressed the requirements if the agency completed initial privacy reviews and PIAs in a timely manner (e.g. prior to acquisition) and with correct information on data transmission, data retention, and training. If the agency addressed the requirement late or without full information, we determined that the agency did not fully address the requirement.

We considered an agency to have assessed privacy needs prior to acquisition as required if the agency completed required privacy checklists on time and with accurate information and if contract documentation, such as terms of agreements reflected privacy needs identified during the acquisition process. We considered an agency to have overseen privacy controls for contractor access to PII as required if the agency executed selected terms in contracts with facial recognition service providers.

If an agency did not address a requirement that would help them determine whether other privacy requirements applied, then we could not evaluate the extent to which the agency addressed the remaining requirements. If an agency did not address, or did not fully address privacy requirements, we interviewed agency officials to determine why. Finally, we compared this information to principles in the *Standards for*

[19] We also requested relevant documentation from agency officials illustrating the extent to which they executed selected privacy requirements in contracts, such as requiring contractor employees to sign non-disclosure agreements and implement training requirements.

Internal Control in the Federal Government that state that management should evaluate and remediate deficiencies on a timely basis.[20]

To address our fourth objective, we reviewed a congressional report and executive order related to policies for facial recognition technology.[21] We also interviewed agency officials and reviewed agency documentation to understand the extent to which agencies had existing policies and guidance that addressed civil rights and civil liberties in the context of facial recognition technology. Specifically, we asked agency officials to identify guidance, memorandums or policies that addressed civil rights and civil liberties in the context of facial recognition technology, or that applied to the use of facial recognition technology.[22]

We then interviewed department officials to understand their efforts to develop and implement new department-wide guidance related to civil rights and civil liberties specific to facial recognition technology, and to address the congressional report and executive order. We compared their efforts to leading project management practices.[23]

We conducted this performance audit from January 2022 to September 2023 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.

[20] Specifically, Principle 16 states that management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. Principle 17 states that management should remediate identified internal control deficiencies on a timely basis. GAO-14-704G.

[21] See H.R. No. 117-97 (2021) (accompanying Pub. L. No. 117-103, 136 Stat. 49 (2022)); Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

[22] We are defining “civil rights” as due process protections and personal rights protected by the U.S. Constitution and federal laws, such as the Civil Rights Act of 1964; and “civil liberties” as the exercise of activities protected under the First Amendment.

[23] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition* (2017). PMBOK is a trademark of Project Management Institute, Inc. The Project Management Institute is a not-for-profit association that, among other things, provides standards for managing various aspects of projects, programs, and portfolios.

Appendix II: Extent to Which Selected Federal Law Enforcement Agencies Took Steps to Address Selected Privacy Requirements

The seven federal law enforcement agencies in our review addressed four selected privacy requirements to varying extents while using facial recognition services.[1] This appendix details the extent to which each agency addressed the four selected privacy requirements.

As discussed earlier, when using facial recognition services, agencies may need to: conduct an initial privacy review; conduct a privacy impact assessment (PIA); assess privacy needs prior to acquisition; and oversee privacy controls for contractor access to personally identifiable information (PII). If an agency determined that a privacy requirement applied, we analyzed the extent to which the agency addressed the requirement. Our review included facial recognition services used between October 2019 and March 2022.

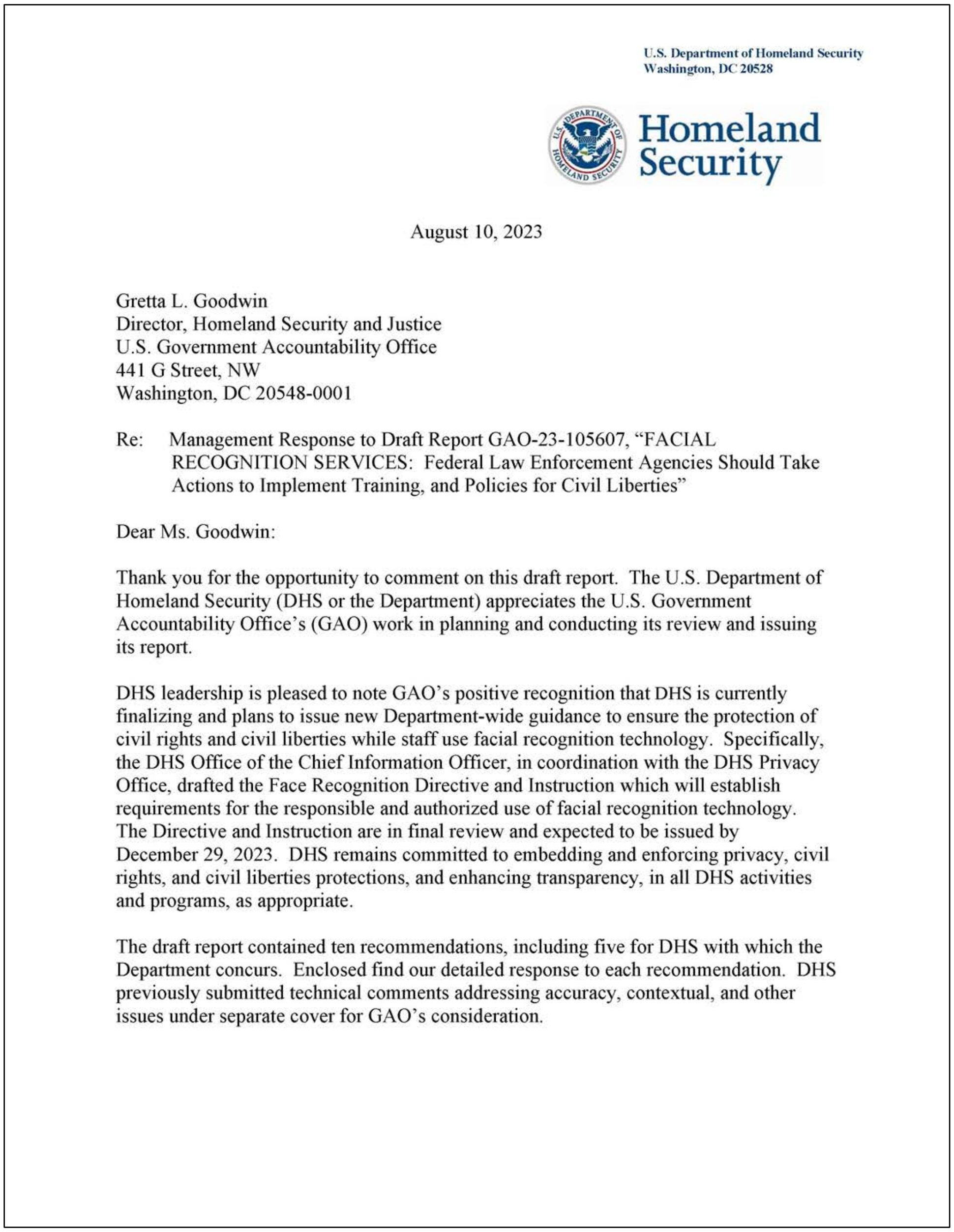
We evaluated the extent to which the agencies addressed these requirements on time (e.g., prior to using the service for criminal investigations). We also evaluated the extent to which agencies' privacy documentation included full and correct information on training requirements and whether PII is transmitted to, or retained by, contractors or contractor systems.

