LAW ENFORCEMENT
DHS Could Better Address Bias Risk and Enhance Privacy Protections for Technologies Used in Public

Report to Congressional Requesters

December 2024

GAO-25-107302

United States Government Accountability Office

Accessible Version

GAO Highlights

View GAO-25-107302. For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov.
Highlights of GAO-25-107302, a report to congressional requesters

LAW ENFORCEMENT

DHS Could Better Address Bias Risk and Enhance Privacy Protections for Technologies Used in Public

Why GAO Did This Study

Technologies such as automated license plate readers and drones can support federal law enforcement activities. However, the use of these technologies in public spaces—where a warrant is not necessarily required prior to use—has led to concerns about how law enforcement is protecting civil rights, civil liberties, and privacy.

GAO was asked to review federal law enforcement's use of detection, observation, and monitoring technologies. This report examines 1) the use of these technologies in public spaces without a warrant by selected DHS law enforcement agencies and 2) the extent to which the agencies have policies to assess the use of technologies for bias and protect privacy.

GAO selected CBP, ICE, and the Secret Service within DHS based on various factors, including the large number of law enforcement officers in these agencies. GAO administered a structured questionnaire and reviewed documents, such as technology policies. GAO also interviewed agency officials.

What GAO Recommends

GAO is making five recommendations including that DHS develop policies and procedures to assess the risks of bias and ensure CBP, ICE and Secret Service implement privacy protections through technology policies. DHS concurred, but ICE and Secret Service described actions they have taken that do not address the recommendations, as discussed.

What GAO Found

Department of Homeland Security (DHS) law enforcement agencies reported using over 20 types of detection, observation, and monitoring technologies in fiscal year 2023. This includes both technologies the agencies owned or leased, as well as technologies the agencies accessed through third parties such as commercial vendors and other law enforcement agencies. For example, all three selected DHS law enforcement agencies reported that they have agreements to query or view information from third-party automated license plate readers, providing law enforcement personnel with access to a nationwide source of license plate data. The selected DHS agencies also reported using a variety of analytic software, including some based on artificial intelligence (AI), that can enhance the capabilities of their detection, observation, and monitoring technologies.

Figure: Examples of Detection, Observation, and Monitoring Technology



Source: Tartila and Svitlana/stock.adobe.com. | GAO-25-107302

DHS is developing policies and procedures to address bias risk from technologies that use AI, but it does not have policies or procedures to assess bias risks from the use of all detection, observation, and monitoring technology. DHS law enforcement agencies may seek out advice from DHS's Office for Civil Rights and Civil Liberties (CRCL) on bias issues related to technology use; however, there are no requirements to do so. As a result, CRCL's level of review of detection, observation, and monitoring technologies has varied. By developing policies and procedures to assess and address the risk of bias posed by DHS law enforcement agencies' use of detection, observation, and monitoring technologies, CRCL could help ensure these technologies are not infringing on civil rights and civil liberties by introducing bias.

Technology use policies GAO reviewed at U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and Secret Service did not always address key privacy protections. DHS conducts privacy impact assessments to provide the public with information on how the agency plans to address key privacy protections. Policies, however, are needed to direct employees in how they are to implement these privacy protections when using a particular technology. By requiring that policies for the use of each technology address key privacy protections, DHS agencies would have better assurance that the privacy protections are being implemented and that technology users are aware of their responsibilities to protect privacy.

Contents

GAO Highlights i

Why GAO Did This Study i

What GAO Recommends i

What GAO Found i

Letter 1

Background 4

DHS Law Enforcement Agencies Use a Variety of Detection, Observation, and Monitoring Technologies in Public Spaces 10

DHS is Developing Policies and Procedures to Assess AI for Bias but Does Not Require Assessments for Other Detection, Observation, and Monitoring Technology 15

DHS Has a Process to Consider Privacy Protections, but Its Technology Policies Do Not Always Address Them 19

Conclusions 23

Recommendations for Executive Action 24

Agency Comments and Our Evaluation 24

Appendix I Department of Homeland Security Law Enforcement Technology 28

Appendix II Comments from the Department of Homeland Security 35

Appendix III GAO Contact and Staff Acknowledgments 39

GAO Contact 39

Staff Acknowledgements 39

Figures

Figure 1: Selected Department of Homeland Security (DHS) Law Enforcement Missions 5

Figure 2: Types of bias 7

Figure 3: Technologies Owned or Accessed and Can Be Used in Public Spaces Without a Warrant, as Reported to GAO by Selected DHS Law Enforcement Agencies for Fiscal Year 2023 11

Figure 4: Analytic Software Owned or Accessed That Can Be Used on Information Collected in Public Spaces Without a Warrant, Reported to GAO by Selected DHS Law Enforcement Agencies for Fiscal Year 2023 14

Figure 5: Assessment of Technology Policies against Selected Privacy Protections 21

Figure 6: Department of Homeland Security (DHS) law enforcement technologies and analytic software systems owned or accessed and can be used in public spaces without a warrant, fiscal year 2023 29

Abbreviations

AI	Artificial Intelligence
CBP	U.S. Customs and Border Protection
CRCL	Office for Civil Rights and Civil Liberties
DHS	Department of Homeland Security
ICE	U.S. Immigration and Customs Enforcement
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
UAS	Uncrewed Aircraft Systems

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

December 3, 2024

Congressional Requesters

As technological advances are made, law enforcement has a broader array of tools for detection, observation, and monitoring. These technologies, such as automated license plate readers, body-worn cameras, gunshot detection, and associated analytic software can help law enforcement catch criminals and prevent unlawful acts. However, the use of these technologies in public spaces—where a warrant is not necessarily required prior to use—has led members of Congress and others to raise concerns about how law enforcement agencies are protecting civil rights, civil liberties, and privacy.[1]

We have previously reported on federal law enforcement's use of one type of detection, observation, and monitoring technology—facial recognition.[2] For example, in September 2023, we found that law enforcement agencies in the Department of Justice and the Department of Homeland Security (DHS) were developing additional policies on civil rights and civil liberties but could do more to ensure training and privacy requirements are met. We made 10 recommendations, including that U.S. Immigration and Customs Enforcement (ICE) establish and implement a process to periodically monitor whether staff using facial recognition services to support criminal investigations have completed training requirements.[3]

You asked us to review federal law enforcement's use of detection, observation, and monitoring technology. This report addresses the use of this technology within DHS, one of the departments with the most federal law enforcement officers.[4] Specifically, this report examines:

1. the detection, observation, and monitoring technologies that selected DHS law enforcement agencies use in public spaces without a warrant, and how they use them;

[1]For the purposes of this engagement, we are defining privacy as individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information, including data such as their names, social security numbers, or photos. Additionally, for the purposes of this report, we define 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.

[2]GAO, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607 (Washington, D.C.: Sept. 5, 2023); *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns,* GAO-24-106293 (Washington, D.C.: Apr. 22, 2024); and *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Washington, D.C.: June 3, 2021). These reports have different scopes and cover different time periods so the information presented may not be comparable.

[3]See GAO-23-105607. As of August 2024, DHS and the Department of Justice agencies have taken action to implement four of the ten recommendations. For example, in April 2024, DHS stakeholders reviewed components' adherence to privacy requirements for facial recognition in response to our recommendation that they conduct such a review. As a result, DHS is better positioned to address privacy requirements and increase transparency of its use of the technology. The recommendation that ICE implement a process to monitor facial recognition training requirements remains open. To fully implement this recommendation, ICE needs to provide evidence of its periodic monitoring of training requirements.

[4]GAO also has ongoing work reviewing the use of detection, observation, and monitoring technology by selected law enforcement agencies within the Department of Justice.

2. the extent to which selected DHS law enforcement agencies have policies and procedures in place to assess the use of technologies for bias; and

3. the extent to which selected DHS federal law enforcement agencies protect privacy by having policies and procedures in place that limit the collection and use of information from these technologies.

To address all three objectives, we administered a standardized questionnaire to three DHS law enforcement agencies—U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (Secret Service). We selected these agencies based on factors such as the number of officers and their roles in criminal investigations, police response, and security and protection. The selected DHS law enforcement agencies are not representative of all DHS or federal law enforcement agencies but are the largest agencies within DHS and represent about 98 percent of DHS law enforcement officers.[5] As such, they provide important context and illustrative examples of the technologies in use.

Standardized questionnaires are subject to nonsampling errors due to practical issues such as differences in interpreting a particular question or the information available to respondent. We took steps to minimize such nonsampling error, such as conducting interviews with officials from the selected agencies before and after the standardized questionnaire to ensure the scope and questions were clear and the responses were comprehensive. As a result of these interviews, we made changes to the questionnaire before finalizing it for administration, and we made updates to questionnaire responses as appropriate based on our follow-up with agency officials.

We also interviewed subject matter experts from nine organizations on the technologies and associated civil rights, civil liberties, and privacy issues. We selected these organizations based on the type and focus of the organization—to include law enforcement, privacy and civil liberties advocacy, public policy, and trade organizations. Specifically, we interviewed subject matter experts from the American Civil Liberties Union, the Brennan Center for Justice, the Cato Institute, the Commission on Accreditation for Law Enforcement Agencies, the Electronic Frontier Foundation, the Electronic Privacy Information Center, the International Association of Chiefs of Police, the International Biometrics and Identity Association, and the Project on Government Oversight. We followed up with these organizations to give them the opportunity to ensure our understanding of their responses were accurate and current. The results of these interviews cannot be generalized beyond these organizations, but they reflect a range of perspectives on the types of and uses for these technologies.

To answer the first objective, we administered a standardized questionnaire to obtain and then analyzed DHS agencies' information on the detection, observation, and monitoring technologies these agencies used in fiscal year 2023. For the purposes of this report, we defined detection, observation, and monitoring technologies as technologies with sensors that capture or use data that is reasonably likely to identify individuals or an activity or action when used singly, or in combination with other information. We included detection, observation, and monitoring technologies that agencies owned or leased or accessed through a third party on a continuous basis via a contract, memorandum of understanding, or other formal arrangement.

[5]See Department of Justice, Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2020 – Statistical Tables*, NCJ 304752 (Sept. 2022).

Further, we limited the scope to those technologies that agencies may use in public spaces without obtaining a warrant, including exceptional situations that may justify the warrantless use of a technology.[6] We also obtained and examined information on the analytic tools the selected federal law enforcement agencies are using on the data these technologies collect.

To answer the second objective, we obtained and analyzed DHS Office for Civil Rights and Civil Liberties and the selected agencies' policies and procedures for assessing technology uses for bias. For the purposes of this report, we are defining bias as a positive or negative preference for a group based on characteristics such as actual or perceived race, ethnicity, national origin, religion, or sex.[7] We assessed the agencies' policies and procedures against agency responsibilities, executive orders, and the control activities component of *Standards for Internal Control in the Federal Government*.[8]

Lastly, to answer the third objective, we reviewed relevant departmental privacy policies and guidance, including those on implementing aspects of the E-government Act of 2002 and the Fair Information Practice Principles.[9] We selected six privacy protections, drawn from the Fair Information Practice Principles, that most directly addressed our research question on policies and procedures to limit the collection and use of personally identifiable information from these technologies.[10] To identify the extent to which agencies addressed selected privacy protections, we obtained and analyzed agencies' privacy documentation, policies, and procedures for each technology.[11] We also interviewed cognizant agency officials. Finally, we assessed agencies' efforts to determine if they had policies and procedures to address selected privacy protections for

[6]For the purposes of this report, we define public spaces as common outdoor areas or locations that are freely accessible to the general population. This includes, but is not limited to, streets, highways, parks, beaches, and open space. We are not including indoor spaces such as federal buildings, airports, or courtrooms. We are also not including technology used during inspection processes at ports of entry or to process individuals who have been arrested. Finally, we are not including "virtual" public spaces, such as social media and the internet. According to DHS policy, various types of exigent or exceptional situations such as potential loss of life or destruction of evidence, may justify a warrantless use of a technology. DHS law enforcement agencies may initially use such technology without a search warrant but are to apply for a warrant within 48 hours, as per DHS policy. We have included technologies that may be used pursuant to this exigent situation in our scope. We did not assess DHS's determination as to which technologies may be subject to a warrant requirement or the exigent circumstances exception under the Fourth Amendment.

