Privacy Impact Assessment

for the

Homeland Security Investigation (HSI) Surveillance Technologies

DHS Reference No. DHS/ICE/PIA-061

January 24, 2022

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), deploys surveillance technologies in furtherance of its criminal investigations and national security missions. Homeland Security Investigations conducts three types of electronic interceptions and surveillance activities: 1) consensual electronic interceptions with the consent of at least one party to the communication; 2) non-consensual electronic interceptions pursuant to a court order; and 3) non-consensual surveillance, without a court order, when the surveillance does not intrude upon an individual's reasonable expectation of privacy. Immigration and Customs Enforcement is conducting this Privacy Impact Assessment (PIA) to document Homeland Security Investigations' privacy protections when using the following surveillance technologies: a) body wire; b) location tracking technology; c) cell-site simulators; d) small unmanned aircraft systems; e) license plate readers and commercial license plate reader data services; and f) video surveillance technology.

Introduction

The Homeland Security Investigations directorate is the principal investigative arm of U.S. Department of Homeland Security and the second largest investigative agency in the federal government. Homeland Security Investigations consists of more than 10,000 employees, 6,700 of whom are special agents, assigned to more than 200 cities throughout the United States and 48 countries around the world. Homeland Security Investigations' mission is to conduct criminal investigations to protect the United States against terrorist and criminal organizations; to combat transnational criminal enterprises that seek to exploit America's legitimate trade, travel, and financial systems; and to uphold and enforce U.S. customs and immigration laws.

Homeland Security Investigations enforces a diverse array of federal statutes to investigate all types of cross-border criminal activity, including: financial crimes; money laundering; bulk cash smuggling; child pornography and exploitation; commercial fraud and intellectual property theft; cybercrimes; human rights violations; human smuggling and trafficking; immigration, document, and benefit fraud; narcotics and weapons smuggling and trafficking; transnational gang activity; export enforcement; and international art and antiquity theft. The availability of technical equipment for use by Homeland Security Investigations special agents when conducting investigations is critical to Homeland Security Investigations' continued success in detecting, deterring, and disrupting terrorist and criminal activity.

The Homeland Security Investigations Technical Operations Unit (Tech Ops) supports Immigration and Customs Enforcement's mission with the most innovative, cutting-edge electronic surveillance and interception[1] equipment in furtherance of Homeland Security

[1] 18 U.S.C. § 2510(4) ("intercept" means the aural (hearing) or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device).

Investigations investigations and Immigration and Customs Enforcement's national security operations. The Technical Operations Unit is currently comprised of four sections: 1) Investigative Interceptions; 2) Title III Investigative Programs;[2] 3) Tactical Communications; and 4) Electronic Surveillance. Surveillance technologies include electronic devices that may be used to collect evidence (e.g., telephone interception equipment; covert tracking, covert video; body wires; audio devices; specialty surveillance vehicles; sensors, computers and workstations used for purposes of electronic surveillance; and telephone data analysis software).

Agents' investigations involve increasingly more complex and sophisticated criminal organizations. The use of new innovative technologies enhances Homeland Security Investigations' capability to gather the necessary evidence needed for prosecution. At the same time, it is Homeland Security Investigations' responsibility to ensure the use of sophisticated technology is accompanied by strict policies and procedures, as well as technical guidance to ensure Homeland Security Investigations' compliance with applicable laws, regulations, and policies by Homeland Security Investigations Technical Enforcement Officers (TEO),[3] Intelligence Research Specialists (IRS), special agents, and other Homeland Security Investigations employees conducting or supporting investigations using electronic surveillance. As technology evolves, Homeland Security Investigations must continue to assess its tools to ensure that practice and applicable policies reflect the agency's law enforcement and national security missions, as well as the agency's commitments to individual privacy and civil liberties.

Homeland Security Investigations only uses surveillance technologies pursuant to a court order; with the consent of a party to the recorded communication; or in a public area where there is no reasonable expectation of privacy under the U.S. Constitution.[4] If Homeland Security Investigations seeks to use any technology outlined in this Privacy Impact Assessment for a new purpose, it will confer with the Office of the Principal Legal Advisor (OPLA) for legal advice and guidance. If these technologies are updated or further developed in a way that raises additional privacy concerns, then Homeland Security Investigations will also consult with OPLA and the ICE Privacy Unit for guidance. Finally, if it is discovered that ICE is using any of these technologies for any purposes not contemplated by the relevant policy or this Privacy Impact Assessment, ICE will reassess the policy and update the Privacy Impact Assessment as appropriate.

This Privacy Impact Assessment discusses the specific surveillance technologies used by Homeland Security Investigations, evaluates the privacy risks associated with the use of

---

[2] Title III of the *Omnibus Crime Control and Safe Streets Act of 1968,* as amended ("Title III") (Pub. L. 90-351). Title III establishes specific protocols and standards for the issuance of a federal court order authorizing electronic surveillance during the course of a federal criminal investigation.

[3] Homeland Security Investigations Technical Operations Handbook, Homeland Security Investigations-HB 14-04, paragraph 4.22 (July 21, 2014) ("A Technical Enforcement Officers is the primary law enforcement officer who supports criminal investigations through the use of electronic surveillance equipment and techniques. The Technical Enforcement Officer's primary responsibility is the gathering of evidence in furtherance of criminal prosecutions.")

[4] Examples of a public area where there is no reasonable expectation of privacy include public sidewalks and public parks.

surveillance technologies, and is intended to enhance the public's understanding of the privacy controls in place regarding those technologies.

I. Consensual Interceptions

A consensual interception of an oral, wire, or electronic communication is a conversation between two or more people monitored and/or recorded by, or under the direction of a law enforcement officer, with the knowledge and prior consent of at least one or more of the participants in the conversation.[5] Homeland Security Investigations uses the following technologies to intercept communications with the consent of at least one party.

Body Wire

Body wire technology includes devices that record audio as well as devices that record both audio and video. The monitoring and recording of consensually-intercepted telephone conversations and face-to-face conversations between a target of an investigation and a cooperating individual and/or an undercover special agent is encouraged by the U.S. Department of Justice (DOJ) as a reliable and effective investigative tool.[6]

The use of body worn audio/video devices requires "one party consent," where one party to the communication wears a device to capture audio/video information in the course of an investigation, or one of the parties to the communication has given prior consent to the interception, in accordance with federal law.[7]

All requests to conduct a telephonic interception with the consent of one party must be approved by the agent's supervisor and the Homeland Security Investigations Special Agent in Charge (SAC) or their designee and coordinated with a U.S. Attorney. In order to obtain this approval, agents must submit an *Electronic Surveillance Request* (ELSUR) to their supervisor using the Investigative Case Management system (ICM).[8] The Electronic Surveillance Request module in the Investigative Case Management system is used to request authorizations, grant authorizations, and transmit reports of use for consensual recording and monitoring of oral communications (including consensual recordings of telephone conversations, as well as covert

[5] Homeland Security Investigations-HB 14-04, paragraph 4.1. *See also* 18 U.S.C. § 2511(2)(c)-(d).
[6] U.S. Department of Justice, *Justice Manual*, 9-7.301 Consensual Monitoring-General Use (September 2004), *available at* https://www.justice.gov/jm/jm-9-7000-electronic-surveillance.
[7] 18 U.S.C. § 2511(2)(c) "(It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception)."
[8] For more information on Electronic Surveillance Requests and the Investigative Case Management system, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SURVEILLANCE SYSTEM (ELSUR), DHS/ICE/PIA-024, and U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT (ICM), DHS/ICE/PIA-044, *available at* https://www.dhs.gov/privacy-documents-ice.

transmitters and recorders). An approved Electronic Surveillance Request must be in place during the time period for which the monitoring occurs.

The case agent planning to conduct a consensual interception is responsible for establishing consent by obtaining: 1) verbal consent from the cooperating individual and document that consent in a Report of Investigation (ROI); or 2) written consent from the cooperating individual. Prior to submitting a request to conduct consensual monitoring, the case agent must coordinate with an Assistant United States Attorney (AUSA). In each request, the agent must state in writing that they discussed the facts of the surveillance or consensual monitoring with the Assistant United States Attorney. The request must also state that the Assistant United States Attorney agrees that the use of consensual monitoring is legal and appropriate and must include the date that such advice was provided. Once approval for the consensual interception is established, the case agent must submit an Electronic Surveillance Request indicating the time period in which the interception will occur.

In the event of an emergency situation requiring an exigent consensual interception, the authority to approve the consensual interception is delegated to the case agent's first-line supervisor. It is also recommended that the Assistant United States Attorney is consulted in these circumstances. On the first business day after the interception has taken place, the case agent must submit the request containing an explanation of the exigent circumstances.[9]

Within five business days after the termination of an Electronic Surveillance Request authorization, a *Monitoring or Interceptions of Consensual Communications Report of Use* must be completed, even to report negative results, and include the names of all individuals whose conversations were recorded and proved to be incriminating (includes not only the primary targets of the investigation, but all those whose conversation were overheard and recorded); all telephone numbers called; all offenses corroborated by the interception; and the number of times during the interception period that incriminating conversations were recorded. Also, any Reports of Investigation documenting consensual recordings should indicate the recording was consensual.