In some instances, an agency did not determine whether a requirement was applicable. For example, if an agency did not complete an initial privacy review, the agency could not determine whether it was required to complete a PIA. In instances where an agency did not determine the applicability of a requirement, we did not evaluate the extent to which the

[1] The agencies we evaluated are the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Customs and Border Protection (CBP), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), the U.S. Marshals Service, and the U.S. Secret Service.

agency addressed the requirement. Appendix I contains additional information on our methodology.

Appendix III: Comments from the Department of Homeland Security



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

Homeland
Security

August 10, 2023

Gretta L. Goodwin
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

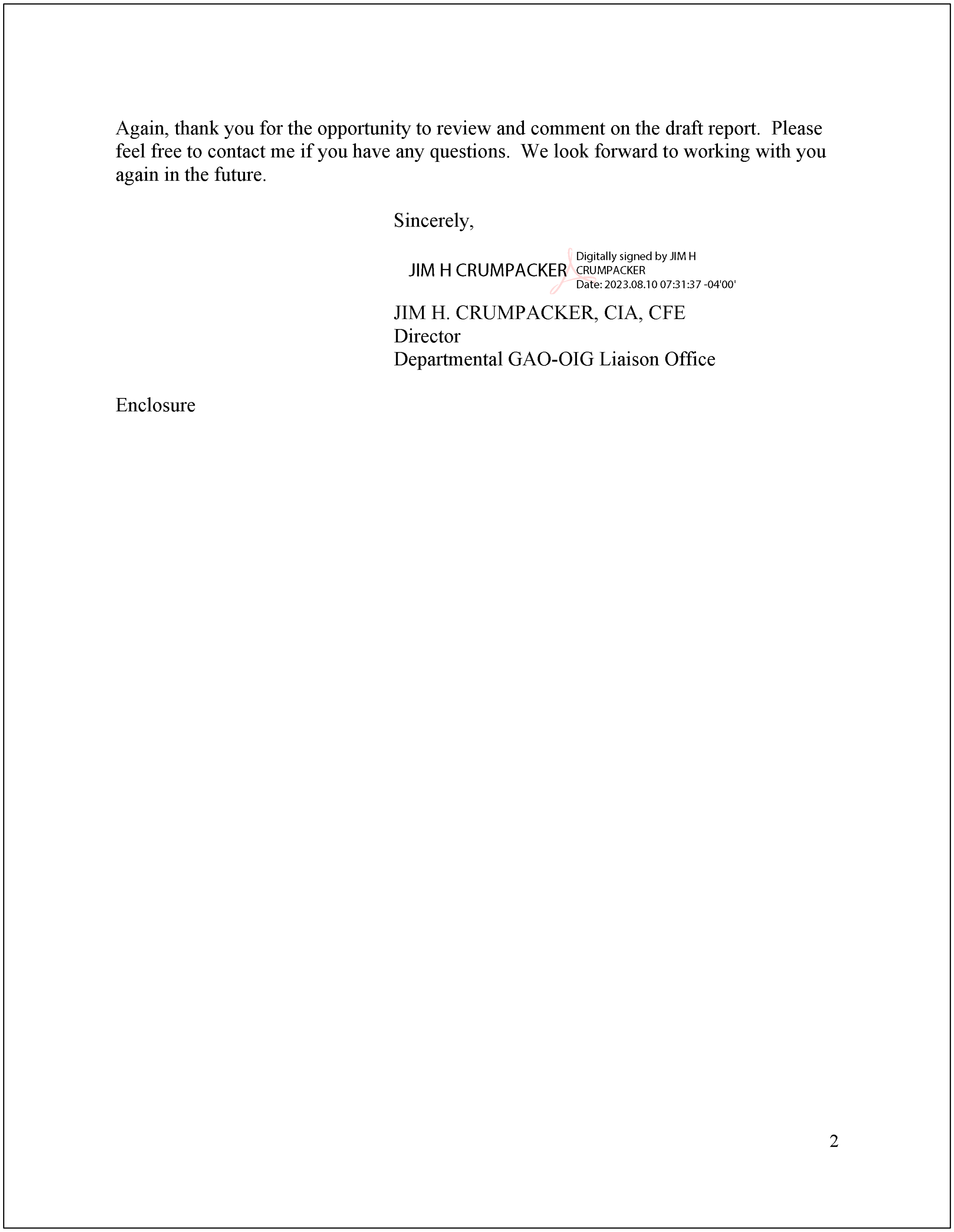
Re: Management Response to Draft Report GAO-23-105607, "FACIAL RECOGNITION SERVICES: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties"