[7]As discussed further in the background section of this report, positive or negative preference for a group can stem from human or systemic biases or can be introduced or replicated through statistical biases from artificial intelligence (AI) algorithms.

[8]DHS, *Instruction for the Office for Civil Rights and Civil Liberties* (Nov. 6, 2013). Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety, Exec. Order No. 14074, 87 Fed. Reg. 32,945 (May 31, 2022).; Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, Exec. Order No. 14901, 88 Fed. Reg. 10825 (Feb. 22, 2023); GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[9]DHS Privacy Office, *Privacy Impact Assessments: Privacy: Office Official Guidance*, (Washington, D.C.: June 2010). DHS Privacy Office, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, Policy Directive 140-03 (Washington, D.C.: Dec. 29, 2008). See E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921.

[10]We determined that the Fair Information Practice Principles of "individual participation" and "data quality and integrity" and parts of the "purpose specification" and "accountability and auditing" principles were not directly applicable in the law enforcement context or were outside the scope of our review. We also split the "data minimization" principle to assess data collection and retention separately.

[11]For this objective, we used the list of technologies identified in the responses to our questionnaire. We also included facial recognition because it is a stand-alone analytic tool. The other analytic tools listed in objective 1—anomaly detection, object recognition, and object tracking—are part of other technologies included in this review.

using detection, observation, and monitoring technology, consistent with *Standards for Internal Control in the Federal Government*.[12]

We conducted this performance audit from February 2023 to December 2024 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

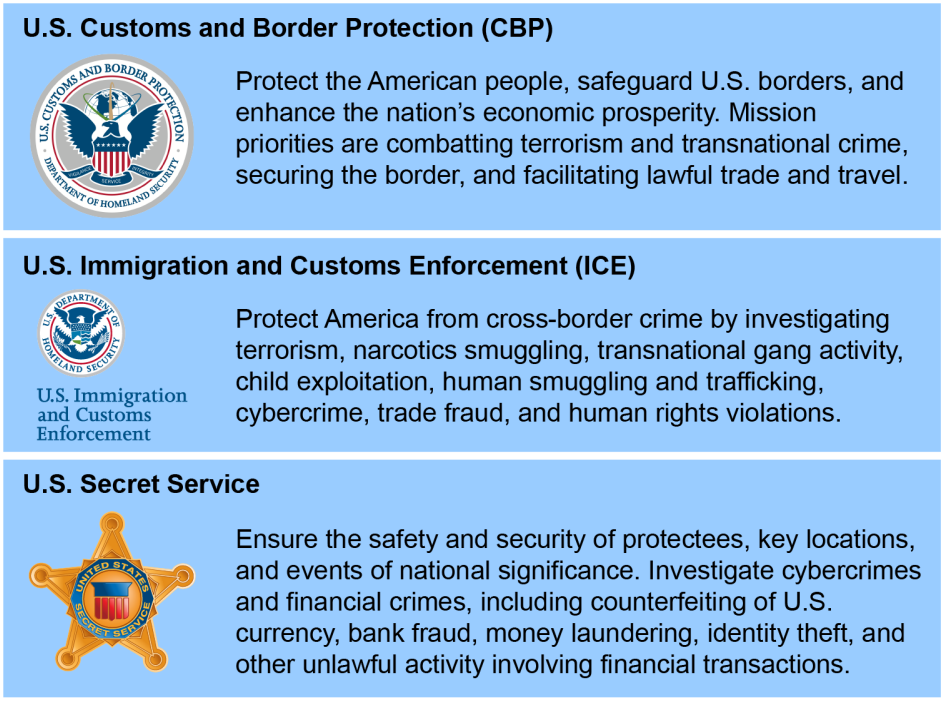
Roles and responsibilities

DHS law enforcement agencies we reviewed are responsible for a wide variety of law enforcement activities that are critically important to maintaining national security, as shown in figure 1. In fiscal year 2020, DHS employed more than 66,000 full-time law enforcement officers, which accounted for nearly half (49 percent) of all full-time federal law enforcement officers that year.[13]

[12]GAO-14-704G. The control activities component of internal control includes the principal that management should implement control activities through policies.

[13]This is the most recent year for which data are available. See Department of Justice, Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2020 – Statistical Tables*, NCJ 304752 (Sept. 2022).

Figure 1: Selected Department of Homeland Security (DHS) Law Enforcement Missions



Source: Agency information; U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Secret Service (seals). | GAO-25-107302

These law enforcement agencies operate across the United States. For example, ICE and Secret Service have field offices across the country to investigate crimes under their jurisdictions. Secret Service also provides protection for U.S. and visiting world leaders, presidential and vice-presidential candidates, and others, and leads security for certain events, such as the U.N. General Assembly and the Democratic and Republican national conventions.[14] As part of its enforcement of immigration laws at the border and surrounding areas, CBP operates immigration checkpoints at more than 110 locations on major U.S. highways and secondary roads, usually 25 to 100 miles inland from the border, to detect and apprehend (1) removable people, including smuggled humans; (2) human and drug (or other contraband) smugglers; and (3) suspected terrorists attempting to travel into the interior of the U.S. after evading detection at the border. At these check points, CBP conducts inspections of vehicles, including taking photos of license plates by an automated camera.

When conducting law enforcement activities, law enforcement agencies must operate within constitutional parameters. For example, the Fourth Amendment—which protects against unreasonable search and seizure—generally requires law enforcement to obtain a warrant for surveillance activities conducted when the individual has a reasonable expectation of privacy.[15] However, if government surveillance does not implicate a

[14]See 18 U.S.C. § 3056.

[15]U.S. Const. amend. IV. The Supreme Court has held that "the Fourth Amendment protects people, not places," and wherever an individual may harbor a reasonable "expectation of privacy," he is entitled to be free from unreasonable governmental intrusion. *Terry v. Ohio*, 392 U.S. 1, 9 (citing *Katz v. U.S.*, 389 U.S. 347, 351, 361 (1967)).

reasonable expectation of privacy, law enforcement can typically conduct such activities.[16] Such situations may include public spaces because the Supreme Court has held that what a person knowingly exposes to the public is not subject to Fourth Amendment protection and does not maintain a reasonable expectation of privacy.[17] Further, as technology has "enhanced the Government's capacity" to conduct detection, observation, and surveillance activities, the Supreme Court has issued decisions that assess advancing technologies and constitutional protections against unreasonable search and seizure under the Fourth Amendment.[18]

Congress has passed laws to help ensure the preservation of civil rights and civil liberties while law enforcement officers execute their duties. For example, the Homeland Security Act of 2002, which created DHS, also established the Officer for Civil Rights and Civil Liberties.[19] In addition, DHS was one of the eight agencies required to designate a senior official for civil liberties under the Implementing Recommendations of the 9/11 Commission Act of 2007.[20] In accordance with these laws, DHS established the Office for Civil Rights and Civil Liberties (CRCL). CRCL is responsible for directing, overseeing, and coordinating the protection and promotion of civil rights and civil liberties of members of the public in all department activities. CRCL's duties also include policy development and implementation and investigating civil rights and civil liberties complaints filed by the public.[21]

Equity, Civil Rights, and Civil Liberties

The use of detection, observation, and monitoring technologies by law enforcement presents questions about bias and the effects on equity, civil rights, and civil liberties, according to researchers and others. Positive or negative preferences for a group can stem from human or systemic biases or can be introduced or replicated through statistical biases from artificial intelligence (AI) algorithms, as shown in figure 2.

[16]See Orin S. Kerr, Lifting The "Fog" Of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 Hastings L.J. 805, 811 (2017) (citing *Florida v. Riley*, 488 U.S. 445, 450 (1989) (allowing law enforcement to pilot a helicopter that allowed them to view the defendant's property and observe it from public airspace without a warrant); *Kirk v. Louisiana*, 536 U.S. 635 (2002) (holding that absent exigent circumstances, the police may not enter a suspect's home without his consent or the consent of someone with common authority over the area entered)).

[17]See *U.S. v. Knotts*, 460 U.S. 276 (1983) (holding "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); see also *Katz.*, 389 U.S. at 361 (Harlan, J., concurring) (noting that "objects, activities, or statements that [a person] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited" and "conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable").

[18]*Carpenter v. United States*, 585 U.S. 296, 305 (2018) (holding that "unrestricted access to a wireless carrier's database of physical location information" violated the fourth Amendment); see generally, *United States v. Kyllo*, 533 U.S. 27 (2001) (holding that the Government's use of "a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion" constitutes a Fourth Amendment search and "is presumptively unreasonable without a warrant"); *California v. Ciraolo*, 476 U.S. 207 (1986) (holding that "[t]he Fourth Amendment simply does not require the police traveling in the public airways [at an altitude of 1,000 feet] to obtain a warrant in order to observe what is visible to the naked eye").

[19]Pub. L. No. 107-296, § 705, 116 Stat. 2135, 2219-2220 (codified as amended at 6 U.S.C. § 345).

[20]Pub. L. No. 110-53, § 803, 121 Stat. 266, 360-362.

[21]DHS, *Instruction for the Office for Civil Rights and Civil Liberties* (Nov. 6, 2013).

Figure 2: Types of bias

Bias	*Description*
Human 	Human biases can be explicit or implicit. Explicit bias occurs when individuals have conscious prejudices and attitudes toward certain groups. Implicit bias is a result of subconscious feelings, perceptions, and attitudes. Individuals may not be aware of how this type of bias affects their decision-making. Researchers have identified many forms of cognitive biases, including confirmation bias where people prefer information that aligns with existing beliefs. Another form of bias is anchoring bias, where people's decisions are influenced by an initially presented value and do not adequately adjust to new information.
Systemic 	Systemic biases are the result of procedures and practices of particular institutions. Systemic biases are not necessarily the result of conscious prejudice or discrimination but rather occur by the majority following existing rules or norms.
Statistical 	Statistical biases stem from data that is not representative of the population. In artificial intelligence (AI) systems, these biases can be present in the datasets and algorithmic processes used to develop the technology. Biases often arise when algorithms are trained on one type of data but are applied to data that is more complex or heterogeneous.

Source: GAO analysis of Department of Justice and National Institute of Standards and Technology guidance; GAO icons. | GAO-25-107302

We and others have reported that the introduction of AI can enhance the capabilities of technology but can also increase the risk of bias.[22] For example, a 2024 National Academies report found that while progress has been made in the accuracy of facial recognition algorithms, they still perform less well for groups with certain characteristics, including those associated with race, ethnicity, or gender.[23] The report also noted that of the six known cases where wrongful arrests have been made on the basis of facial recognition technology, all such arrests were of Black or African American individuals.

Additionally, the Biden administration and others have warned that improper collection and use of people's data could have a chilling effect on First Amendment rights.[24] For example, the International Association of Chiefs of Police identified the enhanced collection and compilation of automated license plate reader data—particularly in areas that can reflect an individual's political, religious, or social views, associations, or activities—as increasing the risk that individuals will become more cautious in the exercise of their protected

[22]GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities,* GAO-21-519SP (Washington, D.C.: June 2021).

[23]National Academies of Science, Engineering, and Medicine*, Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* (Washington, D.C.: 2024).

[24]Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Exec. Order No. 14110, 88 Fed. Reg. 75,191 (Nov. 1, 2023).

rights because they consider themselves under constant surveillance.[25] In addition, civil liberties advocates have noted that the use of facial recognition at certain events—such as protests—could cause people to refrain from engaging in these events in the future for fear of how the their data will be collected and used.[26]

An October 2023 executive order notes that AI, in particular, is making it easier to extract, reidentify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires.[27] The Office of Management and Budget uses the term the "mosaic effect" to describe when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual, but when combined with other available information, could pose such risk.[28]

The Office of Management and Budget issued guidance to federal agencies in March 2024 to help ensure the responsible use of AI so that it does not adversely impact people's rights or safety.[29] The guidance calls for agencies to implement risk management practices including assessing and mitigating disparate impacts and algorithmic discrimination, and continuously monitoring and evaluating the performance of deployed AI.