Consensually monitored interceptions are generally conducted under the control and supervision of a special agent or a Technical Enforcement Officer.[10] Initial authorizations for consensually monitored conversations may be granted for a period of 90 days from the date the monitoring is scheduled to begin. Once an approved consensual monitoring period expires case agents may renew the request to consensually monitor conversations by submitting another request

[9] Exigent Circumstances: an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect, or destruction of evidence.

[10] In rare circumstances, when a special agent or Technical Enforcement Officers is not available, the first-line supervisor can authorize the cooperating individual to record a telephone conversation on their own if: 1) the head of the local office has authorized the recording; 2) the special agent has a written Electronic Surveillance Consent from the cooperating individual; 3) the cooperating individual or target does not fall under a sensitive category of individuals (e.g., government officials, politicians); and 4) the special agent or Technical Enforcement Officers work closely with the cooperating individual on installing and using the device. *See Homeland Security Investigations*-HB 14-04, paragraph 9.3.

to their supervisor. In special cases (e.g., long-term investigations that are closely supervised), authorizations for up to 180 days may be granted with similar extensions.

All non-Title III recorded electronic evidence (i.e., no warrant required) is maintained in secure storage until complete adjudication of the case, and all appeals are exhausted, before being destroyed. All recordings entered into evidence in a hearing or trial will not be destroyed except upon an order from the presiding judge. When evidence media is destroyed, it will be rendered unusable and unrecoverable and this must be documented. Homeland Security Investigations has proposed a five-year retention schedule for these records, but until the proposed retention schedule is approved records will be maintained permanently.

II. Non-Consensual Surveillance

Non-consensual interception of an oral, wire, or electronic communication is the monitoring and/or recording of communications between two or more individuals, by or under the direction of a special agent without the knowledge or consent of any of the participants to the conversation.[11] Wire, oral, and electronic communications are intercepted only with a court-issued warrant based on probable cause that the named subjects are using the targeted device(s)[12] or location(s) to facilitate the commission of identified criminal offenses, in accordance with 18 U.S.C. §§ 2510-2522, often referred to as "Title III," a reference to the portion of the implementing legislation (Title III of the *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. 90-351, *as amended*, and codified at 18 U.S.C. § 2519, also referred *to as* "the "Wiretap Act"), which provides authority for electronic interceptions.[13] All Title III recordings must be maintained for a minimum period of 10 years and may not be destroyed or disposed of without a written order from the court that authorized the interception.

Congress requires Immigration and Customs Enforcement/Homeland Security Investigations, and other law enforcement agencies, to submit an annual report identifying all Title-III investigations.[14] This report includes the target device identification, name of the affiant, date the court order was granted, online date (beginning date), and off-line date (ending date), and is publicly available in the form of Wiretap Reports dating back as far as 1997. Wiretap Reports do not include the names, addresses, or phone numbers of parties investigated.

[11] Information collected in these instances does not link an individual before it becomes part of a case.
[12] Targeted devices include cell phones, landlines, computers, and emails.
[13] Title III Evidence is evidence obtained through non-consensual interception of wire, oral, and electronic communication. For instance, evidence obtained through the interception and monitoring of someone's telephone calls would be considered Title III Evidence.
[14] *See* 18 U.S.C. § 2519.

A. Types of Non-Consensual Surveillance Requiring a Warrant

Location Tracking Technology

Tracking technology uses Global Positioning Satellites (GPS),[15] cellular system infrastructure, satellite system infrastructure, and direction-finding technology to provide location data. There is no one device that meets every operational requirement, so each individual case will dictate the type of technology used. Agents must apply to a court for a warrant authorizing the use of a tracking device.[16]

The National Tracking Program (NTP) is an Homeland Security Investigations program office responsible for tracking technologies. The National Tracking Program manages the collection of tracking data and delivers it to authorized personnel.

The National Tracking Program protects data in transit and at rest through user access controls, enhanced authentication requirements and prompt cancelation of authority to use a device for a terminated operation.

The National Tracking Program may share data with other approved law enforcement agencies consistent with the terms and conditions agreed to by the National Tracking Program and the other law enforcement agency.

Authorization to use a tracking device in consensual and non-intrusive installation situations requires a warrant absent certain circumstances (e.g., consent, exigency) and must also be approved by both the agent's first-line supervisor and second-line supervisor. The authorization may be oral but must be noted by the case agent on the appropriate form located in the case file. The authorization may not exceed 30 days but may be extended upon request.

Cell-Site Simulators

Cell-site simulators permit the tracking of mobile telephones in the course of criminal investigations. Special agents and Technical Enforcement Officers may use cell-site simulators to help 1) locate cellular devices whose unique identifiers are *already known* to law enforcement, or 2) determine the unique identifiers of an *unknown device* by collecting limited signaling information from devices in the simulator user's vicinity. A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider.

When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is searching, it will obtain the

[15] Global Positioning Satellites (GPS) is a satellite-based navigation system that provides location and time information anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
[16] United States v. Jones, 565 U.S. 400 (2012).

signaling information related only to that particular device. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing those from the target device. Mobile identifier information[17] collected from non-target devices will be deleted within 24 hours in all cases. Initial contact with a cell-site simulator represents a general location of the mobile handset but does not provide specific location (i.e., GPS) details about any device.

There are two specific cell-site simulator missions: target location and target development. In a target location mission, a specific mobile identifier is entered into the cell-site simulator. The cell-site simulator will then check all mobile identifiers until the requested mobile identifier is located and will reject all other mobile identifiers. During a target development mission, all mobile identifiers will be captured and processed afterward to identify the target number. Non-target data in the area will be deleted within 24 hours.

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is, however, limited. Cell-site simulators provide only the relative signal strength and general direction and radius of the subject cellular device, and do not obtain or download precise location information from the device or its applications, so they do not function as a Global Positioning Satellites locator.

Importantly, cell-site simulators used by special agents and Technical Enforcement Officers must be configured as pen registers[18] (requiring a search warrant) and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3).[19] This includes contents of any communication stored on the device itself. Cell-site simulators do not remotely capture emails, texts, contact lists, images, or any other data from the device. Moreover, cell-site simulators used by Immigration and Customs Enforcement are not capable of collecting subscriber account information (e.g., an account holder's name, address, telephone number) or the contents of the device's communications. Immediately after either the target is located or the phone is identified, an operator of a cell-site simulator must delete all data collected, including all non-target mobile identifiers.

Special agents and Technical Enforcement Officers must obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent). In accordance with Homeland Security Investigations' *Use of Cell-Site Simulator Technology* policy, which is based on U.S. Department of Homeland Security's

[17] A mobile identifier is a unique identifier used to distinguish a mobile device. It is not tied to personally identifiable information (such as the individual's name, credit card number, or Driver's license number) about an individual that owns or controls the device; rather the mobile identifier is used by to distinguish the device itself.
[18] A pen register is a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information does not include the contents of any communication.
[19] 18 U.S.C. § 3127(3).

cell-site simulator policy,[20] the use of cell-site simulators must be done in a manner that is consistent with the requirements and protections of the United States Constitution, including the Fourth Amendment, and applicable statutory authorities, including the pen register statute (18 U.S.C. § 3121). Any information collected from cell-site simulators must be handled in a manner consistent with applicable statutes, regulations, and policies that guide Homeland Security Investigations data collection, retention, and disclosure.

Homeland Security Investigations has established management controls and approval processes to help ensure only knowledgeable and accountable personnel will use this technology. For instance, the assistant director (AD) of Homeland Security Investigations' Information Management Directorate is responsible for ensuring compliance with Homeland Security Investigations' cell-site simulator policy.

Prior to the court order application for the deployment of this technology, the use of a cell-site simulator must be approved by a first-level supervisor and must be pursuant to a signed search warrant by a judge. Any exigent or emergency use of a cell-site simulator must also be approved by an appropriate second-level supervisor prior to its use.

Although exigent circumstances do not require a warrant under the Fourth Amendment, cell-site simulators still require court approval, consistent with the Pen Register Statute's emergency provisions in order to be lawfully deployed.[21] An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an officer has the requisite probable cause, a variety of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; prevent imminent destruction of evidence; hot pursuit of a fleeing felon; or to prevent the escape of a suspect or convicted fugitive from justice.

All users of cell-site simulators are required to attend training before using the equipment, which is required to include training on both privacy and civil liberties. The Unit Chief of Homeland Security Investigations Technical Operations Unit is responsible for the development and coordination of the initial and advanced training requirements for the use of cell-site simulators.

When deploying cell-site simulators, Homeland Security Investigations operates in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information. Consistent with applicable

[20] *See* Department Policy Regarding the Use of Cell-Site Simulator Technology, Policy Directive 047-02 (October 19, 2015), *available at* https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.
[21] 18 U.S.C. § 3125.

laws and requirements, including any duty to preserve exculpatory or impeaching evidence,[22] Homeland Security Investigations' cell-site simulator practices include the following:

1) Immediately following the completion of a mission, an operator of a cell-site simulator must delete all data;[23]
2) When the equipment is used to locate a target,[24] data must be deleted as soon as the target is located;
3) When the equipment is used to identify a target,[25] data must be deleted as soon as the target is identified, and no less frequently than once every 30 days;
4) Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

After completing a mission, an operator of a cell-site simulator will document whether any useful information was obtained and, if so, a description of the information in a Report of Investigation. The Report of Investigation will be stored in the appropriate investigative case file in the Investigative Case Management system[26] and retained in accordance with the applicable records retention schedule.