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 its report.

DHS leadership is pleased to note GAO's positive recognition that DHS is currently finalizing and plans to issue new Department-wide guidance to ensure the protection of civil rights and civil liberties while staff use facial recognition technology. Specifically, the DHS Office of the Chief Information Officer, in coordination with the DHS Privacy Office, drafted the Face Recognition Directive and Instruction which will establish requirements for the responsible and authorized use of facial recognition technology. The Directive and Instruction are in final review and expected to be issued by December 29, 2023. DHS remains committed to embedding and enforcing privacy, civil rights, and civil liberties protections, and enhancing transparency, in all DHS activities and programs, as appropriate.

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



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

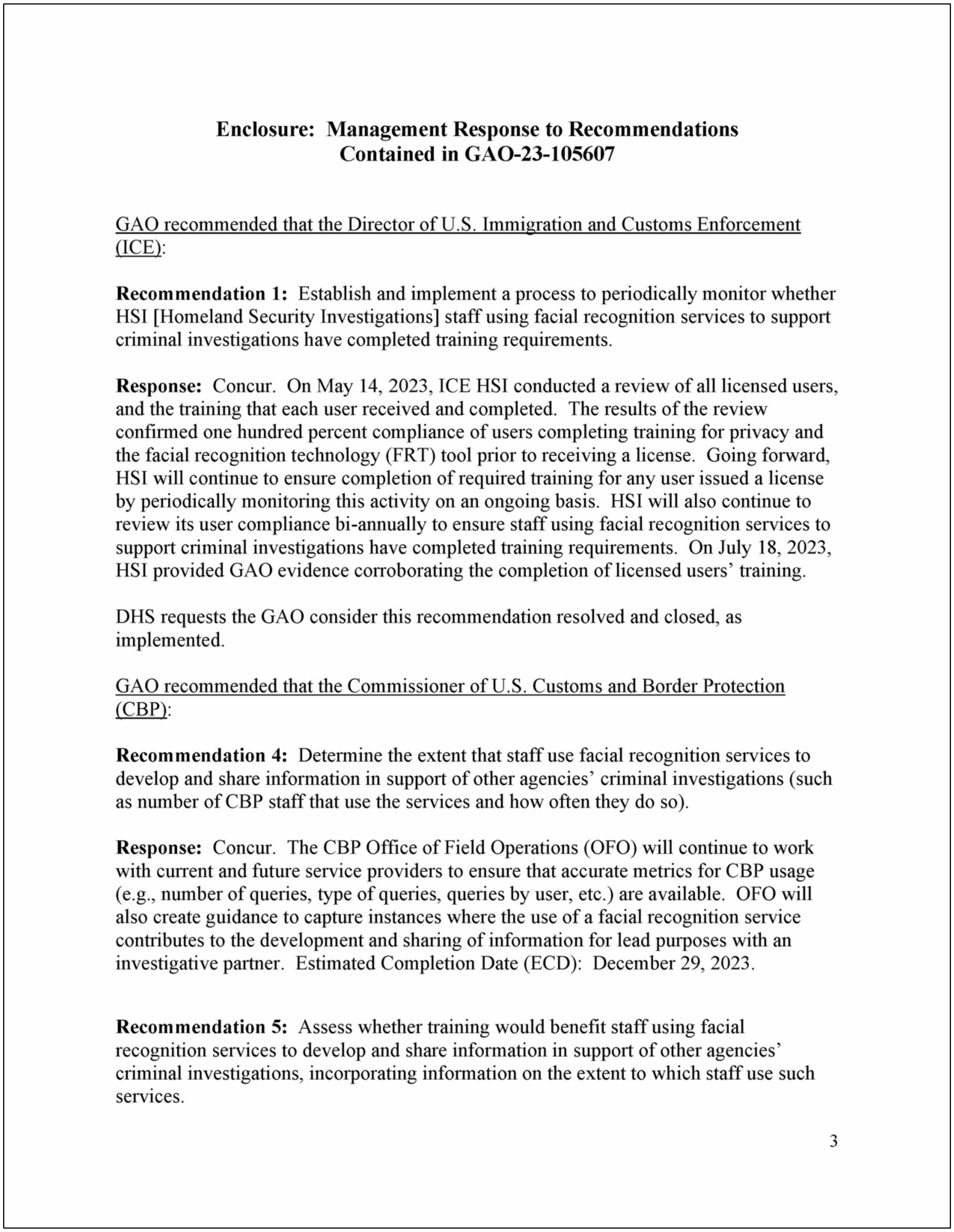
Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER
Date: 2023.08.10 07:31:37 -04'00'

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

Enclosure

2



Enclosure: Management Response to Recommendations Contained in GAO-23-105607

GAO recommended that the Director of U.S. Immigration and Customs Enforcement (ICE):

Recommendation 1: Establish and implement a process to periodically monitor whether HSI [Homeland Security Investigations] staff using facial recognition services to support criminal investigations have completed training requirements.