Privacy Requirements

Detection, observation, and monitoring technologies may collect personally identifiable information (PII). DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, or other information that otherwise can be linked to an individual. For example, this can include a name, license plate number, or photograph.[30]

Federal laws, along with executive branch policy and guidance, establish agency requirements and responsibilities for ensuring the protection of PII. These include the following:

- **Privacy Act of 1974.**[31] The act places limitations on agencies' collection, disclosure, and use of personal information maintained in agency systems of record.[32] Among other requirements, it requires that agencies not maintain records describing how individuals exercise rights guaranteed by the First

[25]International Association of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers* (Alexandria, VA: Sept. 2009).

[26]In our June 2021 report, we reported that six federal agencies used facial recognition technology on images of the unrest, riots, or protests following the death of George Floyd in May 2020. We also reported that three agencies used facial recognition technology on images of the events at the U.S. Capitol on January 6, 2021. See GAO-21-518.

[27]Exec. Order No. 14110, 88 Fed. Reg. at 75,193.

[28]Office of Management and Budget, Memorandum M-13-13*: Open Data Policy-Managing Information as an Asset* (Washington, D.C.: May 9, 2013).

[29]Office of Management and Budget, Memorandum M-24-10*: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Washington, D.C.: Mar. 28, 2024).

[30]DHS, *Privacy Policy and Compliance*, Instruction 047-01-001 (July 25, 2011).

[31]Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

[32]A system of records is a collection of information about an individual under control of an agency from which information is retrieved by the name of an individual or other identifier. 5 U.S.C. § 552a(a)(4), (5).

Amendment, except for limited circumstances such as if the information is within the scope of an authorized law enforcement activity.[33]

- **Fair Information Practice Principles.** In 1973, a U.S. government advisory committee first proposed the Fair Information Practice Principles for protecting the privacy and security of personal information. The principles were central to the Privacy Act of 1974 and include, among others, specifying the purpose for collecting PII and limiting the collection and retention of this information to what is necessary for the stated purpose. While the principles are not legal requirements, the Office of Management and Budget advises agencies to use them to evaluate information systems, processes, programs, and activities that affect individual privacy.[34] DHS guidance requires the department to use the Fair Information Practice Principles to assess and enhance privacy protections.[35]
- **E-Government Act of 2002.**[36] The act requires, among other things, that agencies conduct a privacy impact assessment (PIA) before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form. The act requires that the Director of the Office of Management and Budget develop guidance for agencies specifying the required contents of a PIA, including that a PIA describes what information the agency is collecting, why the information is being collected, how the information will be used and shared, and how the information will be secured.
- **Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource.**[37] The circular contains responsibilities for federal agencies managing information resources that involve PII and summarizes the key privacy requirements for managing those resources. These responsibilities include developing, implementing, documenting, maintaining, and overseeing agency-wide privacy programs to ensure compliance with all applicable statues, regulations, and policies. Specifically, such compliance responsibilities relate to, among other things, the use of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency.
- **DHS PIA guidance.**[38] According to DHS guidance, the PIA is designed to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program. Per the DHS guidance, conducting a PIA at the beginning of the development process ensures that the information is handled appropriately in the first instance and that privacy was considered from the beginning stages. DHS also requires a privacy threshold analysis to document whether a technology needs a PIA. According to officials from the DHS Privacy Office, the program office that intends to use the technology is required to initiate the privacy threshold analysis. These officials stated that the submission of the privacy threshold analysis is how the DHS Privacy Office becomes aware of technologies used by the agencies.

[33]5 U.S.C. § 552a(e)(7).

[34]Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

[35]DHS Privacy Office, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, Policy Directive 140-03 (Washington, D.C.: Dec. 29, 2008).

[36]Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921.

[37]Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

[38]DHS Privacy Office, *Privacy Impact Assessments: The Privacy Office Official Guidance*, (Washington, D.C.: June 2010).

DHS Law Enforcement Agencies Use a Variety of Detection, Observation, and Monitoring Technologies in Public Spaces

Agencies Report Owning and Accessing a Variety of Detection, Observation, and Monitoring Technologies

In response to our standardized questionnaire, DHS law enforcement agencies reported using over 20 unique types of technologies in fiscal year 2023 that they either owned or accessed through third parties.[39] According to DHS, these technologies could be used in public spaces without necessarily obtaining a warrant.[40] This includes technologies used during exigent situations that may justify the warrantless use of a technology.[41] The technologies were either owned or leased by the agencies or the agencies had a formal, written agreement to access the technologies through third parties. Third parties can include commercial vendors, businesses or other organizations, individuals, and other federal, state, tribal, territorial, and local agencies.

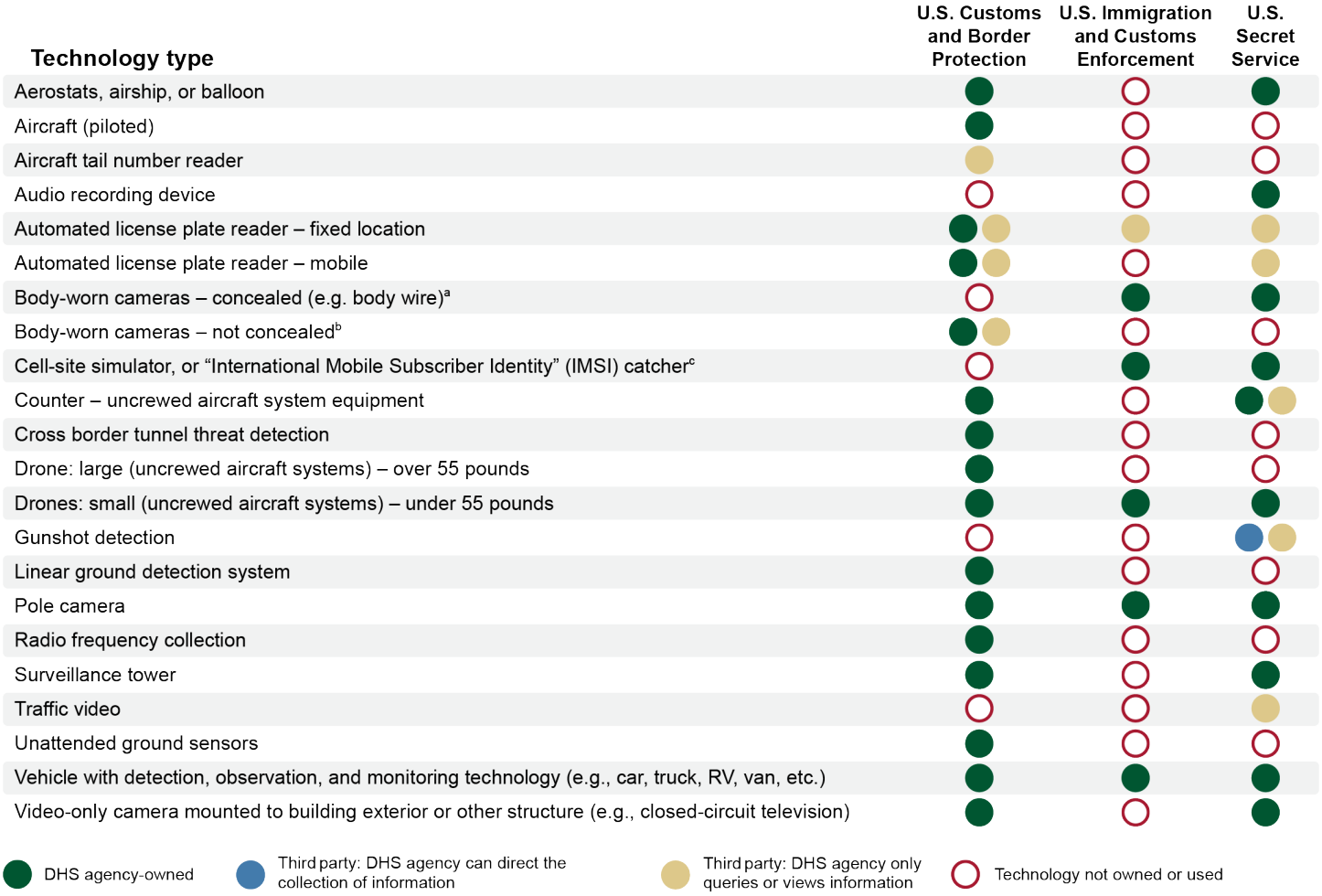
We further characterized third-party access based on whether the agency reported it could (1) direct the third-party technology by controlling when, where, and/or what it detects, observes, or monitors; or (2) query or view information collected by the third-party technology but not direct the collection of information. As reported by the DHS law enforcement agencies in our review, figure 3 presents the detection, observation, and monitoring technologies owned or accessed, for fiscal year 2023.

[39]For the purposes of this report, detection, observation, and monitoring technologies are those that capture or use audio, images, video, radar, thermal imaging, cellphone subscriber identity and location, chemical, biological, or other data that is reasonably likely to identify individuals or an activity or action when used singly, or in combination with other information or tools to analyze the data collected by these technologies.

[40]When conducting law enforcement activities using the DHS reported detection, observation, and monitoring technologies, law enforcement agencies must operate within constitutional parameters. For example, the Fourth Amendment—which protects against unreasonable search and seizure—generally requires law enforcement to obtain a warrant for surveillance activities conducted when the individual has a reasonable expectation of privacy.

[41]According to DHS policy, various types of exigent situations such as potential loss of life or destruction of evidence, may justify a warrantless use of a technology. DHS law enforcement agencies may initially use such technology without a search warrant but are to apply for a warrant within 48 hours, according to the policy. We have included technologies that may be used pursuant to this exigent situation in our scope. We did not assess DHS's determination as to which technologies may be subject to a warrant requirement or the exigent circumstances exception under the Fourth Amendment.

Figure 3: Technologies Owned or Accessed and Can Be Used in Public Spaces Without a Warrant, as Reported to GAO by Selected DHS Law Enforcement Agencies for Fiscal Year 2023



Source: GAO analysis of questionnaire responses from Department of Homeland Security (DHS) agencies. | GAO-25-107302

[a]DHS officials stated that some components refer to concealed body-worn cameras as "body wires" and use them for undercover purposes. They stated that the use of these technologies may require legal process, such as search warrants, which is addressed in consultation with prosecutors. In May 2023, DHS finalized a policy prohibiting body-worn cameras that are designed to be worn on the outside of clothing to be used for undercover purposes. DHS components were given 180 days to comply. See DHS Policy Statement 045-07 (May 22, 2023).

[b]Some U.S. Immigration and Customs Enforcement officers in select locations used non-concealed body-worn cameras as part of a pilot program in fiscal year 2023.

[c]According to DHS's cell-site simulator policy various types of exigent situations such as potential loss of life or destruction of evidence may justify a warrantless use of a cell-site simulator. DHS law enforcement agencies may initially use this technology without a search warrant but are to apply for a warrant within 48 hours. See DHS Policy Directive 047-02 (Oct. 19, 2015). As this technology could be used in public spaces without necessarily obtaining a warrant including during exceptional situations, we determined that this technology was within the scope of our review.

Appendix I presents a detailed listing of each of these technologies and includes brief descriptions of their capabilities.