III. Non-Consensual Video Surveillance Not Requiring a Warrant

Placement of a surveillance camera (without audio) in a public place (i.e., a location where an individual does not have a reasonable expectation of privacy) is an investigative activity that does not require a warrant so long as the camera is placed with any required permissions of the property owner. A "public place" is an area where the public has unrestricted access and where no person has a reasonable expectation of privacy.[27] Public places can include public streets, public parking lots, and hallways of a building open to the public. However, depending on a number of factors, a search warrant may be required to operate a camera that monitors an area where an individual has a reasonable expectation of privacy. If it is determined that a search warrant is

[22] It is not likely, given the limited type of data cell-site simulators collect (as discussed above), that exculpatory evidence would be obtained by a cell-site simulator in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent that investigators know or have reason to believe that information is exculpatory or impeaching, they have a duty to memorialize that information.
[23] A typical mission may last anywhere from less than one day up to several days.
[24] Locating a target means identifying the specific location of one device. Cell-site simulators provide only the relative signal strength and general radius of the subject cellular device, and do not obtain or download any location information from the device or its applications, so they do not function as a Global Positioning Satellites locator.
[25] Identifying a target means determining a single device from many devices.
[26] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT (ICM), DHS/ICE/PIA-044, *available at* https://www.dhs.gov/privacy-documents-ice.
[27] Homeland Security Investigations-HB 14-04, paragraph 13.1.

required, it must be obtained in coordination with the U.S. Attorney's Office and approved by the Department of Justice.[28]

Consensual video surveillance may be conducted in a warrantless manner even though one party to the conversation may have a reasonable expectation of privacy. If video and audio will be recorded, special agents are required to comply with agency procedures and federal law. If the consenting party leaves the area under surveillance, continued video or audio monitoring will no longer be deemed consensual and any monitoring must be discontinued until a consenting party returns.[29]

Where there is video recording only (no audio) in public places with no reasonable expectation of privacy, no supervisory approval is required. Additionally, authorization is not required for consensual video surveillance without audio interception where the person has no reasonable expectation of privacy. However, if video surveillance is used in conjunction with audio surveillance, a request for video must be included with the application for audio surveillance.

However, to be deemed constitutional, a video search warrant with the Title III requirements, including probable cause and minimization, must be present when the individual has a reasonable expectation of privacy. All video surveillance with audio must follow the authorization procedures in the Homeland Security Investigations Handbook.

Small Unmanned Aircraft Systems

Small Unmanned Aircraft Systems technology (commonly referred to as "small drones") offers law enforcement an efficient way to protect and serve the public while promoting officer safety. Small Unmanned Aircraft Systems may be used in a variety of Homeland Security Investigations law enforcement missions (e.g., serving high risk warrants, force protection during undercover meetings with criminal suspects, pre-operation evaluation) and other situational awareness support (e.g., disaster response, search and rescue).

The Federal Aviation Administration (FAA), which regulates the use of small Unmanned Aircraft Systems, defines a small unmanned aircraft (UA) as one weighing less than 55 pounds on takeoff, including everything that is onboard or otherwise attached to the aircraft, and can be operated without the possibility of direct human intervention from within or on the aircraft.[30] An small Unmanned Aircraft Systems refers to the unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small Unmanned Aircraft Systems in the

[28] For those instances where a reasonable expectation of privacy might apply, Agents and Technical Enforcement Officers are to consult with their United States Attorney's Office (USAO) and the Immigration and Customs Enforcement Office of the Principal Legal Advisor (OPLA).
[29] After the consenting individual leaves the area, any additional video/audio recorded will be purged.
[30] 14 C.F.R. § 107.3, *available at* https://www.govinfo.gov/content/pkg/CFR-2002-title14-vol2/xml/CFR-2002-title14-vol2-sec107-3.xml.

National Airspace System (NAS).[31]

Homeland Security Investigations will operate its small Unmanned Aircraft Systems under the same Federal Aviation Administration regulations applicable to commercial and recreational small Unmanned Aircraft Systems users.[32] Furthermore, operation of an small Unmanned Aircraft Systems and collection of video recordings shall be solely for official purposes in compliance with Homeland Security Investigations Directive 19-01 and shall not be used in any manner that would violate the First Amendment or target a person based on his or her race, color, religion, sex, sexual orientation, gender identity, or national origin.[33]

The Remote Pilot in Command (RPIC) may record video and images during the flight from a camera mounted on the small Unmanned Aircraft Systems. At the conclusion of an unmanned aircraft flight where images or video recordings were collected, the Remote Pilot in Command will either delete the material collected, subject to the criteria listed below, or safely secure the information as soon as practical, in either case no later than three business days following the flight. Incidental collection of video recordings or images will be minimized by requiring the deletion of all collected video or images within 30 days, unless: 1) the collected material contains evidence of a crime; 2) the material was collected during an operation that focused on a particular subject of investigation, even if no crime is recorded, to preserve it as exculpatory evidence; 3) the collection was ordered by the court; or 4) the material was collected during a training flight and such images or videos contain individuals who participated in the training knowing that their still or video image might be captured. Immigration and Customs Enforcement small Unmanned Aircraft Systems will only record video (no audio).[34]

License Plate Readers and Commercial License Plate Reader Data Services

A license plate reader (LPR) is a type of Automated Video Surveillance (AVS) technology that extracts text from images using Optical Character Recognition (OCR) technology. License plate readers automate a normally manual, labor-intensive process, which improves efficiencies for Immigration and Customs Enforcement criminal law enforcement agents.

An license plate reader system consists of a high-speed camera, or cameras, and related equipment, mounted on vehicles or in fixed locations (e.g., bridges, toll roads, parking garages) that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come within the range and angle of vision of the device. The system then automatically converts the digital photographic images of license plates and associated data into a

[31] *Id.*
[32] *Id. See also* Federal Aviation Administration, Advisory Circular, *Small Unmanned Aircraft Systems (AC No. 107-2)*, June 21, 2016, *available at* https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf.
[33] U.S. Immigration and Customs Enforcement Homeland Security Investigations, Homeland Security Investigations *Directive 19-01: Use of Small Unmanned Aircraft Systems*, April 3, 2019.
[34] *Id.* at 5.5. The Remote Pilot in Command is an Homeland Security Investigations law enforcement officer who possesses a current Federal Aviation Administration Part 107 license and is determined to be qualified by a Senior Pilot based on meeting all the regulatory and statutory requirements to assume operational control of a mission.

computer-readable format. This computer-readable format, also known as "a read," contains some or all of the following information: (1) license plate number; (2) digital image of the license plate as well as the vehicle's make and model; (3) state of registration; (4) camera identification (i.e., camera owner and type); (5) Global Positioning Satellites coordinates or other location information recorded at the time the information was captured; and (6) date and time of observation.

Homeland Security Investigations' use of license plate readers and data from commercial license plate reader data services support Homeland Security Investigations' criminal investigation mission.[35] Significantly, the use of license plate reader technology is vehicle-centric, as it focuses on a given vehicle of interest to the investigation. This could be a vehicle known to be owned or operated by a target, or a vehicle believed to be smuggling contraband. Typically, agents will be able to add license plates of interest to a criminal investigation to an "alert list" within the license plate reader system used by its partner(s). Homeland Security Investigations personnel upload alert lists, which are not made available to the law enforcement partners that own the databases. When the image of a license plate on an alert list is captured by a camera linked to the database, the agent with whose investigation that license plate is associated receives an automated email notification. The notification typically provides an image of the license plate number, computer-generated text of the information the software has read from the license plate, and the Global Positioning Satellites coordinates for the location where the license plate was photographed. The purpose of these notifications is to provide agents with real-time location information so that they may take action, if appropriate. Agents may upload the images and/or copies of the notifications into the Investigative Case Management system as case documents and link them to subject records. They may also describe this information and any related actions in arrest reports, other incident reports, or Reports of Investigation.