Response: Concur. On May 14, 2023, ICE HSI conducted a review of all licensed users, and the training that each user received and completed. The results of the review confirmed one hundred percent compliance of users completing training for privacy and the facial recognition technology (FRT) tool prior to receiving a license. Going forward, HSI will continue to ensure completion of required training for any user issued a license by periodically monitoring this activity on an ongoing basis. HSI will also continue to review its user compliance bi-annually to ensure staff using facial recognition services to support criminal investigations have completed training requirements. On July 18, 2023, HSI provided GAO evidence corroborating the completion of licensed users' training.

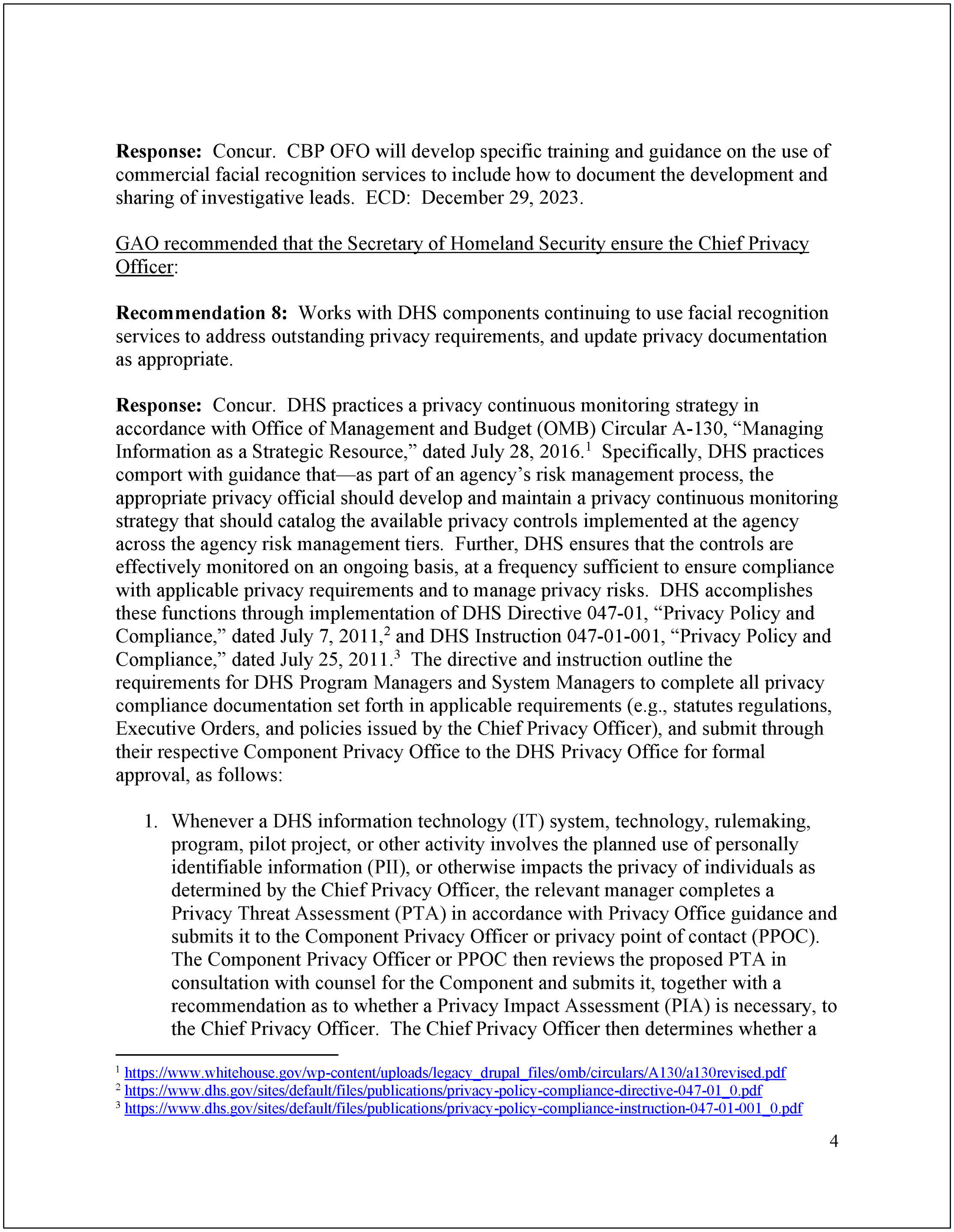
DHS requests the GAO consider this recommendation resolved and closed, as implemented.

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

Recommendation 4: Determine the extent that staff use facial recognition services to develop and share information in support of other agencies' criminal investigations (such as number of CBP staff that use the services and how often they do so).