Owned Technologies

In response to our standardized questionnaire, all three selected DHS law enforcement agencies reported owning or leasing the following technologies:

- **Pole cameras.** Pole cameras can be mounted on utility poles in public spaces and can conduct 24-hour observation and monitoring for a variable period of days. The cameras may be concealed so the public and the subject of investigation may not be aware that they are in use. The cameras may include zoom and panoramic capabilities and can transmit video back to law enforcement. Secret Service, for example, described using pole cameras to collect evidence of criminal activity and to support the agency's protection mission. Secret Service officials stated that a court order is required to use pole cameras in areas where there is a reasonable expectation of privacy.
- **Vehicles with detection, observation, and monitoring technologies.** These government vehicles can have a suite of technologies, such as cameras—including night vision, ground surveillance radars, laser range finders, laser illuminators, radar, and global positioning systems. CBP, for example, described using the technology to record law-enforcement encounters and other public interactions that may be of evidentiary value for arrest and seizure in civil or criminal cases.
- **Small drones.** These drones are also referred to as small, uncrewed aircraft systems. They are remotely operated aircraft that can be equipped with various cameras, thermal imaging devices, and radio frequency sensors. Small drones fly at lower altitudes and with less range than larger drones. According to agencies that deploy small drones, these can be used for law enforcement activities such as monitoring active shooter response, during undercover meetings with criminal suspects, and pre-operation planning.

DHS agencies reported to us that their technology acquisitions for fiscal year 2024 would be focused toward adding to their existing inventories rather than investing in new types of technologies. For example:

- CBP reported it planned to purchase aircraft and vessel registration number readers, audio recording devices; non-concealed body-worn cameras; small drones; pole cameras; and vehicles with detection, observation, and monitoring technology.
- The Secret Service reported it planned to purchase video-only cameras (e.g., closed-circuit television), small drones, and both mobile and fixed location automated license plate readers. In addition, Secret Service reported that it has plans to implement the use of a non-concealed body-worn camera program, but this will occur after fiscal year 2024.[42]
- ICE reported it implemented a non-concealed body-worn camera program during fiscal year 2024.

[42]A May 2022 Executive Order requires that all federal law enforcement agencies that regularly conduct patrols or routinely engage with the public in response to emergency calls shall have policies issued designed to ensure that cameras are worn and activated in all appropriate circumstances, including during arrests and searches. Such policies were to take effect as of August 2022. Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, Exec. Order No 14074, 87 Fed. Reg. 32,945, 32,955 (May 25, 2022).

Third-party Technologies

DHS law enforcement agencies reported to us that they also use detection, observation, and monitoring technologies from third-party entities, including private sector vendors and other law enforcement agencies in federal, state, or local governments.

As figure 3 above shows, all three DHS law enforcement agencies reported to us that they have agreements to query or view information from third-party automated license plate readers. Specifically, CBP and ICE reported to us they have subscriptions with a private sector vendor for this type of data. According to CBP's 2020 privacy impact assessment, the third-party automated license plate reader data provides CBP law enforcement personnel with access to a nationwide source of license plate data for their specific searches.[43] The agency identified the following benefits from the use of commercially aggregated automated license plate reader data:

- enhance both officer and public safety by enabling enforcement actions to occur in locations that minimize inherent dangers associated with encounters; and
- help identify viable leads for investigations.

As figure 3 also shows, Secret Service reported to us that it can both direct the use of, and query data from gunshot detection technology. Secret Service reported it has an agreement with the D.C. Metropolitan Police Department that allows it to direct the locations of its systems. Secret Service also reported that it views or queries gunshot detection information through the agency's subscription with the private sector vendor Shotspotter.

CBP also reported to us its plans to enter into agreements for third-party technologies in fiscal year 2024. Specifically, CBP reported that the agency planned to enter into agreements to direct the collection of information from third-party aircraft tail number readers, automated license plate readers, pole cameras, vehicles with detection, observation and monitoring capabilities, and video-only cameras. ICE and Secret Service reported that they had no plans for additional third-party technologies in fiscal year 2024.

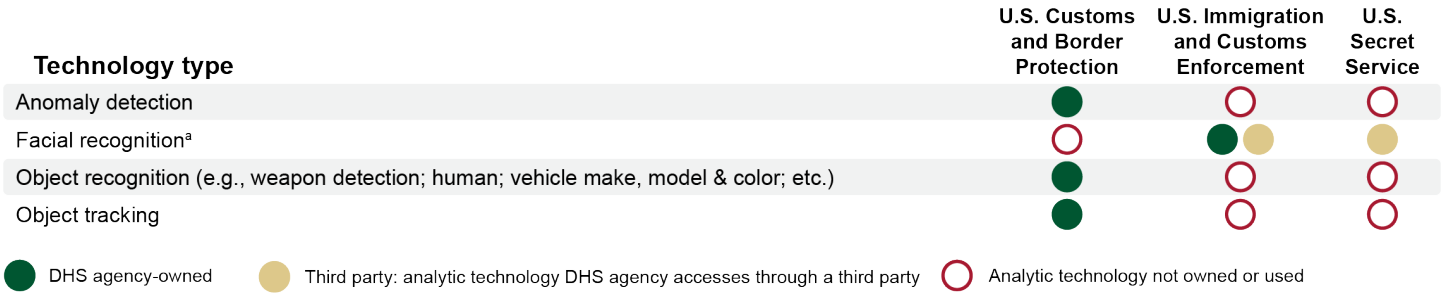
Agencies Report Owning and Accessing a Variety of Analytic Software

In response to our standardized questionnaire, the selected DHS agencies reported using a variety of analytic software systems, including some based on artificial intelligence (AI), that can enhance the capabilities of their

[43]Department of Homeland Security, Privacy Impact Assessment for the CBP License Plate Reader Technology DHS Reference No. DHS/CBP/PIA-049(a), July 6, 2020, (Washington, D.C.).

detection, observation, and monitoring technologies used in public spaces, as shown in figure 4.[44] Analytic capabilities may be built into a specific technology or may be independent software systems that can analyze information from various sources. For example, CBP's surveillance towers can automatically detect, classify, and track objects within view of its cameras. In contrast, Clearview AI, the third-party facial recognition service provider used by ICE, uses software to analyze photographs from various sources.

Figure 4: Analytic Software Owned or Accessed That Can Be Used on Information Collected in Public Spaces Without a Warrant, Reported to GAO by Selected DHS Law Enforcement Agencies for Fiscal Year 2023



Source: GAO analysis of questionnaire responses from Department of Homeland Security (DHS) agencies. | GAO-25-107302

[a]CBP uses facial recognition, but its use is outside of the scope of this review. For example, CBP reported to us using facial recognition on travelers seeking to enter or exit the United States. However, our scope does not include technologies or analytic software used at airports and ports of entry. We define public spaces as common outdoor areas or locations that are freely accessible to the general population, such as streets, highways, parks, beaches, and open space.

See appendix I for a listing of each of these technologies and includes brief descriptions of their capabilities.

Owned Analytic Software

DHS agencies reported to us that they owned four unique types of analytic software that use AI to enhance the capabilities of their detection, observation, and monitoring technologies. For example:

- **Object tracking.** CBP reported owning analytic software that can perform object tracking—the detection, identification, tracking, and classification of items of interest.
- **Anomaly detection.** CBP reported using this type of analytic software to automate threat recognition in streaming video, prerecorded video, or images. This can help reduce the amount of time agents spend reviewing images and video.

[44]For the purposes of our review, we defined analytic systems as technological tools or software programs that can perform computations of data and statistics for the purposes of evaluation, analysis, or prediction. We defined artificial intelligence (AI) based on section 238(g) of the Fiscal Year 2019 National Defense Authorization Act because, although there are various definitions for AI, this definition is incorporated into guidance issued by the Federal Chief Information Officers Council to all federal agencies for creating agency inventories of AI use cases. AI includes the following: (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets; (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action; (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks; (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task; or (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

- **Object recognition.** CBP reported using this analytic software. It can identify items of interest such as vehicles, firearms, explosives, humans, or animals by using existing video feeds.

CBP reported plans for investments in object recognition in fiscal year 2024. However, ICE and Secret Service did not report any investments of analytic systems for fiscal year 2024.

Third-party Analytic Software

In response to our standardized questionnaire, DHS law enforcement agencies reported accessing third-party facial recognition. For example, ICE subscribes to private sector facial recognition services, while Secret Service uses facial recognition services provided by DHS's Office of Biometric Identity Management. These DHS agencies stated they use facial recognition to identify an unknown individual captured in a photo as part of an authorized criminal investigation. They also used it to locate the whereabouts of a known individual as part of an authorized criminal investigation. Facial recognition is to be used for investigative leads and may not be used as the sole basis for law enforcement action, according to DHS policy.[45] DHS officials stated that facial recognition is not used to scan members of the general public.

For fiscal year 2024, CBP reported to us its plans to access object recognition and object tracking software systems through third-party arrangements. However, ICE and Secret Service did not report any investments of analytic software systems for fiscal year 2024.

DHS is Developing Policies and Procedures to Assess AI for Bias but Does Not Require Assessments for Other Detection, Observation, and Monitoring Technology

DHS is Developing Policies and Procedures to Assess AI Technologies for Bias

DHS has begun to develop department-wide policy, assessment capabilities, and training for employees for AI technology.[46] The policy would include detection, observation, and monitoring technologies using AI. In its 2024 AI Roadmap and a 2023 policy statement, DHS identified the following principles it would use to develop department-wide policy:[47]

- DHS will not collect, use, or disseminate data used in AI activities, or establish AI-enabled systems that make or support decisions, based on the inappropriate consideration of race, ethnicity, gender, national

[45]DHS, *Use of Face Recognition and Face Capture Technologies*, Directive 026-11 (Sept. 11, 2023).

[46]GAO has previously reviewed DHS's use of AI for cybersecurity and found that it had not fully implemented key practices to ensure the quality and reliability of data. GAO made eight recommendations to DHS, including that it (1) expand its review process to include steps to verify the accuracy of its AI inventory submissions and (2) fully implement key AI Framework practices such as documenting sources and ensuring the reliability of the data used. As of September 2024, the recommendations are open. See GAO, *Artificial Intelligence: Fully Implementing Key Practice Could Help DHS Ensure Responsible Use for Cybersecurity*, GAO-24-106246 (Washington, D.C.: Feb. 7, 2024).

[47]See DHS, *Artificial Intelligence: Roadmap 2024* (2024). The principles were originally included in DHS, Policy Statement 139-06, *Acquisition and Use of Artificial Intelligence and Learning Technologies by DHS Components* (Washington D.C.: Aug. 8, 2023).

origin, religion, sexual orientation, gender identity, age, nationality, medical condition, or disability. DHS will continually strive to minimize inappropriate bias utilizing standards required by law and policy.

- DHS will not use AI to improperly profile, target, or to discriminate against any individual, or entity, based on the individual characteristics identified above, as reprisal or solely because of exercising their Constitutional rights. DHS will not use AI technology to enable improper systemic, indiscriminate, or large-scale monitoring, surveillance, or tracking of individuals.

DHS established an AI Responsible Use Group led by the Office for Civil Rights and Civil Liberties (CRCL) to help with these efforts. CRCL officials stated that this group is advising on policy development and is in the process of identifying what additional project level policy and procedural guidance is needed to identify and mitigate risks—including bias—associated with AI. DHS has set a goal of issuing the guidance by the end of 2024.

DHS is also establishing processes to assess agencies' AI technology in order to help mitigate and manage the risk of bias. The assessment process is to include testing of the AI technology at different times in its lifecycle—including during the development period and to provide continuous monitoring once in use. DHS has set a goal of issuing a testing and evaluation action plan and standing up an AI test bed for providing independent assessments by the end of 2024.

DHS CRCL officials stated they are working collaboratively with AI experts and agency personnel to advise on these efforts. They said these efforts will help position DHS to fully implement the Office of Management and Budget guidance, which calls for impact assessments and ongoing monitoring of AI technology.[48] Additionally, DHS reported that it is planning to provide and expand training on AI technology. The training is to cover how to use the technology as well as associated risks, including bias.

These efforts are generally consistent with bias mitigation practices discussed by the subject matter experts we interviewed.[49] Subject matter experts from eight of the nine organizations we interviewed discussed practices to mitigate bias, including conducting assessments, providing training, and establishing policies on the use of the technology. Specifically:

- Subject matter experts from seven organizations identified assessments or audits as a practice to mitigate bias. These included both assessments of algorithms prior to use as well as post-deployment assessments or audits of performance in real world conditions to determine if there have been differential impacts on different groups.
- Subject matter experts from seven organization stated that training could help mitigate bias. For example, some subject matter experts said providing training on bias or training on the proper use and interpretation of data from the technologies could help.