Immigration and Customs Enforcement also may obtain location data via arrangements with other law enforcement agencies or task forces that collect and use license plate reader technology, such as from U.S. Customs and Border Protection's license plate reader cameras at ports of entry or through established partnerships with federal, state, and local law enforcement agencies (e.g., High Intensity Drug Trafficking Area task forces). Immigration and Customs Enforcement enters into these partnerships pursuant to terms detailed in Memoranda of Agreement and agents who have access to this information are required to comply with the U.S. Department of Homeland Security and Immigration and Customs Enforcement Rules of Behavior covering access to and appropriate use of sensitive data.[36] Among other requirements, the Immigration and Customs Enforcement Rules of Behavior include limitations on the use of the data (i.e., only for authorized law enforcement purposes), strict criteria for creating alerts, a prohibition on *ad hoc*

[35] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR), DHS/ICE/PIA-039, *available* at https://www.dhs.gov/privacy-documents-ice.
[36] DHS 4300A, Sensitive Systems Handbook, Attachment G, Rules of Behavior (Aug. 5, 2014), *available at* https://www.dhs.gov/publication/dhs-4300a-handbook-attachment-g-rules-behavior

and historical queries, specified timeframes for refreshing alerts, and a requirement to manually verify the accuracy of data contained within notifications.[37]

License plate reader data can help resolve cases that might otherwise be closed for lack of viable leads, enhance both officer and public safety by enabling enforcement actions to occur in locations that minimize the inherent dangers associated with these encounters, and reduce the hours required to conduct in-person physical surveillance. Consequently, Immigration and Customs Enforcement has procured a third-party vendor for Homeland Security Investigations personnel with authorized access to query commercial license plate reader data. The license plate reader data assists Immigration and Customs Enforcement in developing and validating criminal and administrative law enforcement leads based on the location of vehicles that are associated with Immigration and Customs Enforcement criminal and administrative investigations.[38]

Immigration and Customs Enforcement does not take any enforcement action against an individual based solely on the results of a query. Rather, Immigration and Customs Enforcement uses information from the license plate reader database to develop and corroborate other investigative information, including information from government systems. The vendor's commercial license plate reader database stores vehicle license plate numbers that are recorded from cameras equipped with license plate reader technology. The commercial database receives data from a variety of governmental and private sources, including:

- Toll road cameras;
- Parking lot cameras;
- Vehicle repossession companies; and
- Law enforcement agencies.[39]

The vendor compiles license plate reader records from at least 25 states and 24 of the top 30 most populous metropolitan statistical areas[40] within the United States, to the extent that collection of license plate reader data is authorized by law in those jurisdictions. Immigration and Customs

[37] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR), DHS/ICE/PIA-039, *available at* https://www.dhs.gov/privacy-documents-ice.

[38] The principles and practices Immigration and Customs Enforcement adheres to when accessing and using license plate reader data are described in agency guidance, "Privacy Guidance: Agency Access to and Use of License Plate Reader Data and Technology", issued December 2017, from the Immigration and Customs Enforcement Office of Information Governance & Privacy.

[39] For a discussion of the information that the license plate reader database stores, *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR), DHS/ICE/PIA-039, *available at* https://www.dhs.gov/privacy-documents-ice. ICE will update this Privacy Impact Assessment as query requirements change.

[40] A metropolitan statistical area is defined in the contract as: "a geographical region with a relatively high population density at its core and close economic ties throughout the area as defined by the Office of Management and Budget (OMB) and used by the Census Bureau and other federal government agencies for statistical purposes."

Enforcement does not contribute data to the commercial license plate reader database. Further, the terms of the contract do not permit the commercial license plate reader vendor to use any of Immigration and Customs Enforcement's query data, including photographs, for its own purposes or share information from Immigration and Customs Enforcement queries with other customers, business parties, or any other individual or entity without express permission from Immigration and Customs Enforcement.[41]

Other license plate reader functionality that is available to select authorized Homeland Security Investigations personnel include:

- Geographic query – conducting a query within a specified geographic area during a specified time period;
- Partial license plate query – conducting a query using a partial license plate when the full license plate character sequence is inaccessible or unclear; and
- Mobile plate scan feature – using a phone's camera to scan license plates in a continuous automatic manner, rather than "snapping" license plate photo images one at a time.

These functionalities produce data-driven, real-time, actionable intelligence and allow Immigration and Customs Enforcement to more efficiently apprehend offenders, prevent and solve crimes, improve both public and officer safety, and increase situational awareness.

Video Surveillance Technology

The Homeland Security Investigations Covert Video Surveillance (CVS) section provides video surveillance solutions to include both covert and overt devices as well as large scale video management systems. A variety of data transmission methods are used in support of the Homeland Security Investigations video surveillance systems including cellular data, terrestrial Internet Protocol (IP) connections,[42] and digital microwave[43] systems; all of which use encryption to secure the data while in transit.

The Video Evidence Collection System (VECS) is a series of interconnected video collections sites installed at Homeland Security Investigations locations around the country. The Video Evidence Collection System is used to operate cameras, collect video evidence during criminal investigations, and distribute video evidence to investigators and prosecuting attorneys in the prosecution of criminal violations. The Video Evidence Collection System is scheduled to be

[41] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR), DHS/ICE/PIA-039, *available at* https://www.dhs.gov/privacy-documents-ice.

[42] Terrestrial IP connections use cable or wire for the communications link, typically used for home or business connectivity.

[43] Digital microwave is a specific type of radio frequency communications (audio/video) link, which is an efficient way of transmitting data and employing encryption.

deployed at 46 Homeland Security Investigations office locations to ensure that collected evidence remains in the appropriate chain of custody/judicial district. The Video Evidence Collection System collects video from covert surveillance solutions, which transmit video to the Video Evidence Collection System sites for processing, storage, and maintenance. The Video Evidence Collection System allows authorized users to view both live and recorded video throughout the course of the investigation. The connection from the collection device to the server, as well as the link from the server to the end-user viewing the collected video, use advanced network security hardware and software to maintain government IT security compliance with full auditing capabilities.

In the course of an investigation, authorized system administrators may grant Task Force Officers (i.e., national, state, and local law enforcement officers), and prosecuting attorneys, credentials to access the system via a secure web portal. All users' access, regardless of employment type, is restricted to cases (live or archived) to which they have a valid need-to-know. The system enforces these restrictions by requiring the administrator to specifically assign users to any case they need to access while newly created cases are only visible to the administrator who created them.

Because the captured video is used as evidence, the retention period for the entire recording, or only portions of it, varies by judicial district. However, video is generally only stored within the Video Evidence Collection System for the duration of an investigation. Once the investigation is complete, the data is either moved off the Video Evidence Collection System and stored as digital evidence or purged if there is no evidentiary value.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[44] articulates concepts of how the federal government should treat individuals and their information, and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[45]

In response to this obligation, the U.S. Department of Homeland Security Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of U.S. Department of Homeland Security.[46] The Fair Information Practice Principles account for the

[44] 5 U.S.C. § 552a.
[45] 6 U.S.C. § 142(a)(2).
[46] Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *available at* https://www.dhs.gov/privacy-policy-guidance.

nature and purpose of the information being collected in relation to U.S. Department of Homeland Security's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208[47] and the Homeland Security Act of 2002 Section 222.[48] As part of its law enforcement operations, Immigration and Customs Enforcement uses surveillance technologies to conduct criminal investigations. As such, this Privacy Impact Assessment examines the collection of personally identifiable information by surveillance technologies within the construct of the Fair Information Practice Principles.

1. Principle of Transparency

Principle: U.S. Department of Homeland Security should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information. Technologies or systems using personally identifiable information must be described in a SORN and PIA, as appropriate.

Criminal law enforcement is always careful in disclosing technical aspects of investigative techniques and technology, which may weaken the effectiveness of sophisticated equipment and seriously jeopardize the safety of law enforcement personnel. Immigration and Customs Enforcement's published Privacy Impact Assessments and System of Record Notices (SORN) provide significant public documentation of the systems that collect, use, maintain, and disseminate personally identifiable information captured from surveillance technology.[49] The use of surveillance technology in criminal investigations is tightly governed by law, policy, and regulation. As discussed, a warrant is required when the target(s) of the electronic interception has a reasonable expectation of privacy and has not otherwise consented to such surveillance (e.g., home, tracking location of a car). In situations when a target has no expectation of privacy, such as a public square, or where there is a consensual interception, Homeland Security Investigations policies and procedures constrain the prior approval, supervision, and limited duration of the operation.

---

[47] 44 U.S.C. § 3501 note.
[48] 6 U.S.C. § 142.
[49] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR), DHS/ICE/PIA-039; U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SURVEILLANCE SYSTEM (ELSUR), DHS/ICE/PIA-024; U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT (ICM), DHS/ICE/PIA-044; U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE SECURITY MANAGEMENT CCTV SYSTEM, DHS/ICE/PIA-030, *available at* https://www.dhs.gov/privacy-documents-ice. *See* DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010); DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) 81 FR 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

Privacy Risk: There is a risk that a member of the public will not know that Immigration and Customs Enforcement is collecting audio, photos, videos, or other information through surveillance technology.

Mitigation: This risk is partially mitigated through the publication of this Privacy Impact Assessment, which provides notice of Immigration and Customs Enforcement's surveillance technologies. Immigration and Customs Enforcement is a law enforcement agency and its surveillance technologies are used in furtherance of a criminal investigation or arrest. More explicit prior notice could reveal U.S. Department of Homeland Security' investigative interest in a subject, who might then attempt to impede an ongoing investigation by tampering with witnesses, evidence, or take steps to avoid detection and/or apprehension.

2. Principle of Individual Participation

Principle: U.S. Department of Homeland Security should involve the individual in the process of using personally identifiable information. U.S. Department of Homeland Security should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of personally identifiable information and should provide mechanisms for appropriate access, correction, and redress regarding U.S. Department of Homeland Security's use of personally identifiable information.