Response: Concur. The CBP Office of Field Operations (OFO) will continue to work with current and future service providers to ensure that accurate metrics for CBP usage (e.g., number of queries, type of queries, queries by user, etc.) are available. OFO will also create guidance to capture instances where the use of a facial recognition service contributes to the development and sharing of information for lead purposes with an investigative partner. Estimated Completion Date (ECD): December 29, 2023.

Recommendation 5: Assess whether training would benefit staff using facial recognition services to develop and share information in support of other agencies' criminal investigations, incorporating information on the extent to which staff use such services.



Response: Concur. CBP OFO will develop specific training and guidance on the use of commercial facial recognition services to include how to document the development and sharing of investigative leads. ECD: December 29, 2023.

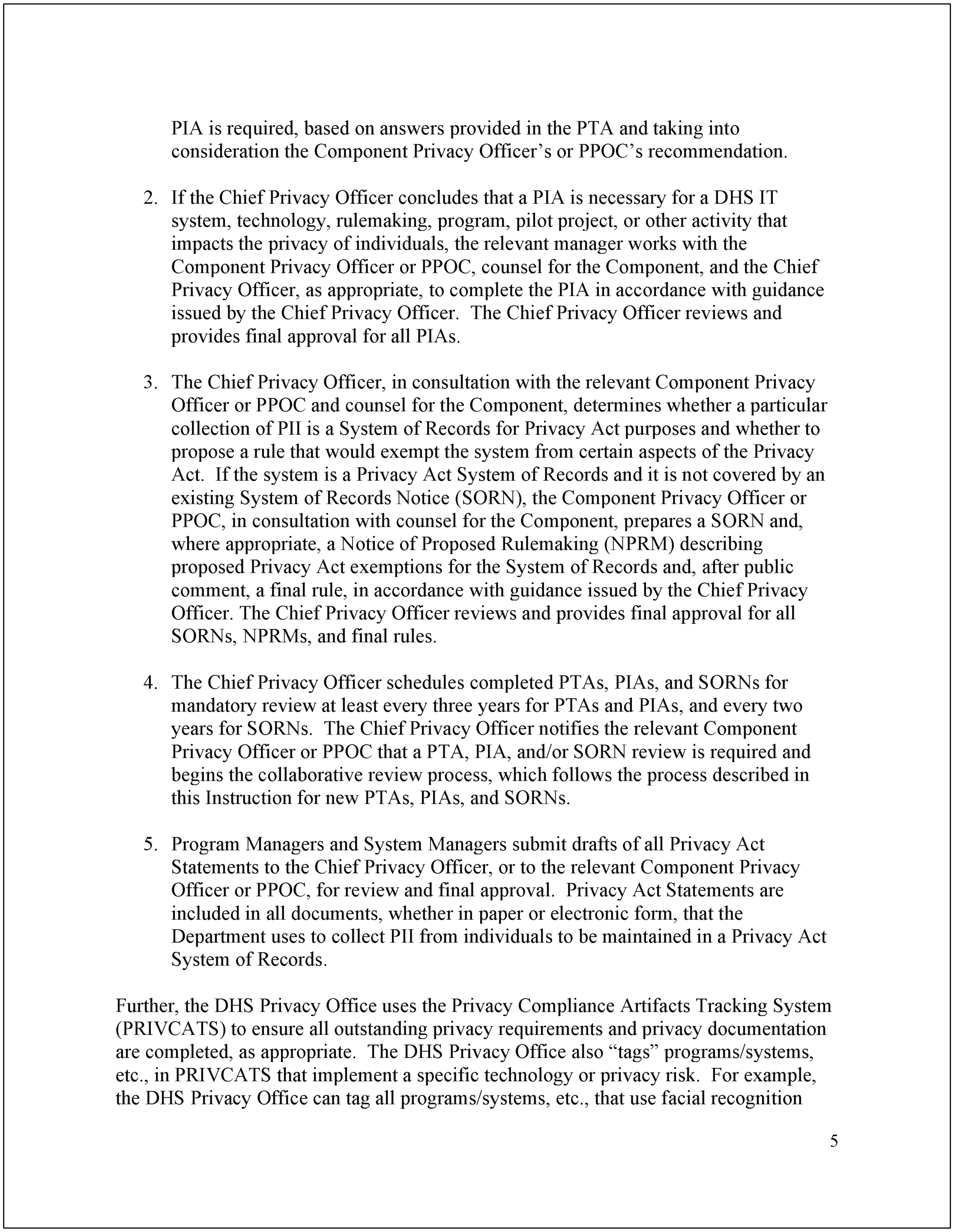
GAO recommended that the Secretary of Homeland Security ensure the Chief Privacy Officer:

Recommendation 8: Works with DHS components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate.