[48]Office of Management and Budget, Memorandum M-24-10*: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Washington, D.C.: Mar. 28, 2024).

[49]We selected various organization types—to include law enforcement, privacy and civil liberties advocacy, public policy, and trade organizations—in order to obtain a range of perspectives. Specifically, we interviewed subject matter experts from the American Civil Liberties Union, the Brennan Center for Justice, the Cato Institute, the Commission on Accreditation for Law Enforcement Agencies, the Electronic Frontier Foundation, the Electronic Privacy Information Center, the International Association of Chiefs of Police, the International Biometrics and Identity Association, and the Project on Government Oversight. Subject matter experts' support for mitigation practices should not be seen as organizational support for the use of these technologies.

- Additionally, the subject matter experts from seven organizations highlighted how policies could help mitigate bias. For example, they highlighted policy elements such as having clear rules on the use of the technologies, supervisory requirements, penalties for misuse, and limits on the retention or use of data from the technologies as helping to mitigate bias. We discuss the extent to which the selected agencies have policies for these technologies later in this report.

It is too soon to assess DHS's efforts, but if fully implemented they could help DHS assess detection, observation, and monitoring technologies with AI for bias and mitigate effects on equity, civil rights, and civil liberties.

DHS and Selected Agencies Do Not Have Policies to Assess All Detection, Observation, and Monitoring Technology Use for Bias

While DHS is developing policies and procedures to help ensure that AI technologies are assessed for bias, it has no plans to develop such policies or procedures for other detection, observation, and monitoring technologies as it is not required to. CBP, ICE, and Secret Service stated that they do not have policies or procedures to assess their use of all detection, observation, and monitoring technology specifically for bias.[50] Instead, all three agencies pointed to other more general processes that could help ensure equitable treatment and protect civil rights and civil liberties. For example, CBP, ICE, and Secret Service officials stated they consult with their agency's privacy officials on technology acquisition and use. Additionally, DHS requires information systems to have a formal declaration called an "Authority to Operate," which requires a review by DHS's chief privacy officer, among other things.[51] CBP and Secret Service officials explained that they follow this requirement to use detection, observation, and monitoring technology.

Taking steps to protect privacy may help mitigate bias in certain cases, but protecting privacy is only one part of the overall civil liberties framework. Specifically, federal privacy protections provide certain safeguards that regulate the collection, maintenance, use, and dissemination of PII.[52] However, such protections do not necessarily protect against biased action that may be otherwise involved, consciously or not. For example, some subject matter experts we met with said that decisions about where to deploy technology could disparately impact certain communities. Subject matter experts we met with also said that bias could be introduced if law enforcement uses detection, observation, and monitoring technology to target surveillance of certain groups for lawful activism and First Amendment-protected activity, such as religious worship, protest, and dissent.

While DHS law enforcement agencies may seek out advice from CRCL on bias issues related to technology use, DHS does not require agencies to do so. For example, Secret Service is required by policy to conduct privacy impact assessments (PIA) for relevant technologies, but officials stated that they may consult with officials from CRCL and Secret Service's Office of the Chief Counsel on bias issues associated with technology. CRCL officials said that it is their goal to work with law enforcement agencies early in the technology lifecycle to identify and mitigate potential impacts on civil rights and civil liberties, including bias.

[50]For the purposes of this report, we are defining bias as a positive or negative preference for a group based on characteristics such as actual or perceived race, ethnicity, national origin, religion, or sex.

[51]The Authority to Operate is also designed to ensure agencies review system security requirements. DHS, *System Security Authorization Process Guide* (Apr. 4, 2019).

[52]See generally 5 U.S.C. § 552a.

However, they pointed out that while DHS requires agencies to conduct privacy reviews prior to using certain technologies, it does not require reviews for civil rights and civil liberties. Therefore, CRCL does not have policies and procedures in place to assess all detection, observation, and monitoring technologies for bias.

As a result, CRCL's level of review of detection, observation, and monitoring technologies has varied. CRCL officials said they use a range of policy advice and oversight tools. For example, CRCL officials reported directly supporting department and agency policy development for license plate readers, drones, facial recognition systems, and cell-site simulators. CRCL has also contributed to guidance on protecting civil rights, civil liberties, and privacy in drone programs. Additionally, CRCL may conduct a civil rights civil liberties impact assessment which allows CRCL to evaluate whether an agency's activities are resulting in differential impacts or chilling protected political or religious expression of particular groups, among other things, although CRCL has not conducted such an assessment recently.[53] However, CRCL officials acknowledged that they do not know all the technologies that DHS law enforcement agencies are using and that CRCL is facing workforce challenges.

While CRCL must operate within resource constraints, recent executive orders have articulated the need to prevent profiling and remedy discrimination.[54] Specifically, a May 2022 executive order notes the need for law enforcement agencies to take proactive measures to prevent profiling, including by ensuring that new law enforcement technologies do not exacerbate disparities based on actual or perceived race, ethnicity, national origin, religion, sex or disability.[55] Further, a February 2023 executive order requires that agencies comprehensively use their respective civil rights authorities and offices to prevent and address discrimination and advance equity for all.[56] By law and department policy, CRCL is responsible for the protection and promotion of civil rights and civil liberties across all department activities, which would include preventing inappropriate bias.[57] In addition, standards for internal control call for agencies to identify risks and design control activities, such as policies and procedures, to achieve their objectives and address related risks.[58]

Assessing detection, observation, and monitoring technologies for bias could help DHS address the provisions of the executive orders related to reducing disparities and discrimination. This is because, according to the subject matter experts and reports we reviewed, bias can affect how detection, observation, and monitoring technologies are used and lead to disparate impacts on certain communities or groups.

[53]Officials said that is has been a decade since CRCL has conducted a civil right civil liberties impact assessment. According to CRCL guidance, civil rights civil liberties impact assessments are a more thorough review that CRCL can conduct to evaluate whether an agency's activities are resulting in differential impacts or chilling protected political or religious expression of particular groups, among other things. However, civil rights civil liberties impact assessments are not required by law or DHS policy. DHS, *Instruction for the Office for Civil Rights and Civil Liberties*, Instruction 046-01-001, (Nov. 6, 2013). Officials said that these assessments are resource intensive.

[54]Exec. Order No. 14074, 87 Fed. Reg. 32,945 (May 25, 2022); Exec. Order No. 14091, 88 Fed. Reg. 10,825 (February 16, 2023). Of note, Executive Order 14091 also requires that agencies consider opportunities to increase the capacity, including staffing capacity, of their respective civil rights offices, in coordination with the Office of Management and Budget. Exec. Order No. 14091, 88 Fed. Reg. 10,825, 10,831 (February 16, 2023).

[55]Exec. Order No 14074, 87 Fed. Reg. at 32,946.

[56]Exec. Order No 14091, 88 Fed. Reg. 10,831.

[57]See generally 6 U.S.C. § 345(a) and DHS, *Instruction for the Office for Civil Rights and Civil Liberties* (Nov. 6, 2013).

[58]GAO-14-704G.

For example, in a 2024 report, the National Academies described how human and systemic biases can result in racial inequalities within the criminal justice system.[59] The report found that broadening systems of surveillance and enforcement contribute to racial inequality by increasing the likelihood of criminal justice contact among low-income Black or African American, Hispanic or Latino, and American Indian or Alaskan Native populations. The report explains that because there are high rates of residential segregation by race and income in the U.S., decisions about where to deploy police resources, along with police officers' perceptions of certain neighborhoods as having more crime, can lead to racial inequalities in initial contacts with police. These inequalities can be compounded as people move deeper into the criminal justice system.

Similarly, a Chicago Office of Inspector General's report concluded that the introduction of ShotSpotter gunshot detection technology changed the way Chicago police officers perceived and interacted with people in areas with more frequent ShotSpotter alerts.[60] Specifically, the report found that some police officers cited being in an area known to have frequent ShotSpotter alerts as an element of reasonable suspicion to justify a stop or to conduct "protective pat downs" during a stop.

While DHS has identified the need to address bias in technologies that use AI, by developing policies and procedures to assess and address bias related to DHS law enforcement agencies' other detection, observation, and monitoring technologies prior to their use, CRCL could help ensure these risks are mitigated before the technologies are deployed in public spaces. In addition, by applying these policies and procedures to assess and address the risk of bias posed by DHS law enforcement agencies' detection, observation, and monitoring technologies currently in use, CRCL could help ensure these technologies are not introducing bias and infringing on civil rights and civil liberties. Policies and procedures to assess and address bias risks could better position CRCL to use its limited resources effectively and determine the appropriate level of guidance and oversight based on risk.

DHS Has a Process to Consider Privacy Protections, but Its Technology Policies Do Not Always Address Them

Technology policies help ensure that agency officials using the technology understand how to implement privacy protections. However, the technology policies we reviewed at CBP, ICE, and the Secret Service did not always address key privacy protections.[61] According to Office of Management and Budget Circular A-130, agencies should use the Fair Information Practice Principles when evaluating information systems, processes, programs, and activities that affect individual privacy.[62] In addition, DHS's Privacy Policy Guidance Directive

[59]National Academies of Sciences, Engineering, and Medicine, *Reducing Racial Inequality in Crime and Justice: Science, Practice, and Policy*, (Washington, D.C.: 2023).

[60]City of Chicago Office of Inspector General, *The Chicago Police Department's Use of ShotSpotter Technology* (Chicago: Aug. 2021).

[61]We use the term "policies" here to refer to any technology policies, standard operating procedures, directives, or other documents that direct a user in how they are to use a technology. These policies may cover more than one technology but should make clear the expectations for the users of each technology.

[62]Office of Management and Budget, *Circular No. A-130, Managing Information as a Strategic Resource*.

memorializes the Fair Information Practice Principles as the foundational principles for privacy policy and implementation at DHS.[63]

We assessed whether technology policies at CBP, ICE, and the Secret Service addressed six key privacy protections: data collection, purpose specification, information sharing, data security, retention, and accountability, which are drawn from the Fair Information Practice Principles.[64] The following summarizes each privacy protection, as described in DHS's directive, and our assessment approach.

- **Data collection.** DHS should collect only PII that is directly relevant and necessary to accomplish the specified purpose(s). We assessed whether the policy for each technology states what information is or is not allowed to be collected.
- **Purpose specification.** DHS should specifically articulate the purpose(s) for which the PII is intended to be used. We assessed whether the policy states how the information or technology is or is not to be used.
- **Information sharing.** Sharing PII outside the department should be for a purpose compatible with the purpose for which the information was collected. We assessed whether the policy states under what conditions the agency is allowed to share information collected by the technology.
- **Data security.** DHS should protect PII through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. We assessed whether the policy identifies security safeguards.
- **Data retention.** DHS should only retain PII for as long as is necessary to fulfill the specified purpose(s). We assessed whether the policy specifies what information will be retained and for how long.
- **Accountability.** DHS should be accountable for complying with these principles, including by auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements. We assessed whether the policy includes information on audits or supervisory review to ensure compliance with applicable privacy protection requirements.

The technology policies we reviewed varied in the extent to which they addressed these protections, but most did not address all six protections.[65] For example,

- CBP's policies for non-concealed body-worn cameras addressed all six protections. However, CBP's policy for pole cameras did not address any of the six protections.
- ICE's policies for automated license plate readers addressed all six protections. However, ICE's policy for pole cameras addressed two of the six protections.
- The Secret Service's policy for counter-uncrewed aircraft systems addressed five of six protections but did not address data security. However, the Secret Service's policy for concealed body-worn cameras addressed one of six protections (data collection).

[63]Department of Homeland Security, Privacy Office, *Policy Directive 140-03, Privacy Policy Guidance Memorandum* (December 29, 2008).