In light of Immigration and Customs Enforcement's criminal law enforcement and national security missions, a traditional approach to individual participation (e.g., verbal or written consent) is not always practical or possible. Surveillance technologies are valuable tools in conducting or supporting Immigration and Customs Enforcement's criminal investigations. Allowing an individual to consent to the collection, use, dissemination, and maintenance of video, images, intercepts, and other data would compromise operations and would interfere with the U.S. government's ability to protect public safety and national security. Nevertheless, in a limited manner, verbal or written consent is required by a cooperating individual prior to equipping that individual with a body wire, for example, for the purpose of gathering evidence in the course of a criminal investigation.

Individuals do not have the opportunity to restrict Immigration and Customs Enforcement's ability to collect information in public places. Any information associated with an individual becomes part of the case file that is created as part of a law enforcement investigation or encounter. Providing individuals of interest access to information about them during a pending law enforcement investigation may alert them or otherwise compromise the investigation. Consequently, there is no immediate mechanism for correction or redress for the data captured by surveillance technology. Once the data is associated with an individual's case file, the individual must follow procedures outlined in the corresponding privacy documents (Privacy Impact Assessment or System of Record Notice) in order to request access to, or amendment of records maintained on them in a U.S. Department of Homeland Security or Immigration and Customs

Enforcement system of records. While individuals cannot participate in the initial collection of this information, they may contest or seek redress through any resulting proceedings brought against them.

The right to request amendment of records under the Privacy Act of 1974 (5 U.S.C. § 552a) is limited to U.S. citizens and Lawful Permanent Residents. Individuals not covered by the Privacy Act or the Judicial Redress Act[50] may request access to their records by filing a Freedom of Information Act (FOIA) request.

DHS Privacy Policy makes clear that there is an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records.[51] Collecting, maintaining, using, and disseminating accurate information helps U.S. Department of Homeland Security to efficiently meet its operational goals, prevent waste, and improve outcomes. Failure to maintain accurate records serves to undermine efficient decision making by U.S. Department of Homeland Security personnel, and can create the risk of errors made by U.S. Department of Homeland Security and its personnel. To that end, the Privacy Unit in the Immigration and Customs Enforcement Office of Information Governance & Privacy accepts record amendment requests from individuals not covered by the Privacy Act of 1974.

Individuals seeking notification of and access to any of the records covered by this Privacy Impact Assessment may submit a request electronically at https://www.ice.gov/webform/foia-request-form or in writing to the Immigration and Customs Enforcement Freedom of Information Act (FOIA) officer at the below address:

U.S. Immigration and Customs Enforcement
Office of Information Governance & Privacy
Freedom of Information Act Division
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

Individuals seeking to correct records contained in the appropriate system of records, or seeking to contest its content, may submit a request in writing to the Immigration and Customs Enforcement Privacy Division:

U.S. Immigration and Customs Enforcement
Office of Information Governance & Privacy

[50] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017, include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the U.S. Department of Justice website https://www.justice.gov/opcl/judicial-redress-act-2015.

[51] Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *available at* https://www.dhs.gov/privacy-policy-guidance.

Attn: Privacy Division
500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
(202) 732-3300
http://www.ice.gov/management-administration/privacy

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for Immigration and Customs Enforcement records.

Mitigation: This risk is mitigated. This Privacy Impact Assessment and the External Investigations System of Record Notice describe how individuals may make access requests under FOIA or the Privacy Act, as applicable. Redress is available for U.S. citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents U.S. Department of Homeland Security from extending Privacy Act redress to individuals who are not U.S. citizens, Lawful Permanent Residents, or covered by the Judicial Redress Act. However, to ensure the records it maintains are accurate, Immigration and Customs Enforcement may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law and policy.

Privacy Risk: There is a risk that individuals will not have the opportunity to consent to Immigration and Customs Enforcement collecting their personal information in public places.

Mitigation: This risk is partially mitigated. While individuals cannot participate in the initial collection of their information in public places, they may contest or seek redress through any resulting proceedings brought against them. Individuals can look to the System of Records Notice(s) listed above to determine appropriate procedures to obtain access to and correct their requested record(s). All or some of the requested information may be exempt from access pursuant to the Privacy Act and FOIA in order to prevent harm to law enforcement investigations or interests. Providing individuals of interest access to information about them during a pending law enforcement investigation may alert them or otherwise compromise the investigation. Consequently, there is no direct mechanism for correction or redress for the data captured by surveillance technology. Homeland Security Investigations takes precautions to minimize the collection of data from non-targets and has implemented oversight procedures to ensure that any data incidentally collected is destroyed in compliance with applicable laws, regulations, and policies.

3. Principle of Purpose Specification

Principle: U.S. Department of Homeland Security should specifically articulate the authority which permits the collection of personally identifiable information and specifically articulate the purpose or purposes for which the personally identifiable information is intended to be used.

Under its statutory authority, Homeland Security Investigations may use telephone intercepts, covert tracking data, video, audio, radar, and sensor data, obtained from surveillance equipment during a criminal investigation, as it works to establish a strong case for federal prosecution.[52]

Checks are in place to ensure the collection and use of personally identifiable information during a criminal investigation are consistent with Homeland Security Investigations' authority. For example, non-consensual Title III interceptions require probable cause, minimization of the scope of the interception, close coordination with the Assistant United States Attorney, and court approval. In consensual interceptions, case agents must obtain first-line supervisory approval to conduct a consensual interception and closely coordinate with the Assistant United States Attorney. Each request for a consensual interception must state in writing that the facts of the surveillance or consensual monitoring have been discussed with the Assistant United States Attorney, who has advised that the consensual monitoring is legal and appropriate. In addition, the information gathered using surveillance technologies may only be shared with state, local, federal, tribal, and foreign law enforcement agencies in a manner consistent with the purpose for which it was collected, in accordance with applicable laws and System of Record Notices.

Privacy Risk: There is a risk that data from Homeland Security Investigations surveillance technologies will be collected and used in a manner inconsistent with the purposes for which it is authorized.

Mitigation: This risk is mitigated. Federal law authorizes the use of each technology outlined in this Privacy Impact Assessment. Immigration and Customs Enforcement is authorized by19 U.S.C. § 1589a to investigate all federal crimes and by 8 U.S.C. § 1357 to investigate immigration-related crimes. These authorities likewise authorize Immigration and Customs Enforcement to collect information in the course of the investigation of such crimes, which may include the interception of oral, wire, and electronic communications in accordance with Title III. Moreover, as stated above, this program implements various measures to ensure that Homeland Security Investigations personnel use surveillance technology data for purposes that are consistent with its authorized use. Specifically, the information gathered using surveillance technologies may only be shared with state, local, federal, tribal, and foreign law enforcement agencies in a manner aligned with the objective for which it was collected, in accordance with applicable laws and Systems of Record Notices.

To ensure that consensual interceptions (e.g., body wires) are performed for the purposes of which they were intended, case agents must obtain first-line supervisory approval to conduct a

[52] Homeland Security Act of 2002 (6 U.S.C. §§ 201-203); the Immigration and Nationality Act, as amended (Title 8, United States Code, "Aliens and Nationality"); Title 18, United States Code, "Crimes"; Title 19, United States Code, "Customs Duties"; 22 U.S.C. § 2778; 40 U.S.C. § 1315; 50 U.S.C. §§ 1701 and 2410.

consensual interception while maintaining close coordination with the Assistant United States Attorney.

For non-consensual Title III interceptions, minimization of the scope of the interception and close coordination with the Assistant United States Attorney are required. A court-issued search warrant, which establishes that probable cause for the search exists, is required for Immigration and Customs Enforcement to use location tracking technology and cell-site simulators. Furthermore, the search warrant must articulate the facts and circumstances supporting probable cause for the search. As a warrant provides a rationale for the search, the warrant helps ensure that these surveillance technologies stay within the scope of the search.

The operation of small Unmanned Aircraft Systems and the collection of video recordings must be consistent with the official purposes in compliance with Homeland Security Investigations Directive 19-01 and must be approved by a Homeland Security Investigations supervisor, and to ensure it is not used in any manner that would violate an individual's rights or otherwise target a specific individual. The Homeland Security Investigations Small Unmanned Aircraft Systems program is approved as a federal aviation program by the DHS Office of the Chief Readiness Support Officer (OCRSO), Aviation and Marine Integration Office (AMIO) as required under Department policy. This program is reviewed every three years to ensure compliance.

Furthermore, Immigration and Customs Enforcement is authorized to collect commercial license plate reader data in furtherance of its investigative and enforcement missions under numerous authorities, including various criminal and civil provisions in Titles 8, 18, 19, 21, and 31 of the United States Code, and associated U.S. Department of Homeland Security regulations.[53] Agents who have access to license plate reader data are required to comply with the Rules of Behavior (ROB) that Immigration and Customs Enforcement created in coordination with license plate reader commercial vendors. These ROBs outline requirements pertaining to access to and appropriate use of license plate reader data, and limitations on the use of the data (i.e., only for authorized law enforcement purposes). Additionally, there are strict criteria for creating alerts and a prohibition on running historical queries beyond a certain time period.