Response: Concur. DHS practices a privacy continuous monitoring strategy in accordance with Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," dated July 28, 2016.[1] Specifically, DHS practices comport with guidance that—as part of an agency's risk management process, the appropriate privacy official should develop and maintain a privacy continuous monitoring strategy that should catalog the available privacy controls implemented at the agency across the agency risk management tiers. Further, DHS ensures that the controls are effectively monitored on an ongoing basis, at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. DHS accomplishes these functions through implementation of DHS Directive 047-01, "Privacy Policy and Compliance," dated July 7, 2011,[2] and DHS Instruction 047-01-001, "Privacy Policy and Compliance," dated July 25, 2011.[3] The directive and instruction outline the requirements for DHS Program Managers and System Managers to complete all privacy compliance documentation set forth in applicable requirements (e.g., statutes regulations, Executive Orders, and policies issued by the Chief Privacy Officer), and submit through their respective Component Privacy Office to the DHS Privacy Office for formal approval, as follows:

1. Whenever a DHS information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of personally identifiable information (PII), or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer, the relevant manager completes a Privacy Threat Assessment (PTA) in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or privacy point of contact (PPOC). The Component Privacy Officer or PPOC then reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a Privacy Impact Assessment (PIA) is necessary, to the Chief Privacy Officer. The Chief Privacy Officer then determines whether a

[1] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[2] https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf
[3] https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf



PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation.

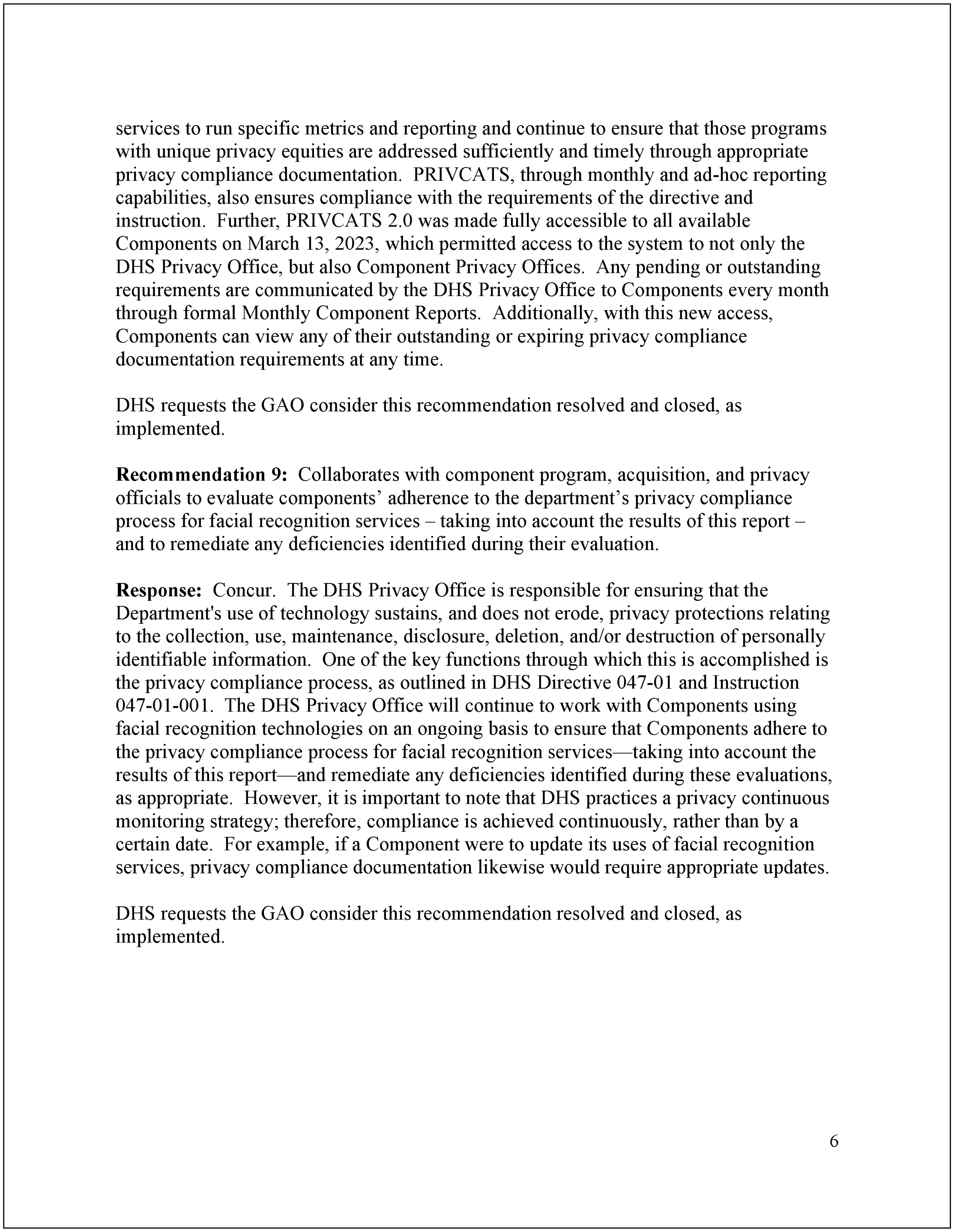
2. If the Chief Privacy Officer concludes that a PIA is necessary for a DHS IT system, technology, rulemaking, program, pilot project, or other activity that impacts the privacy of individuals, the relevant manager works with the Component Privacy Officer or PPOC, counsel for the Component, and the Chief Privacy Officer, as appropriate, to complete the PIA in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all PIAs.

3. The Chief Privacy Officer, in consultation with the relevant Component Privacy Officer or PPOC and counsel for the Component, determines whether a particular collection of PII is a System of Records for Privacy Act purposes and whether to propose a rule that would exempt the system from certain aspects of the Privacy Act. If the system is a Privacy Act System of Records and it is not covered by an existing System of Records Notice (SORN), the Component Privacy Officer or PPOC, in consultation with counsel for the Component, prepares a SORN and, where appropriate, a Notice of Proposed Rulemaking (NPRM) describing proposed Privacy Act exemptions for the System of Records and, after public comment, a final rule, in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all SORNs, NPRMs, and final rules.

4. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review at least every three years for PTAs and PIAs, and every two years for SORNs. The Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs.

5. Program Managers and System Managers submit drafts of all Privacy Act Statements to the Chief Privacy Officer, or to the relevant Component Privacy Officer or PPOC, for review and final approval. Privacy Act Statements are included in all documents, whether in paper or electronic form, that the Department uses to collect PII from individuals to be maintained in a Privacy Act System of Records.

Further, the DHS Privacy Office uses the Privacy Compliance Artifacts Tracking System (PRIVCATS) to ensure all outstanding privacy requirements and privacy documentation are completed, as appropriate. The DHS Privacy Office also "tags" programs/systems, etc., in PRIVCATS that implement a specific technology or privacy risk. For example, the DHS Privacy Office can tag all programs/systems, etc., that use facial recognition



services to run specific metrics and reporting and continue to ensure that those programs with unique privacy equities are addressed sufficiently and timely through appropriate privacy compliance documentation. PRIVCATS, through monthly and ad-hoc reporting capabilities, also ensures compliance with the requirements of the directive and instruction. Further, PRIVCATS 2.0 was made fully accessible to all available Components on March 13, 2023, which permitted access to the system to not only the DHS Privacy Office, but also Component Privacy Offices. Any pending or outstanding requirements are communicated by the DHS Privacy Office to Components every month through formal Monthly Component Reports. Additionally, with this new access, Components can view any of their outstanding or expiring privacy compliance documentation requirements at any time.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

Recommendation 9: Collaborates with component program, acquisition, and privacy officials to evaluate components' adherence to the department's privacy compliance process for facial recognition services – taking into account the results of this report – and to remediate any deficiencies identified during their evaluation.

Response: Concur. The DHS Privacy Office is responsible for ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of personally identifiable information. One of the key functions through which this is accomplished is the privacy compliance process, as outlined in DHS Directive 047-01 and Instruction 047-01-001. The DHS Privacy Office will continue to work with Components using facial recognition technologies on an ongoing basis to ensure that Components adhere to the privacy compliance process for facial recognition services—taking into account the results of this report—and remediate any deficiencies identified during these evaluations, as appropriate. However, it is important to note that DHS practices a privacy continuous monitoring strategy; therefore, compliance is achieved continuously, rather than by a certain date. For example, if a Component were to update its uses of facial recognition services, privacy compliance documentation likewise would require appropriate updates.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

Text for Appendix III: Comments from the Department of Homeland Security

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

August 10, 2023

Gretta L. Goodwin
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-105607, "FACIAL RECOGNITION SERVICES: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties"

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 its report.

DHS leadership is pleased to note GAO's positive recognition that DHS is currently finalizing and plans to issue new Department-wide guidance to ensure the protection of civil rights and civil liberties while staff use facial recognition technology. Specifically, the DHS Office of the Chief Information Officer, in coordination with the DHS Privacy Office, drafted the Face Recognition Directive and Instruction which will establish requirements for the responsible and authorized use of facial recognition technology. The Directive and Instruction are in final review and expected to be issued by December 29, 2023. DHS remains committed to embedding and enforcing privacy, civil rights, and civil liberties protections, and enhancing transparency, in all DHS activities and programs, as appropriate.

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

Again, thank you for the opportunity to review and comment on the 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

Enclosure: Management Response to Recommendations Contained in GAO-23-105607

GAO recommended that the Director of U.S. Immigration and Customs Enforcement (ICE):

Recommendation 1: Establish and implement a process to periodically monitor whether HSI [Homeland Security Investigations] staff using facial recognition services to support criminal investigations have completed training requirements.

Response: Concur. On May 14, 2023, ICE HSI conducted a review of all licensed users, and the training that each user received and completed. The results of the review confirmed one hundred percent compliance of users completing training for privacy and the facial recognition technology (FRT) tool prior to receiving a license. Going forward, HSI will continue to ensure completion of required training for any user issued a license by periodically monitoring this activity on an ongoing basis. HSI will also continue to review its user compliance bi-annually to ensure staff using facial recognition services to support criminal investigations have completed training requirements. On July 18, 2023, HSI provided GAO evidence corroborating the completion of licensed users' training.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

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

Recommendation 4: Determine the extent that staff use facial recognition services to develop and share information in support of other agencies' criminal investigations (such as number of CBP staff that use the services and how often they do so).

Response: Concur. The CBP Office of Field Operations (OFO) will continue to work with current and future service providers to ensure that accurate metrics for CBP usage (e.g., number of queries, type of queries, queries by user, etc.) are available. OFO will also create guidance to capture instances where the use of a facial recognition service contributes to the development and sharing of information for lead purposes with an investigative partner. Estimated Completion Date (ECD): December 29, 2023.

Recommendation 5: Assess whether training would benefit staff using facial recognition services to develop and share information in support of other agencies' criminal investigations, incorporating information on the extent to which staff use such services.

Response: Concur. CBP OFO will develop specific training and guidance on the use of commercial facial recognition services to include how to document the development and sharing of investigative leads. ECD: December 29, 2023.