[64]We selected these six privacy protections from the Fair Information Practice Principles because they most directly addressed our research question on policies and procedures to limit the collection and use of information from these technologies. For more information about our selection, see the discussion of our methodology in the introduction of this report.

[65]We considered a protection to be addressed if the policy discussed the protection to any degree.

Figure 5 below presents the extent to which use policies for each technology addressed the protections in the Fair Information Practice Principles we assessed.

Figure 5: Assessment of Technology Policies against Selected Privacy Protections

	Collection	Purpose	Sharing	Security	Retention	Accountability
U.S. Customs and Border Protection						
Aerostats, airship, or balloon	○	○	○	○	○	○
Aircraft (piloted)	●	●	●	●	●	●
Aircraft tail number reader	●	●	●	●	●	●
Automated license plate reader – fixed location	●	●	●	●	●	●
Automated license plate reader – mobile	●	●	●	●	●	●
Body-worn cameras – not concealed	●	●	●	●	●	●
Counter-uncrewed aircraft system equipment	●	●	●	○	●	●
Drones (uncrewed aircraft systems): large – over 55 pounds	●	●	●	●	●	○
Drones (uncrewed aircraft systems): small – under 55 pounds	●	●	●	●	●	●
Linear ground detection system	○	○	○	○	○	○
Pole camera	○	○	○	○	○	○
Radio frequency collection	●	●	●	●	●	○
Surveillance tower	○	○	○	○	○	○
Vehicle with detection, observation, and monitoring technology (e.g., car, truck, RV, van, etc.)	●	●	●	●	●	●
U.S. Immigration and Customs Enforcement						
Automated license plate reader – fixed location	●	●	●	●	●	●
Body-worn cameras – concealed (e.g. body wire)	●	●	○	○	○	○
Cell-site simulator, or “International Mobile Subscriber Identity” (IMSI) catcher	●	●	●	○	●	●
Drones (uncrewed aircraft systems): small – under 55 pounds	●	●	●	●	●	○
Facial recognition	●	●	●	○	○	●
Pole camera	●	●	○	○	○	○
Vehicle with detection, observation, and monitoring technology (e.g., car, truck, RV, van, etc.)	●	●	○	○	○	○
U.S. Secret Service						
Aerostats, airship, or balloon	●	●	●	●	●	●
Audio recording device	●	●	●	○	●	●
Automated license plate reader – fixed location	●	●	●	●	○	●
Automated license plate reader – mobile	●	●	●	●	○	●
Body-worn cameras – concealed (e.g. body wire)	●	○	○	○	○	○
Counter-uncrewed aircraft system equipment	●	●	●	○	●	●
Drones (uncrewed aircraft systems): small – under 55 pounds	●	●	●	●	●	●
Facial recognition	●	●	●	○	●	○
Gunshot detection	○	○	○	○	○	○
Pole camera	●	●	●	●	●	●
Surveillance tower	●	●	●	●	●	●
Traffic video	○	○	○	○	○	○
Vehicle with detection, observation, and monitoring technology (e.g., car, truck, RV, van, etc.)	●	●	●	○	●	○
Video-only camera mounted to building exterior or other structure (e.g., closed-circuit television)	●	●	●	●	●	●

● Addressed ○ Not addressed

Source: GAO analysis of Department of Homeland Security policies. | GAO-25-107302

Note: The privacy protections are drawn from the Fair Information Practice Principles. Technology policies may include standard operating procedures, directives, or other documents that direct a user in how they are to use a technology. We did not include privacy impact assessments in this analysis as they are not policies that instruct users in how to use a technology. We considered a protection to be addressed if the policy discussed the protection to any degree.

Officials from CBP, ICE, and the Secret Service stated that they consider the Fair Information Practice Principles and demonstrate how they intend to protect privacy when using these technologies in each PIA, as required by DHS guidance.[66] They noted that PIAs are publicly available, and the DHS employees who use the technologies could access them.[67] However, having end users rely on the public PIAs to understand how they are to operationally implement key privacy protections when using a particular technology presents challenges. For example:

- Due to the public nature of the PIAs, they may lack the level of detail that could be included in an internal policy. For example, privacy officials from the DHS law enforcement agencies stated that to protect law enforcement sensitive information, PIAs may not provide detailed information on technologies.
- PIAs may not always name specific systems or technologies so that the PIAs do not need to be updated whenever the technology changes names.
- A single PIA may cover multiple technologies and not delineate each technology in use, making it difficult for the end user to identify whether the technology in question is covered by a particular PIA. For example, ICE has one PIA that covers its use of automated license plate readers, cell-site simulators, concealed body-worn cameras, pole cameras, small drones, and vehicles with detection, observation, and monitoring technology.

Officials also stated that they have higher-level policies that address certain privacy protections across technologies. For example, DHS has a handbook for safeguarding sensitive PII that addresses data security and information sharing. We found, however, that these general policies were not always identified in technology policies, meaning an end user would have to be aware of and consult multiple different policies to identify all the privacy protections applicable to a particular technology.[68]

Technology policies protect privacy by guiding and instructing end users when using a given technology. Detection, observation, and monitoring technologies collect a wide variety of information, so the specifics of what a user needs to know and do can vary by technology. For example, ICE's policy for automated license plate readers addresses the data collection protection by stating that ICE law enforcement personnel may place license plate reader cameras at locations relevant to a particular investigation, for instance, along a known smuggling route or outside a business where an investigative target is known to frequent. The Secret Service's facial recognition policy addresses data retention by stating that search results that cannot be validated through other investigative techniques are not to be retained in any format. Such technology policies make it easier for users to know what they should be doing, including by linking to other, more general policies.

[66]The E-Government Act and DHS policy require the DHS Privacy Office to complete a PIA before DHS develops or procures technology that collects, maintains, or disseminates PII to ensure that the agencies have sufficient privacy protections as they use the technologies. See § 208, 116 Stat. at 2921; DHS, Privacy *Office, Privacy Impact Assessments: Privacy Office Official Guidance,* (Washington, D.C.: June 2010*)*. The Homeland Security Act also provides that the Chief Privacy Officer is to assume the primary responsibility for privacy policy, including assuring that the use of technologies employed at DHS sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information. See Pub. L. No. 107-296, § 222(1), 116 Stat. 2135, 2155 (2002).

[67]We found that CBP, ICE, and the Secret Service had PIAs for all the technologies included in our review.

[68]For the purpose of our analysis, we considered a protection addressed if a technology policy referenced a higher-level policy that covered the respective protection.

Making requirements transparent and easily accessible also allows agencies to hold users accountable if they do not implement the required privacy protections.

DHS's privacy policy states that program managers, in coordination with the agency privacy officer, are responsible for developing and implementing privacy procedures to safeguard PII in program and system operations.[69] Further, according to *Standards for Internal Control in the Federal Government*, management should implement control activities through policies.[70] Specifically, management is to document in policy each unit's responsibility for an operational process's objectives and related risks. In effect, technology policies are needed to direct employees in how they are to operationally implement key privacy protections when using a particular technology. CBP, ICE, and the Secret Service could have better assurance that employees are implementing privacy protections by requiring that technology policies for each detection, observation, and monitoring technology address the key privacy protections from the Fair Information Practice Principles. Agencies could still address some privacy protections through broader policies, but referencing these in the technology policies would help ensure technology users are aware of their responsibilities to protect privacy and the policies they are to follow.

Conclusions

DHS employs the most federal law enforcement officers and is responsible for a broad array of law enforcement activities. DHS law enforcement agencies are using a variety of technologies, such as license plate readers, gunshot detection, and pole cameras, to help them detect and solve crimes. However, the use of these technologies in public spaces raises questions about bias and the effects on civil rights, civil liberties, and privacy. While DHS is taking steps to help ensure AI technologies are assessed for bias, there are no such requirements for other detection, observation, and monitoring technologies.

By developing policies and procedures to assess and address bias and associated civil rights and civil liberties risks related to technologies prior to their use, CRCL could help ensure these risks are mitigated before the technologies are deployed in public spaces. Further, by applying these policies and procedures to assess and address the risk of bias posed by DHS law enforcement agencies' detection, observation, and monitoring technologies currently in use, CRCL could help ensure these technologies are not introducing bias and infringing on civil rights and civil liberties.

DHS agencies we reviewed—CBP, ICE, and the Secret Service—have taken the important step of conducting a PIA for all the detection, observation, and monitoring technology we reviewed. However, while each agency identified how it intended to address the Fair Information Practice Principles in its technology PIAs, these agencies' implementing policies did not always capture how technology users were to do so in practice, which could result in the unintended use and sharing of protected information. By requiring that technology policies for each detection, observation, and monitoring technology address the key privacy protections from the Fair Information Practice Principles, DHS agencies could have better assurance that employees are implementing these protections when using these technologies. While agencies could still address some privacy protections through broader policies that are not technology specific, referencing these in the technology policies would

[69]Department of Homeland Security, *Privacy Policy and Compliance,* Instruction Number 047-01-001 (July 25, 2011).

[70]GAO-14-704G.

help ensure technology users are aware of their responsibilities to protect privacy and the policies they are to follow.

Recommendations for Executive Action

We are making the following five recommendations to DHS. The Secretary of Homeland Security should ensure that:

The Officer for Civil Rights and Civil Liberties develop policies and procedures to assess and address bias risks for DHS law enforcement agencies' detection, observation, and monitoring technologies prior to their use. (Recommendation 1)

The Officer for Civil Rights and Civil Liberties apply the policies and procedures to assess and address bias risks to DHS law enforcement agencies' detection, observation, and monitoring technologies currently in use. (Recommendation 2)

The Commissioner of CBP require each detection, observation, and monitoring technology policy to address the privacy protections in the Fair Information Practice Principles. (Recommendation 3)

The Director of ICE require each detection, observation, and monitoring technology policy to address the privacy protections in the Fair Information Practice Principles. (Recommendation 4)

The Director of the Secret Service require each detection, observation, and monitoring technology policy to address the privacy protections in the Fair Information Practice Principles. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. In its comments, reproduced in appendix II, DHS concurred with the recommendations and provided information on its planned actions. However, ICE and Secret Service described actions that do not address our recommendations. DHS's comments are summarized below.

With regard to recommendations 1 and 2, DHS concurred and stated CRCL would develop guidance to ensure that bias risks associated with detection, observation, and monitoring technologies are assessed and appropriately mitigated. If implemented effectively, these actions would address our recommendations.

With regard to recommendation 3, DHS concurred and stated CBP would take steps to ensure that the technology policies we reviewed addressed all of the key privacy protections. These actions are consistent with our recommendation. To fully address the recommendation, CBP should require that detection, observation, and monitoring technologies it acquires in the future have use policies that address the privacy protections in the Fair Information Practice Principles.

With regard to recommendations 4 and 5, DHS concurred but ICE and Secret Service stated that their current policies and processes address the recommendation and requested the recommendations be considered implemented. Specially, both ICE and Secret Service stated that privacy protections for these technologies are

addressed in privacy impact assessments (PIA) and/or privacy threshold analyses. However, as we note in this report, while PIAs provide the public with information about how the agencies intend to manage privacy risks, they do not provide agency employees with specific guidance on how to use these technologies in a way that ensures privacy is protected. We therefore maintain that a requirement to address the Fair Information Practice Principles in technology use policies would be beneficial.[71]

Further, Secret Service stated that, with regard to technologies managed or maintained by third parties, its privacy program reviews company terms of service to ensure that their policies align with the Fair Information Practice Principles and evaluates them using its PIA and privacy threshold analysis processes. The agency further noted that creating a separate analysis for these services would be duplicative and that adherence to the Fair Information Practice Principles falls on the third parties managing these technologies and information. However, federal agencies retain responsibility for ensuring that their employees use technologies provided by third parties in a manner that is consistent with privacy requirements. Indeed, we found that Secret Service's technology use policies for third-party systems did not always address the key privacy protections in the Fair Information Practice Principles, indicating additional action is needed. Such policies are needed to direct employees in how they are to operationally implement key privacy protections when using a particular technology. Accordingly, we continue to believe that technology use policies are needed at Secret Service to help ensure that agency staff using the technology—including third-party technologies—understand what privacy protections are required and how to effectively implement them.