4. Principle of Data Minimization

Principle: U.S. Department of Homeland Security should only collect personally identifiable information that is directly relevant and necessary to accomplish the specified purpose(s) and only retain personally identifiable information for as long as is necessary to fulfill the specified purpose(s). personally identifiable information should be disposed of in accordance with U.S. Department of Homeland Security records disposition schedules as approved by the National Archives and Records Administration (NARA).

[53] 8 U.S.C. Title 8—ALIENS AND NATIONALITY; 18 U.S.C. Title 18—CRIMES AND CRIMINAL PROCEDURE; 19 U.S. Code Title 19—CUSTOMS DUTIES; 21 U.S.C. Title 21—FOOD AND DRUGS; 31 U.S.C. Title 31—MONEY AND FINANCE.

In criminal investigations, minimization is critical to avoid monitoring and recording conversations that are not of a criminal nature. Federal law (18 U.S.C. § 2518(5)) requires the purpose of the interception to be limited, as practicable, to the target communications constituting evidence of a crime. Therefore, agents are required to avoid conversations of innocent persons not associated with the subject(s) and irrelevant conversations of the subjects and their associates. To that end, as an example, Title III interceptions use Immigration and Customs Enforcement cleared contract "monitors"— Homeland Security Investigations personnel acting under the direct supervision of a supervising attorney—and operate and monitor Title III or consensual interceptions of oral, wire, or electronic communications to ensure only communications pertaining to the target's criminal activities are recorded.[54] Prior to commencing an interception, the supervising attorney provides the monitors with instructions on how the intercept should be conducted. Initial minimization guidelines for specific cases are provided by the supervising attorney that may be modified as the case develops. The amount of time that a monitor is allowed to listen to a conversation before determining if the communication is "pertinent" or "innocent" may also be determined by the judge issuing the warrant and varies according to the judicial district.

For instance, conversations concerning crimes other than those described in the interception application and court order, which are unexpectedly intercepted, may be recorded if either of two circumstances exist: 1) the evidence is so intertwined with the authorized offense evidence that segregation is impractical; or 2) law enforcement obtain the evidence during an effort to minimize the collection (e.g., time spent listening to the communication was to determine if the conversation was pertinent to the investigation, in accordance with the minimization guidelines).

The various sections of the Technical Operations Unit implement their own individual procedures for minimizing data. Specifically, Title III recordings must be maintained for a minimum period of 10 years and may not be destroyed or disposed of without a written order from the court which issued the order authorizing the intercept. The Technical Operations Unit maintains consensual electronic surveillance evidence for five years.

All non-Title III recorded electronic evidence must be maintained in secure storage until final adjudication of the case and the exhaustion of all appeals are completed before being destroyed. All recordings entered into evidence in a hearing or trial must not be destroyed except upon receipt of a judicial order. When evidence media (e.g., CD/DVD, minidisc, Compact Flash card, Secure Digital card) is destroyed, it is to be rendered unusable and unrecoverable.

For consensually monitored conversations, initial authorizations may be granted for a period of 90 days from the date the monitoring is scheduled to begin. If there is a need for continued monitoring, extensions for additional periods of up to 90 days may be granted. In special cases (e.g., long-term investigations that are closely supervised), authorizations for up to 180 days may

[54] Homeland Security Investigations-HB 14-04, page 5.

be granted with similar extensions. Recorded activities captured inadvertently by small Unmanned Aircraft Systems will be destroyed after 30 days.

Privacy Risk: There is risk that the surveillance technologies will collect more information than necessary.

Mitigation: This risk is partially mitigated. Individuals who are not targets of an investigation may be recorded during a consensual interception with a body wire; however, as stated above, Title III intercepted communications are tightly controlled to ensure only criminal conversations are recorded, and the monitors will stop recording after a certain period of time when conversations of innocent persons not associated with the subject(s), or irrelevant non-criminal conversations of subjects and their associates are taking place. The amount of time that a monitor is allowed to listen to a conversation before determining the relevance of the communication will depend on the issuing judge and the judicial district. In the case where the consenting individual leaves the area, any additional video/audio recorded will be purged.

In order to preserve electronic evidence in an unadulterated state, Homeland Security Investigations securely stores non-Title III evidence until complete adjudication of the case and the exhaustion of all appeals are completed before being destroyed. Homeland Security Investigations destroys all recordings entered into evidence during a hearing or trial only pursuant to a judicial order. When Homeland Security Investigations destroys evidence media, the destruction renders it unusable and unrecoverable, so it must be documented.

Location tracking technology also provides its own procedures to minimize the data that it collects. The National Tracking Program Tracking server system allows for input of the court ordered tracking warrant inclusive dates, in order to prevent over-collection of geo-location data captured by the device.

In accordance with federal law, Homeland Security Investigations requires that each cell-site simulator be configured such that it is only capable of identifying the existence of mobile phones within the proximity of the device. Once the cell-site simulator identifies the specific cellular device for which it is searching, it will obtain the signaling information related only to that particular device. However, when it is used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing those from the target device. Any data collected from non-target devices will be deleted within 24 hours in all cases.

Homeland Security Investigations also implements procedures to minimize data collection in its use of small Unmanned Aircraft Systems. Incidental collection of video will be minimized by requiring the deletion of all collected video within 30 days, unless the video recording 1) contains evidence of a crime; 2) was collected during an operation that focused on a particular subject of investigation, even if no crime is recorded, to preserve its exculpatory evidence; 3) was ordered by the court; or 4) does not contain personally identifiable information. In addition, the

Remote Pilot in Command conducting the video recording must store any collected video in a secure facility under the Remote Pilot in Command's control and must personally ensure permanent deletion of video before 30 days has elapsed from the date of recording, unless the video is retained.

For the use of license plate reader technology, all Immigration and Customs Enforcement personnel (including Homeland Security Investigations) must adhere to Immigration and Customs Enforcement license plate reader policy guidance, which states that Immigration and Customs Enforcement will not engage in the overcollection of license plate reader data.[55] To determine whether information obtained from the license plate reader data service is relevant to an investigation or enforcement matter, Homeland Security Investigations reviews all search results returned upon querying the database. If Homeland Security Investigations determines that certain records are not relevant, those records are not printed, saved, or stored. For example, some license plate reader images may display the environment surrounding a vehicle, which may include other drivers and passengers. Immigration and Customs Enforcement will not record any information or images of such individuals if they are not relevant to an investigation.

Privacy Risk: There is a risk that Immigration and Customs Enforcement will maintain data acquired from surveillance technologies for longer than necessary.

Mitigation: This risk is mitigated. Various oversight procedures ensure that any data collected is destroyed upon the cessation of law enforcement operations. For example, location tracking technology destroys data that it collects following the end of a specific operation. Also, the National Tracking Program server system allows for input of the court ordered tracking warrant inclusive dates, in order to prevent over-collection of geo-location data captured by the device. Furthermore, immediately after either law enforcement locates the target or identifies the phone, an operator of a cell-site simulator must delete all data collected.

All non-Title III recorded electronic evidence is maintained in secure storage until complete adjudication of the case, and the exhaustion of all appeals are completed, before being destroyed.

At the conclusion of an unmanned aircraft flight where images or video recordings were collected, the Remote Pilot in Command will either delete the material collected or safely secure the information no later than three business days following the flight. The incidental collection of video recordings or images using small Unmanned Aircraft Systems will be minimized by requiring the deletion of all collected video or images within 30 days.

[55] The principles and practices Immigration and Customs Enforcement adheres to when accessing and using license plate reader data are described in agency guidance titled, "Privacy Guidance: Agency Access to and Use of License Plate Reader Data and Technology", issued June 15, 2021, from the Immigration and Customs Enforcement Office of Information Governance & Privacy.

Hard copy records of information printed from the commercial license plate reader data service are maintained for three years from the end of the calendar year in which the record was created, [56] while hard copy records included in the relevant investigative files are retained onsite for 10 years, after which they are transferred to the Federal Records Center, and destroyed when they are 20 years old. Longer retention may be authorized if there is a justified business need (e.g., ongoing investigation, pending litigation). Electronic license plate reader records maintained in Immigration and Customs Enforcement source systems (e.g., Investigative Case Management system) adhere to the National Archives and Records Administration-approved retention schedules of those systems. Immigration and Customs Enforcement does not contribute data to the commercial license plate reader database and Immigration and Customs Enforcement query data is not retained by the vendor except to maintain audit logs for use by Immigration and Customs Enforcement.

In the case of video surveillance, because the captured video is used as evidence, the retention period for the entire recording, or only portions of it, varies by judicial district. However, video is generally only stored within the Video Evidence Collection System for the duration of an investigation. Once the investigation is complete, the data is either removed from the Video Evidence Collection System and stored as digital evidence or purged if there is no evidentiary value.

5. Principle of Use Limitation

Principle: U.S. Department of Homeland Security should use personally identifiable information solely for the purpose(s) specified in the notice. Sharing personally identifiable information outside the Department should be for a purpose compatible with the purpose for which the personally identifiable information was collected.