GAO recommended that the Secretary of Homeland Security ensure the Chief Privacy Officer:

Recommendation 8: Works with DHS components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate.

Response: Concur. DHS practices a privacy continuous monitoring strategy in accordance with Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," dated July 28, 2016.[1] Specifically, DHS practices comport with guidance that—as part of an agency's risk management process, the appropriate privacy official should develop and maintain a privacy continuous monitoring strategy that should catalog the available privacy controls implemented at the agency across the agency risk management tiers. Further, DHS ensures that the controls are effectively monitored on an ongoing basis, at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. DHS accomplishes these functions through implementation of DHS Directive 047-01, "Privacy Policy and Compliance," dated July 7, 2011,[2] and DHS Instruction 047-01-001, "Privacy Policy and Compliance," dated July 25, 2011.[3] The directive and instruction outline the requirements for DHS Program Managers and System Managers to complete all privacy compliance documentation set forth in

[1] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[2] https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf

[3] https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf

applicable requirements (e.g., statutes regulations, Executive Orders, and policies issued by the Chief Privacy Officer), and submit through their respective Component Privacy Office to the DHS Privacy Office for formal approval, as follows:

1. Whenever a DHS information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of personally identifiable information (PII), or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer, the relevant manager completes a Privacy Threat Assessment (PTA) in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or privacy point of contact (PPOC). The Component Privacy Officer or PPOC then reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a Privacy Impact Assessment (PIA) is necessary, to the Chief Privacy Officer. The Chief Privacy Officer then determines whether a PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation.
2. If the Chief Privacy Officer concludes that a PIA is necessary for a DHS IT system, technology, rulemaking, program, pilot project, or other activity that impacts the privacy of individuals, the relevant manager works with the Component Privacy Officer or PPOC, counsel for the Component, and the Chief Privacy Officer, as appropriate, to complete the PIA in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all PIAs.
3. The Chief Privacy Officer, in consultation with the relevant Component Privacy Officer or PPOC and counsel for the Component, determines whether a particular collection of PII is a System of Records for Privacy Act purposes and whether to propose a rule that would exempt the system from certain aspects of the Privacy Act. If the system is a Privacy Act System of Records and it is not covered by an existing System of Records Notice (SORN), the Component Privacy Officer or PPOC, in consultation with counsel for the Component, prepares a SORN and, where appropriate, a Notice of Proposed Rulemaking (NPRM) describing proposed Privacy Act exemptions for the System of Records and, after public comment, a final rule, in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all SORNs, NPRMs, and final rules.
4. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review at least every three years for PTAs and PIAs, and every two years for SORNs. The Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs.

5. Program Managers and System Managers submit drafts of all Privacy Act Statements to the Chief Privacy Officer, or to the relevant Component Privacy Officer or PPOC, for review and final approval. Privacy Act Statements are included in all documents, whether in paper or electronic form, that the Department uses to collect PII from individuals to be maintained in a Privacy Act System of Records.

Further, the DHS Privacy Office uses the Privacy Compliance Artifacts Tracking System (PRIVCATS) to ensure all outstanding privacy requirements and privacy documentation are completed, as appropriate. The DHS Privacy Office also “tags” programs/systems, etc., in PRIVCATS that implement a specific technology or privacy risk. For example, the DHS Privacy Office can tag all programs/systems, etc., that use facial recognition services to run specific metrics and reporting and continue to ensure that those programs with unique privacy equities are addressed sufficiently and timely through appropriate privacy compliance documentation. PRIVCATS, through monthly and ad-hoc reporting capabilities, also ensures compliance with the requirements of the directive and instruction. Further, PRIVCATS 2.0 was made fully accessible to all available Components on March 13, 2023, which permitted access to the system to not only the DHS Privacy Office, but also Component Privacy Offices. Any pending or outstanding requirements are communicated by the DHS Privacy Office to Components every month through formal Monthly Component Reports. Additionally, with this new access, Components can view any of their outstanding or expiring privacy compliance documentation requirements at any time.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

Recommendation 9: Collaborates with component program, acquisition, and privacy officials to evaluate components’ adherence to the department’s privacy compliance process for facial recognition services – taking into account the results of this report – and to remediate any deficiencies identified during their evaluation.

Response: Concur. The DHS Privacy Office is responsible for ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of personally identifiable information. One of the key functions through which this is accomplished is the privacy compliance process, as outlined in DHS Directive 047-01 and Instruction 047-01-001. The DHS Privacy Office will continue to work with Components using facial recognition technologies on an ongoing basis to ensure that Components adhere to the privacy compliance process for facial recognition services—taking into account the results of this report—and remediate any deficiencies identified during these evaluations, as appropriate. However, it is important to note that DHS practices a privacy continuous monitoring strategy;

therefore, compliance is achieved continuously, rather than by a certain date. For example, if a Component were to update its uses of facial recognition services, privacy compliance documentation likewise would require appropriate updates.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

Appendix IV: GAO Contact and Staff Acknowledgements

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Jeffrey Fiore (Assistant Director), Kathleen Donovan (Analyst-in-Charge), Ricki Gaber, Sheerine Karamzadeh-Rahimi, Grace Kwon, Brooke Linsenbardt and John Vocino made key contributions to this report. Also contributing to this report were Benjamin Crossley, Caitlin Cusati, Richard Hung, Lydie Loth, Lee McCracken, Heidi Nielson, Monica Perez-Nelson, 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/about/what-gao-does/fraudnet

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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