Secret Service also pointed to other steps it takes to address privacy concerns, including oversight over acquisitions and privacy training. We agree that these actions can help ensure that privacy protections are considered and implemented. However, privacy protections should still be documented and implemented through technology policies, as our recommendation calls for.

Documentation of responsibilities through policies is a cornerstone of federal internal control standards and helps ensure program objectives are achieved and risks are addressed.

DHS also provided technical comments, which we incorporated as appropriate.

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

If you or your staff have any questions about this report, please contact 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 major contributions to this report are listed in appendix III.

[71]In the agency comments, Secret Service stated that its policy and PIA for body-worn cameras fully address the key privacy protections in the Fair Information Practice Principles. However, the policy and PIA Secret Service referenced were for non-concealed body-worn cameras, which Secret Service officials stated they did not use or own in fiscal year 2023 and were therefore not the subject of our assessment. Instead, Secret Service reported using "body wires" as concealed body-worn cameras. Our assessment of policies related to the Secret Service's use of body wires found that one of six privacy protections in the Fair Information Practice Principles was addressed.



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 Cory A. Booker
Chair
Subcommittee on Criminal Justice and Counterterrorism
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 Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives
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: Department of Homeland Security Law Enforcement Technology

The following is a list and brief descriptions of the detection, observation, and monitoring technologies and analytic software systems that the three selected Department of Homeland Security (DHS) law enforcement agencies reported owning or accessing since 2023.[1] Further, according to these agencies, these technologies could be used in public spaces without a warrant; this includes technologies used during exceptional situations which may justify the warrantless use of a technology.[2] The information below was compiled from selected DHS law enforcement agencies' responses to our questionnaire and the policies, guidance, and privacy compliance documents they provided, as well as our own literature review and interviews with subject matter experts.

[1]For the purposes of our review, these are technologies—hardware such as audio, images, video, radar, thermal imaging, cellphone subscriber identity and location, chemical or biological detection, and other sensors—that can capture or use data that is reasonably likely to identify individuals or an activity or action when used singly, or in combination with other information or tools to analyze the data collected by these technologies. In addition, we defined "third parties" to include both commercial vendors and other federal, state, tribal, territorial, and local agencies. To be included, the DHS agency must have a written agreement that provides for access to a third party's technology, such as a memorandum of agreement, contract, or subscription. We defined analytic systems as technological tools or software programs that can perform computations of data and statistics for the purposes of evaluation, analysis, or prediction.

[2]According to DHS policy, various types of exigent or exceptional situations such as potential loss of life or destruction of evidence, may justify a warrantless use of a technology. DHS law enforcement agencies may initially use such technology without a search warrant but are to apply for a warrant within 48 hours. We have included this exigent situation in the scope of our identification of technologies.

Figure 6: Department of Homeland Security (DHS) law enforcement technologies and analytic software systems owned or accessed and can be used in public spaces without a warrant, fiscal year 2023

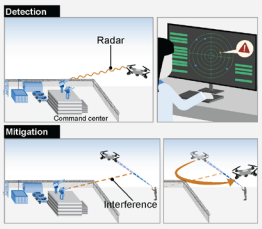
Figure 6: Department of Homeland Security (DHS) law enforcement technologies and analytic software systems owned or accessed and can be used in public spaces without a warrant, fiscal year 2023

TECHNOLOGY TYPE	DESCRIPTION | FEATURES	DHS AGENCIES : OWN OR USE
Aerostats, airship, or balloon 	Also known as rapid aerostat initial deployment, persistent ground surveillance system, tethered aerostat radar system, and persistent threat detection system. Aerostats can provide persistent ground surveillance aloft up to 10,000 ft. These can be equipped with high-resolution, 360-degree video and infrared cameras that vary in size and altitude of operation. The aerial surveillance provided by aerostats can provide a better angle to view items of interest and allow agencies to have a broader surveillance range than ground-based cameras.	U.S. Customs and Border Protection U.S. Secret Service
Aircraft (piloted)	Includes several types of piloted aircraft including helicopters and fixed-wing aircraft. These aircraft may be equipped with video, radar, and sensor technologies to assist in conducting surveillance for law enforcement investigations or tactical operations and patrolling the border.	U.S. Customs and Border Protection
Aircraft tail number reader 	Also known as aircraft tail number recognition. Camera with embedded software that recognizes a nation's issued identification numbers (e.g., the U.S. Federal Aviation Administration, or Transport Canada) stenciled on the exterior of every aircraft. The software collects other aircraft ID metadata such as country, type, time, date, GPS position, the full and sub-image of the code, and the position of the code within the original image.	U.S. Customs and Border Protection
Anomaly detection	An analytic capability that can identify deviations by looking for activity that is different from normal behavior. This includes artificial intelligence (AI)-enabled commercially available off-the-shelf systems capable of tracking and classifying items of interest. This tool can use still photos or video, and can be integrated with audio, infrared cameras, or radar capabilities.	U.S. Customs and Border Protection
Audio recording device	These devices record audio on specific subjects of relevance during an authorized investigation to collect evidence of criminal activity. For example, U.S. Secret Service officials stated these are body-worn devices (sometimes referred as body wires) with microphones for audio collection. If there is reasonable expectation of privacy, a court order or warrant may be required, which is addressed in consultation with prosecutors, according to DHS officials.	U.S. Customs and Border Protection U.S. Secret Service
Automated license plate reader – fixed location 	License plate readers automate a normally manual, labor-intensive process. Computer-controlled cameras are mounted to fixed locations and automatically capture all license plates that come into view along with locations, dates, times, and photographs. This information is loaded onto a server, checked for warrants, and can be retained to aid in criminal investigations. In addition to license plates, automated license plate readers can capture photographs of cars, drivers, and passengers. This information is uploaded to a database where it can be analyzed to study movements, associations, and relationships to crimes.	U.S. Customs and Border Protection U.S. Immigration and Customs Enforcement U.S. Secret Service

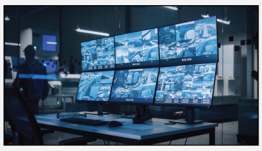
Page 38 GAO-25-107302 DHS Law Enforcement

TECHNOLOGY TYPE	DESCRIPTION | FEATURES	DHS AGENCIES : OWN OR USE
Automated License Plate Reader – mobile	License plate readers automate a normally manual, labor-intensive process. Computer-controlled cameras are mounted on specially equipped mobile units and automatically capture all license plates that come into view along with locations, dates, times, and photographs. This information is loaded onto a server, checked for warrants, and can be retained to aid in criminal investigations. In addition to license plates, automated license plate readers can capture photographs of cars, drivers, and passengers. This information is uploaded to a database where it can be analyzed to study movements, associations, and relationships to crimes.	U.S. Customs and Border Protection U.S. Secret Service
Body-worn cameras – concealed (e.g., body wires)	Used in support of authorized criminal investigations to collect evidence of criminal activity. Specifically, body-worn devices (sometimes referred as body wires) come with video cameras and microphones for audio collection. If there is reasonable expectation of privacy a court order or warrant may be required, which is addressed in consultation with prosecutors, according to DHS officials.	U.S. Immigration and Customs Enforcement U.S. Secret Service
Body-worn cameras – not concealed 	Body cameras are used to record an officer's interactions with the public and store the video for future review or use in criminal or civil proceedings. Body cameras were originally developed and used by police agencies for accountability to the public during police-public interactions. Some video records have also been useful in criminal investigation and raw information collection. In May 2023, DHS finalized a policy prohibiting body-worn cameras that are designed to be worn on the outside of clothing to be used for undercover purposes. DHS components were given 180 days to comply. See DHS Policy Statement 045-07 (May 22, 2023).	U.S. Customs and Border Protection
Cell-site simulator 	Also known as "Stingrays" "dirtbox" (DRT box), or "international mobile subscriber identity" (IMSI) catchers. Cell-site simulators permit the tracking of cellphones during criminal investigations. The cell-site simulators will simulate actual cellphone towers (cell sites) that register all active cellphones within range so the simulator can log the dates, times, locations, and identifying numbers of cell phones in the area. Some devices have the capability to intercept communications; however, DHS policy requires that cell-site simulators used by the Department's law enforcement agencies be configured so that they do not collect the contents of any communication.[3]	U.S. Immigration and Customs Enforcement U.S. Secret Service

[3] DHS agencies reported that the use of cell site simulator technologies are covered by a October 2015 DHS policy Directive 047-02, whereby DHS law enforcement components must first obtain a search warrant supported by probable cause pursuant to Rule 41 of the Federal Rules of Criminal Procedure; or must also apply within 48 hours, as required by 18 U.S.C. § 3125, under exigent or exceptional circumstances such as the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice. Even under exigent circumstances, an exception to the Fourth Amendment's warrant requirement, law enforcement agencies must still comply with 18 U.S.C. § 3121, et seq.

TECHNOLOGY TYPE	DESCRIPTION | FEATURES	DHS AGENCIES : OWN OR USE
Counter-uncrewed aircraft system (UAS) equipment 	Counter-UAS (drone) technologies generally fall into two categories: detection and mitigation. Detection technologies can include radar systems, radio frequency detection, infrared devices to track heat signatures, radio frequency systems to scan for control signals, and acoustic methods to recognize the unique sounds produced by a drone's motors. Mitigation technologies can repel, intercept, and/or destroy a drone posing a credible threat to a covered facility or asset. For example, interference signals can jam or break the communications connection between the drone and its operator, which can trigger the drone to land or return to its operator. Other mitigation capabilities can include jamming radio frequencies or GPS, and projectiles to disable or destroy the drone or seize operational control.	U.S. Customs and Border Protection U.S. Secret Service
Cross-border tunnel threat	Technologies provide capabilities for detection and disruption of cross border tunnel threats and other subterranean activity.	U.S. Customs and Border Protection
Drones - Large (uncrewed aircraft systems) - over 55 pounds 	Also known as Uncrewed Aircraft Systems (UAS) or Uncrewed Aerial Vehicles (UAVs). Large drones are remotely operated aircraft — ranging in size — that can be equipped with various cameras, sensors, and other devices. These systems can deploy cameras capable of facial recognition and can also contain GPS trackers and cell-site simulator devices. For example, U.S. Customs and Border Protection's large drone aircraft are equipped with video and radar sensors primarily to provide intelligence, surveillance, and reconnaissance capabilities, such as full-motion video, radar images of terrain, structures and moving objects.	U.S. Customs and Border Protection
Drones - Small (uncrewed aircraft systems) - under 55 pounds 	Also known as Uncrewed Aircraft Systems (UAS) or Uncrewed Aerial Vehicles (UAVs). These are remotely operated aircraft that can be equipped with various cameras, sensors, and other devices. These devices fly at lower altitudes and with less range than large drones. These provide highly mobile, hand-launched fixed-wing uncrewed aircraft systems or vertical take-off multi-rotor systems. Small drones can be equipped with video surveillance systems, rangefinders, thermal imaging devices, and radio frequency sensors.	U.S. Customs and Border Protection U.S. Immigration and Customs Enforcement U.S. Secret Service
Facial recognition 	Analytical tool that enables the automated searching of a facial image (probe) against a gallery of photos to determine if there are potential matches. This automated process is commonly referred to as a one-to-many comparison. Facial recognition technology uses specialized algorithms to analyze human faces captured in photographs or video footage. Law enforcement officials can also use this technology to help identify a victim in a photo or video.	U.S. Immigration and Customs Enforcement U.S. Secret Service