As a matter of policy, reflected in this Privacy Impact Assessment, and in the applicable Privacy Act Systems of Record Notices that describe Immigration and Customs Enforcement's purposes for collecting data, Immigration and Customs Enforcement only retains information collected from surveillance technologies discussed here (body wire, video surveillance, small Unmanned Aircraft Systems, location tracking, cell-site simulators, and license plate readers) linked or connected to a person of law enforcement interest or connected to a criminal activity.

ICE only shares information with agencies outside of U.S. Department of Homeland Security consistent with the Privacy Act, the routine uses published in the relevant Systems of Record Notices (e.g., External Investigations), and pursuant to information sharing agreements with other agencies. When Immigration and Customs Enforcement enters into Memoranda of

[56] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0567-2015-0016-0001, U.S. DEPARTMENT OF HOMELAND SECURITY, FUGITIVE OPERATIONS SCHEDULE, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2015-0016_sf115.pdf.

Agreement with outside partners (e.g., federal and state law enforcement, task forces), agents who access information captured by surveillance equipment are required to comply with Immigration and Customs Enforcement Rules of Behavior covering access to and appropriate use of the data. Immigration and Customs Enforcement Rules of Behavior limit the use of the data to only for authorized law enforcement purposes, have strict criteria for creating alerts, prohibit *ad hoc* and historical queries, specify the timeframes for refreshing alerts, and have a requirement to manually verify the accuracy of data contained within notifications.

Privacy Risk: There is a risk that surveillance technologies will be used for purposes beyond those described in this Privacy Impact Assessment.

Mitigation: This risk is mitigated. Individuals responsible for the use and oversight of electronic surveillance technologies must take basic law enforcement and technical training. The individual sections of the Technical Operations Unit implement their own procedures to mitigate the risk that surveillance technologies will be used for purposes beyond those articulated in this Privacy Impact Assessment. For instance, a judge authorizing a Title III interception may require periodic progress reports. These progress reports should contain enough summarized excerpts from intercepted conversations to establish that there is still probable cause for the interception. Any new investigative information pertinent to the interception, such as newly identified subjects or the addition of new violations, will be brought to the court's attention in the progress reports and then included in the next extension request (if an extension is sought). The duration of a Title III interception is also limited by federal law. No court order entered under 18 U.S.C. § 2518 may authorize or approve interceptions of wire, oral, or electronic communications for a period longer than is necessary to achieve the objective of the authorization, or in any event no longer than 30 days, or as otherwise extended by the court. In the event the court order needs to be extended or expanded, the supervising attorney is notified. If the existing court order is not expanded to include the new information, then a separate order will be required to disclose any such "other offense" in any state or federal proceeding.

The implementation of location tracking technology access controls helps mitigate the risk that the surveillance technology will be used for purposes beyond those described in this Privacy Impact Assessment. Specifically, data collected by the National Tracking Program's central tracking server is accessible only by authorized account users with a valid need-to-know. The National Tracking Program implemented multi-factor authentication for all user accounts. National Tracking Program users are authorized either by the National Tracking Program manager or by their local field level Technical Enforcement Officer. Additionally, Technical Enforcement Officers must attend a minimum of 80 hours of electronic surveillance training annually. Homeland Security Investigations trains law enforcement personnel to only consider and record relevant, accurate information in order to build a strong case for prosecution. In addition, as described in Section 8 (below), all Immigration and Customs Enforcement employees must

complete annual privacy awareness training via the Performance and Learning Management System (PALMS).[57]

As with location tracking technology, Immigration and Customs Enforcement implements controls to its use of cell-site simulators to mitigate this risk. Specifically, prior to the court order application for the deployment of this technology, the use of a cell-site simulator must be approved by a Homeland Security Investigations supervisor and an Assistant United States Attorney (AUSA). Any exigent or emergency use of a cell-site simulator must also be approved by an appropriate second-level supervisor and Assistant United States Attorney (AUSA) prior to its use.

Regarding small Unmanned Aircraft Systems, only authorized personnel who pass the Federal Aviation Administration Part 107 exam and receive a flight evaluation from a senior pilot, or attend a Homeland Security Investigations approved small Unmanned Aircraft Systems training course, may pilot small Unmanned Aircraft Systems. Those using the license plate reader service must complete training to ensure they use the service appropriately and understand the privacy, civil rights, and civil liberties safeguards. Immigration and Customs Enforcement helps ensure that its personnel use license plate reader for its intended purpose by requiring the vendor's license plate reader data service to maintain an immutable log of queries of the license plate reader data. This log will be reviewed quarterly or more frequently by Immigration and Customs Enforcement supervisory personnel to ensure that license plate reader data is accessed for authorized purposes only. Anomalies in the audit trail that reveal inappropriate activity will be referred to the Immigration and Customs Enforcement Office of Professional Responsibility (OPR) for further action.

6. Principle of Data Quality and Integrity

Principle: U.S. Department of Homeland Security should, to the extent practical, ensure that personally identifiable information is accurate, relevant, timely, and complete, within the context of each use of the personally identifiable information.

All electronically intercepted data and media on which it is recorded, regardless of quality or apparent usefulness, will be handled and preserved to facilitate admissibility as evidence for trial. Federal law (18 U.S.C. § 2518(8)(a)) requires that recordings of intercepted conversations be sealed immediately upon the expiration of the court order or any extensions. The purpose of the sealing requirement is to preserve the integrity of the evidence. Immediately upon termination of the interception, or when otherwise directed in the court order, the primary evidence of the interceptions must be submitted to the judge authorizing the interception and sealed personally by the judge or by the special agent under the supervision of the judge.

[57] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE PERFORMANCE AND LEARNING MANAGEMENT SYSTEM (PALMS), DHS/ALL/PIA-049, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

In consensual interceptions (e.g., use of a body wire) the majority of audio/video devices use software to validate and authenticate the recordings to verify that a true recording occurred without data manipulation. The evidence collected from a computer intercept will be stored on a removable storage media. A copy of this evidence is also maintained on a separate drive as the working copy. Similarly, if a small Unmanned Aircraft Systems records its surveillance, then the video is transferred onto a DVD where it is stored in a locked custody locker.[58]

As discussed regarding cell-site simulators, after completing a mission, an operator will document whether any useful information was obtained in a Report of Investigation and, if so, provide a description of the information. Homeland Security Investigations stores the Report of Investigation in the appropriate investigative case file and retains it in accordance with the applicable records retention schedule. Prior to deploying cell-site simulator equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data. Cell-site simulators used by special agents and Technical Enforcement Officers must be configured as pen registers, which requires a search warrant, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes the contents of any communication stored on the device itself. Cell-site simulators do not remotely capture emails, texts, contact lists, images or any other data from the device.

Privacy Risk: There is a risk that the data collected by Homeland Security Investigations Surveillance Technologies is inaccurate or may be manipulated.

Mitigation: This risk is mitigated. Homeland Security Investigations takes significant precautions to ensure that the integrity and accuracy of its data is maintained for both consensual and non-consensual surveillance. Homeland Security Investigations agents undergo training to ensure data accuracy and that manipulating data or misusing data could result in consequences against the user. Concerning non-consensual surveillance specifically, as discussed above, the recordings of intercepted conversations are sealed immediately upon the expiration of the court order or any extensions, as required by federal law. Furthermore, the primary evidence of the interceptions must be submitted to the judge authorizing the interception and sealed personally by the judge or by the special agent under the supervision of the judge. Regarding consensual surveillance, these technologies help promote accuracy as a majority of the audio/video devices utilize technology to validate and authenticate the recordings.

For cell-site simulators, the case agent or operator must first obtain the requisite internal approval to use a pen register before using a cell-site simulator. In order to comply with the terms of this policy and with 18 U.S.C. § 3125, the case agent or operator must contact the duty Assistant United States Attorney in the local U.S. Attorney's Office, who will coordinate approval within the Department of Justice. Upon approval, the Assistant United States Attorney, or state or local prosecutor, must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125.

[58] Individuals will not be linked to recordings by using software to validate any videos.

Under the provisions of the pen register statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or after 48 hours, whichever comes first.

At the conclusion of an unmanned aircraft flight where images or video recordings were collected, the Remote Pilot in Command will transfer the video onto a DVD where it is securely stored in a locked custody locker as soon as practical, no later than three business days following the flight, to preserve its integrity.

For the use of license plate reader technology, as discussed, Immigration and Customs Enforcement does not take enforcement action against any individual based solely on the information obtained from the vendor's license plate reader service. Authorized Immigration and Customs Enforcement personnel receive training to verify all accessed data is relevant to ongoing investigative and enforcement activities. Agency guidance pertaining to the use of license plate reader Data and technology includes a requirement to manually verify the accuracy of data contained within the notifications that provide agents with real-time location information so that they may take action, if appropriate.

7. Principle of Security

Principle: U.S. Department of Homeland Security should protect personally identifiable information (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Homeland Security Investigations limits access to surveillance technology and the information collected to only authorized users with a need-to-know to perform their official duties in connection with a particular investigation. In location tracking, moreover, several security and privacy precautions are taken to protect the communications between the tracking devices and the central tracking server. As mentioned previously, data collected by the server is distributed only to authorized users and only for the requested period via a secure connection. National Tracking Program users are authorized either by the National Tracking Program manager or by the case agent. In order to use a tracking device in a multi-agency operation, the case agent must submit a request to National Tracking Program—a "Tracking Support Request"—that must include an operational plan, the type and identifying information of the device, a deployment plan, the names of those who require access to the data, and other information required for proper system management. The National Tracking Program Tracking server system allows for input of the court ordered tracking warrant inclusive dates, in order to prevent over-collection of geo-location data captured by the device.