TECHNOLOGY TYPE	DESCRIPTION | FEATURES	DHS AGENCIES : OWN OR USE
Gunshot detection	This technology uses audio sensors to pick up sounds that appear to be gunshots within the radius of the unit. Audio snippets are automatically sent to a private sector vendor who attempts to verify whether the sound represents a shooting.	U.S. Secret Service
Linear ground detection	Performs detection and identification of items of interest by collecting seismic and acoustic sensor data, using fiber optic detection and identification capabilities that are scalable and deployable across all environments. For example, Customs and Border Protection reported that its program fills current gaps in the surveillance capability, improving upon the current in-ground system (Unattended Ground Sensor).	U.S. Customs and Border Protection
Object recognition (e.g., weapon detection, human, vehicle make, model and color, etc.)	A high-level automated identification of items of interest such as a vehicle, human, or animal in existing remote video surveillance system camera feeds. This tool can be used for detection, identification, tracking, classification, and mitigation of items of interest.	U.S. Customs and Border Protection
Object tracking	Object tracking software is used to identify objects in an image or video. Software may include algorithms use advanced machine-learning to detect objects based on, for example, size, shape, color, texture, location, and other features. Used for detection, identification, tracking, classification, and mitigation of items of interest, such as small drones. They are primarily radio frequency detectors and can be integrated with audio, night vision cameras, or radar capabilities.	U.S. Customs and Border Protection
Pole camera 	Cameras that can be mounted on utility poles in public spaces that can conduct 24-hour surveillance for a variable period of days or months. Cameras may be concealed so the public or subject of investigation is not aware that they are there.	U.S. Customs and Border Protection U.S. Immigration and Customs Enforcement U.S. Secret Service
Radio Frequency (RF) Collection	A radio frequency sensor is designed to passively detect radio frequency signals and power, usually operating within a specific range. This technology intercepts radio communications on high frequency, very high frequencies, and ultra high frequencies, enabling law enforcement officials to log the location of transmission, code names, and code words to log suspicious activity, along with date, time, frequency, and location of the event.	U.S. Customs and Border Protection
Surveillance tower 	Surveillance towers allow officers to monitor areas from several stories above street level as well as record movements within a targeted area. Towers can be relocated and equipped with, among other things, ground surveillance radars, multiple color and infrared cameras, and onboard artificial intelligence that autonomously alerts operators of illicit activity.	U.S. Customs and Border Protection U.S. Secret Service

TECHNOLOGY TYPE	DESCRIPTION | FEATURES	DHS AGENCIES : OWN OR USE
Traffic video 	An analytic system that provides subscribers with incident assessment and situational awareness by providing network publicly-accessible highway traffic camera displays across multiple jurisdictions.	U.S. Secret Service
Unattended Ground Sensors	Covertly deployed sensors that can be frequently relocated, and are used to detect, identify, and track threats and activity in the area of operations. Provides detection, identification, classification, and tracking of items of interest using seismic and acoustic sensor data. This technology is mobile and can be carried and used by, for example, Border Patrol Agents in areas where fixed and vehicle-mounted solutions are not feasible or appropriate.	U.S. Customs and Border Protection
Vehicle with detection, observation, and monitoring technology (e.g., car, truck, RV, van, etc.) 	Also known as mobile surveillance capability, and mobile video surveillance system (within U.S. Customs and Border Protection). Government vehicles can provide a suite of radars, day or night cameras, ground surveillance radars, laser range finders, laser illuminators, GPS, and a command, control, and communication system.	U.S. Customs and Border Protection U.S. Immigration and Customs Enforcement U.S. Secret Service
Video-only camera mounted to building exterior or other structure (e.g., closed-circuit television) 	Current closed-circuit television technology has enhanced power and scope, including night vision cameras, computer-assisted operations, and motion detectors. A camera that is integrated with a motion detection system could, for example, alert law enforcement staff in a control room to remotely investigate potential security incidents such as a terrorist placing a package in an isolated location.	U.S. Customs and Border Protection U.S. Secret Service

Additional Source Information for Images, Tables, or Figures

This appendix contains credit, copyright, and other source information for images, tables, or figures in this product when that information was not listed adjacent to the image, table, or figure.



Sources from top to bottom

Page 38: GAO (balloon); GAO (tail number); Thrimage/stock.adobe.com (license plate)

Page 39: Skyward/stock.adobe.com (body-worn camera); GAO (cell-site simulator)

Page 40: GAO (counter-uncrewed aircraft); Jules/stock.adobe.com (drone-large); Tartila/stock.adobe.com (drones-small); Gorodenkeff/stock.adobe.com (facial recognition)

Page 41: Lucia/stock.adobe.com (pole camera); Youm/stock.adobe.com (surveillance tower)

Page 42: Vector Tradition/stock.adobe.com (traffic video); Josh Denmark, U.S. Immigration and Customs Enforcement (vehicle with detection); Gorodenkeff/stock.adobe.com (video-only camera mount)

Appendix II: Comments from the Department of Homeland Security

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

By Electronic Submission

October 30, 2024

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

Re: Management Response to Draft Report GAO-25-107302, “LAW ENFORCEMENT: DHS Could Better Address Bias Risk and Enhance Privacy Protections for Technologies Used in Public”

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) planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO’s recognition that the Department is developing policies and procedures to address the risk of bias in technologies that involve Artificial Intelligence. The Department, through the DHS Office of Civil Rights and Civil Liberties (CRCL), remains committed to mitigating bias issues as it relates to DHS’s use of detection, observation, and monitoring technologies by providing guidance and oversight for the protection of individuals' civil rights and civil liberties.

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

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

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Enclosure

Enclosure: Management Response to Recommendations Contained in GAO-25-107302

GAO recommended that the Officer for CRCL:

Recommendation 1: Develop policies and procedures to assess and address bias risks for DHS law enforcement agencies' detection, observation, and monitoring technologies prior to their use.

Response: Concur. CRCL will continue to work with DHS Components, including the

U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), and the U.S. Secret Service, as well as headquarters offices, as appropriate, to ensure oversight of detection, observation, and monitoring technologies. Specifically, CRCL's Security, Intelligence, and Information Policy section (SIIP) will seek law enforcement Component' inputs and perspectives, as appropriate, when leading the creation of guidance for DHS law enforcement agencies to ensure that the use of these technologies does not introduce bias, prevents potential infringement of individuals' civil rights and civil liberties, and that bias risks are assessed and appropriately mitigated. Estimated Completion Date (ECD): September 30, 2025.

Recommendation 2: Apply the policies and procedures to assess and address bias risks to DHS law enforcement agencies' detection, observation, and monitoring technologies currently in use.

Response: Concur. Once CRCL SIIP creates the guidance needed to assess and address bias risks for DHS law enforcement agencies' use of detection, observation, and monitoring technologies by the end of September 2025, SIIP will then work with other DHS Component stakeholders , as appropriate, to implement this guidance within each Component and across the joint enterprise. Once implemented, this guidance should ensure that the use of these technologies does not introduce bias or potential infringement on individuals' civil rights and civil liberties. Further, this guidance should ensure that bias risks are identified, assessed, and appropriately mitigated. ECD: March 31, 2026.

GAO recommended that the Commissioner of CBP:

Recommendation 3: Require each detection, observation, and monitoring technology policy to address the privacy protections in the Fair Information Practice Principles [FIPP].

Response: Concur. CBP's Privacy and Diversity Office (PDO) will coordinate with program owners and operational offices responsible for each of the six law enforcement technologies used by CBP that do not currently have a specific privacy policy (or have a policy which does not have a privacy principle discussed in GAO's draft report) to assist in the development of internal guidance documents, as appropriate. Once developed, these documents will address any outstanding privacy principles noted by this audit for those six technologies. ECD: October 31, 2025.

GAO recommended that the Director of ICE:

Recommendation 4: Require each detection, observation, and monitoring technology policy to address the privacy protections in the [FIPP].

Response: Concur. ICE agrees with the importance of ensuring that privacy protections in the FIPPs1 are addressed in policies governing use of surveillance technologies.

Accordingly, ICE follows a statutorily-and-policy2-defined privacy process guided by the FIPPs that aligns the policy framework and ICE program office processes for the use of detection, observation, and monitoring technology tools. The standardized process for embedding privacy protections into operational functional tasks is systemically applied across surveillance technologies usage, and currently guides the development of policies associated with these technologies. ICE will continue to incorporate the FIPPS into stakeholder development documents associated with such tools through this established process on an ongoing basis. We request that GAO consider this recommendation resolved and closed, as implemented.

GAO recommended that the Director of the Secret Service:

Recommendation 5: Require each detection, observation, and monitoring technology policy to address the privacy protections in the Fair Information Practice Principles.

Response: Concur. The Secret Service agrees with the importance of addressing the critical issues highlighted in this recommendation, and already has in place the following activities that meet the spirit and intent of this recommendation. Specifically, the Secret Service's Office of Intergovernmental and Legislative Affairs' Privacy Program addresses and implements the FIPPs in agency use of technology via: (1) the Privacy Impact Assessment (PIA) compliance process; (2) office inspection processes; (3) the acquisition process; and (4) mandatory training requirements.

Secret Service's Privacy Program collaborates internally with respective program offices, legal counsel, and the Secret Service Chief Information Officer, as needed, in the drafting and publication of PIAs that clearly address the FIPPs. For example, GAOs' draft report alleges that the Secret Service did not fully address the FIPPs protections in the instance of body worn cameras; however, the Secret Service determined that the FIPPS were fully addressed within the corresponding Incident Driven Video Recording System PIA.3 Additionally, the Privacy Program partners with the Office of Professional Responsibility's Inspection Division (ISP) to establish clear accountability mechanisms and privacy policy oversight in the training of all new ISP Inspectors on privacy best practices and implementation of the FIPPs when conducting compliance inspections of Secret Service offices.

Regarding technologies managed or maintained by third-parties, or where the agency merely subscribes to information, Secret Service's Privacy Program thoroughly reviews company terms of service to ensure that their policies align with the FIPPs. The Privacy Program also evaluates the FIPPs in PTA and PIA analyses. Creating a separate analysis and discussion of FIPPs would be duplicative and therefore not a good use of government resources. Furthermore, Secret Service's Privacy Program exercises due diligence by reviewing Statements of Work from third-party vendors to ensure that their privacy practices and incident/breach response protocol are clearly articulated in the event of a data spill. Ultimately, however, it is important that readers of this report understand that adherence to the FIPPs falls on the respective third party managing the information and/or information technology system (e.g., gunshot detection and traffic video systems).

Finally, annual completion of employee privacy and cybersecurity awareness training are required in order to continue use of such technologies. Currently, the Secret Service, Office of Training, James J. Rowley Training Center provides leadership with a list of employees that have not completed their annual training, as appropriate, as well as alerts employees to complete training in order to continue use.

We request that GAO consider this recommendation resolved and closed, as implemented.

1. Policy Directive 140-03,“The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,” dated December 29, 2008; (https://www.dhs.gov/sites/default/files/2024-01/Fair%20Information%20Principles_12_2008.pdf).

2. Pursuant to the requirements of the “e-Government Act of 2002” (SEC. 208., SUBSEC B., “PRIVACY PROVISIONS”) and the “Homeland Security Act of 2002” (SEC. 222(2), in accordance with the Office of Management and Budget (OMB) Memorandum M-03-22, “Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” dated September 26, 2003; (https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/) and applicable DHS policy, ICE Privacy ensure all information technology systems that collect, maintain, or disseminate information in an identifiable form have a privacy impact assessment or privacy threshold analysis conducted by the system owner and approved by the ICE Component Privacy Officer.

3. “DHS/USSS/PIA-031 USSS Incident Driven Video Recording System (IDVRS),” dated July 21, 2023; (https://www.dhs.gov/sites/default/files/2023-07/privacy-pia-usss-pia031-idvrs-july2023.pdf).

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgements

In addition to the contact named above Joseph P. Cruz (Assistant Director), Heather May (Analyst-in-Charge), Jenny Chanley, Benjamin Crossley, Rosanna Guerrero, Lee McCracken, Heidi Nielson, Kevin Reeves, Janet Temko-Blinder, Mary Turgeon, John Vocino, Kelsey Wilson, and John Yee made key contributions to this report.

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.

Connect with GAO

Connect with GAO on Facebook, Flickr, X, 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

Sarah Kaczmarek, Managing Director, KaczmarekS@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