Privacy Risk: There is a risk that information collected by Homeland Security Investigations Surveillance Technologies will be inappropriately accessed.

Mitigation: This risk is mitigated. Homeland Security Investigations limits access to surveillance technology and the information collected to only authorized users, with a need-to-know, as pre-defined by user access roles established by their respective offices based on the individual's position and duties, to perform their official duties in connection with a particular investigation.

For example, Homeland Security Investigations has established management and role-based access controls to ensure only authorized personnel have access to the information collected and processed using the cell-site simulator technology. After completing a mission, an operator of a cell-site simulator will document whether any useful information was discovered in a Report of Investigation, which will be stored in the appropriate investigative case file in the Investigative Case Management system.[59] Investigative Case Management system users have role-based permissions and role-based training is required. Roles are defined by job position, duty, and office assignment, and users are granted the lowest level of privileges necessary to perform their job-related responsibilities related to their assignment on the case. Additionally, the audit logs for the Investigative Case Management system capture user activity including, but not limited to, uploading records or data, extracting information from the system, resolving entities, searches, and viewing records.

For the use of license plate reader technology, Immigration and Customs Enforcement requires the vendor's commercial license plate reader data service to maintain an immutable log of queries of the license plate reader data, and this log will be reviewed quarterly or more frequently by Immigration and Customs Enforcement supervisory personnel to ensure that license plate reader data has been accessed for authorized purposes only. Anomalies in the audit trail that reveal inappropriate activity will be referred to Immigration and Customs Enforcement Office of Professional Responsibility for further action. Immigration and Customs Enforcement will ensure, through contract requirements, that any vendor supplying license plate reader data to Immigration and Customs Enforcement employ data security technologies comparable to those required of Immigration and Customs Enforcement systems in order to protect the integrity of its data from hacking and other risks.

Furthermore, during the course of an investigation using video surveillance technology, authorized system administrators grant Task Force Officers and prosecuting attorneys' credentials to access the Video Evidence Collection System via a secure web portal. However, access is restricted to cases (live or archived) to which the Task Force Officers and prosecuting attorneys have a valid need-to-know. To further ensure that information will not be inappropriately accessed, Homeland Security Investigations encrypts all recorded video data using appropriate system

[59] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT (ICM), DHS/ICE/PIA-044, *available at* https://www.dhs.gov/privacy-documents-ice.

encryption software. An access key is provided to the user which allows access to the recorded data.

8. Principle of Accountability and Auditing

Principle: U.S. Department of Homeland Security should be accountable for complying with these principles, providing training to all employees and contractors who use personally identifiable information, and should audit the actual use of personally identifiable information to demonstrate compliance with these principles and all applicable privacy protection requirements.

ICE offices must conduct comprehensive, annual self-inspections of their respective technical operations, and report their level of compliance to Immigration and Customs Enforcement's Office of Professional Responsibility. Specifically, questions asked in Homeland Security Investigations' self-inspection include whether an Electronic Surveillance Request authorization received approval for the period of time in which monitoring occurred; whether personnel store electronic surveillance equipment in a controlled access area; and whether personnel properly label evidence. The results of these self-inspections must be certified as accurate by program leadership for the results to be considered official. Each Homeland Security Investigations office must maintain all documentation used to complete the self-inspection for a period of three years, including all supporting documentation, samples used to answer the questions, and any generated corrective action plans for self-identified deficiencies.

All Immigration and Customs Enforcement employees must also complete annual privacy awareness training in the Performance and Learning Management System. In addition, Homeland Security Investigations coordinates with the Federal Law Enforcement Training Centers (FLETC) to provide initial basic law enforcement and technical training to all individuals responsible for the use and oversight of electronic surveillance technologies. The initial law enforcement training consists of a basic course to be completed within six months of employment and a second phase to be completed within one year of employment. Newly hired Technical Enforcement Officers may not participate in field electronic surveillance or law enforcement functions without having first successfully completed the training. Due to the rapid changes and developments in electronic surveillance technology, and to ensure the proper and most efficient use of electronic surveillance systems, Technical Enforcement Officers must stay up to date with the law and technical systems. Technical Enforcement Officers must attend a minimum of 80 hours of electronic surveillance training annually.

Also, authorized Immigration and Customs Enforcement users, contractors, and other law enforcement personnel with access to license plate reader data must complete training that describes policy requirements and associated privacy, civil rights, and civil liberties safeguards. This supplements existing mandatory training required of all Immigration and Customs Enforcement personnel on data security, data privacy, integrity awareness, and records management. In addition, as an auditing measure, Immigration and Customs Enforcement users of

license plate readers must complete a mandatory free-text field to reference the specific case for which the query was performed. This provides information for an auditor to determine what led to the particular query.

Homeland Security Investigations requires a weekly wiretap report, used by the Title III National Program Manager, which identifies the current wiretaps in progress and those that are completed. This report includes the Homeland Security Investigations case number, target device identification, name of the affiant, date the court order was granted, online date, and off-line date. Additionally, in order to ensure accountability for cell-site simulators, the Homeland Security Investigations Assistant Director of Homeland Security Investigations' Information Management Directorate is charged with ensuring compliance with Homeland Security Investigations' cell-site simulator policy.

Additionally, the ICE Privacy Unit will continue working with appropriate Homeland Security Investigations stakeholders to ensure that the use of cell-site simulators and location tracking technologies remain in compliance with this Privacy Impact Assessment and will conduct additional oversight activities in response to audits or other reviews.

Privacy Risk: There is a risk that Homeland Security Investigations surveillance technologies are not in compliance with privacy principles and privacy program protection requirements.

Mitigation: This risk is mitigated. Concerning training, as described above, all sections of the Technical Operations Unit must complete annual privacy training in the Performance and Learning Management System. Additional training varies depending on the surveillance technologies at issue (as indicated above), including nondiscriminatory use of technology, validation of data, data security and privacy, permitted information sharing, and records management.

To ensure compliance with privacy principles, Immigration and Customs Enforcement offices must conduct annual self-inspections and report their level of compliance to Immigration and Customs Enforcement's Office of Professional Responsibility. Compliance includes whether an Electronic Surveillance Request authorization received approval for the period of time in which monitoring occurred; whether personnel store electronic surveillance equipment in a controlled access area; and whether personnel properly label evidence. Subsequently, the results of these self-inspections must be certified as accurate by program leadership for the results to be considered official.

Cell-site simulators must be used in a manner consistent with the requirements and protections of the United States Constitution, including the Fourth Amendment and applicable statutory authorities. Any information collected from cell-site simulators must be handled in a way that is consistent with applicable statutes, regulations, and policies that guide Homeland Security Investigations data collection, retention, and disclosure.

Homeland Security Investigations operates small Unmanned Aircraft Systems under the same Federal Aviation Administration regulations applicable to commercial and recreational small Unmanned Aircraft Systems users. The collection of video recordings must be in compliance with Homeland Security Investigations Directive 19-01 and must be approved by a Homeland Security Investigations supervisor in coordination with ICE counsel to ensure it is not used in any manner that would violate the individual's rights or target a person based on his or her race, color, religion, sex, sexual orientation, gender identity, or national origin.

The Immigration and Customs Enforcement Office of Information Governance and Privacy has issued guidance describing best practices when accessing and using license plate reader data and technology[60] and continues to work closely with Homeland Security Investigations to ensure that the privacy and civil liberties protections have been implemented.

Conclusion

Homeland Security Investigations deploys surveillance technologies in furtherance of its criminal investigations and national security missions. Surveillance technologies are valuable tools with which to collect evidence in a timely and efficient manner to establish a strong case for federal prosecution. It is incumbent on Homeland Security Investigations to ensure the use of sophisticated technology is accompanied by strict policies and procedures, as well as technical guidance for Technical Enforcement Officers, Intelligence Research Specialists, special agents, and other Homeland Security Investigations personnel conducting or supporting investigations involving surveillance equipment. Consensual interceptions, which are limited in duration, require prior approval, supervision, close monitoring, and coordination with the Assistant United States Attorney. The DHS, ICE, and Homeland Security Investigations policies and procedures regulating the use of surveillance equipment help to not only preserve the evidence in manner so it can be used in court, but also facilitate the protection of personal privacy and civil liberties during and after a surveillance operation.

Responsible Officials

Tracy Cormier
Acting Assistant Director
Office of Cyber and Operational Technology
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
(703) 551-5500

[60] The principles and practices Immigration and Customs Enforcement adheres to when accessing and using license plate reader data are described in agency guidance, "Privacy Guidance: Agency Access to and Use of License Plate Reader Data and Technology", issued June 15, 2021, from the Immigration and Customs Enforcement Office of Information Governance & Privacy.

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
(202) 732-3000

Approval Signature

Approved, signed copy on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717