OFFICE OF INSPECTOR GENERAL

~~LAW ENFORCEMENT SENSITIVE~~

# CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data (REDACTED)

~~LAW ENFORCEMENT SENSITIVE~~

**OFFICE OF INSPECTOR GENERAL**

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 28, 2023

MEMORANDUM FOR: The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2023.09.28 09:54:25 -04'00'

SUBJECT: *CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data* – ~~Law Enforcement Sensitive~~

Attached for your action is our final report, *CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data*. We incorporated the formal comments provided by your office.

The report contains eight recommendations aimed at improving policies and internal controls related to the use of commercial telemetry data. Your office concurred with six recommendations. Based on information provided in your response to the draft report, we consider recommendations 3, 4, and 6 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Based on information provided in your response to the draft report, we consider recommendations 1, 2, and 8 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Recommendations 5 and 7 are closed and resolved.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please contact me with any questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

cc: Troy A. Miller, Senior Official Performing the Duties of the Commissioner, U.S. Customs and Border Protection
Patrick J. Lechleitner, Senior Official Performing the Duties of the Director, U.S. Immigration and Customs Enforcement
Kimberly A. Cheatle, Director, United States Secret Service
Mason Clutter, Chief Privacy Officer
Robert Silvers, Under Secretary, Office of Strategy, Policy, and Plans
Garth White, Acting Chief Data Officer, Office of Chief Information Officer, Management Directorate

# DHS OIG HIGHLIGHTS

## *CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data*

**September 28, 2023**

## Why We Did This Audit

Department of Homeland Security law enforcement components use CTD for investigative purposes. CTD collected from mobile device applications and sold commercially may include historical device location. Our objective was to determine whether DHS and its components have developed, updated, and adhered to policies related to the use of CTD.

## What We Recommend

We made eight recommendations to improve policies and internal controls related to the use of CTD.

**For Further Information:**
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

## What We Found

U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the United States Secret Service (Secret Service) did not adhere to Department privacy policies or develop sufficient policies before procuring and using commercial telemetry data (CTD). Specifically, the components did not adhere to DHS' privacy policies and the *E-Government Act of 2002,* which require certain privacy-sensitive technology or data obtained from that technology, such as CTD, to have an approved Privacy Impact Assessment (PIA) before such technology is developed or procured. This occurred because the components did not have sufficient internal controls to ensure compliance with DHS privacy policies, and because the DHS Privacy Office did not follow or enforce its own privacy policies and guidance. Without a PIA in place, privacy risks may not be identified and mitigated.

Additionally, the components did not have sufficient policies and procedures to ensure appropriate use of CTD. According to CBP, its CTD rules of behavior were interim policies and procedures until complete policies and procedures were developed. ICE and Secret Service did not develop CTD-specific policies and procedures. PIAs are intended to identify privacy risks and mitigation strategies that may facilitate developing policies and procedures for ensuring proper use and oversight of CTD.

We also noted that the Department does not have a DHS-wide policy governing component use of CTD. Given the number of components using CTD and the significant congressional and public interest in the potential privacy implications with law enforcement use of CTD for investigative purposes, the Department should take a proactive approach to providing DHS-wide guidance.

## DHS Response

DHS concurred with 6 of 8 recommendations.

## Table of Contents



## Appendixes



## Abbreviations

| | |
|---|---|
| AdID | Advertising Identifier |
| BSS | Border Surveillance System |
| CBP | U.S. Customs and Border Protection |
| CTD | commercial telemetry data |
| HSI | Homeland Security Investigations |
| ICE | U.S. Immigration and Customs Enforcement |
| IT | information technology |
| PIA | Privacy Impact Assessment |
| PII | personally identifiable information |
| PTA | Privacy Threshold Analysis |
| SORN | System of Records Notice |

## Background

U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the United States Secret Service (Secret Service) are law enforcement components within the Department of Homeland Security. Collectively, these components' law enforcement missions include investigations related to countering terrorism; securing the border; and combating transnational crime, narcotics smuggling, human trafficking, gang activity, money laundering, and counterfeiting and other financial crimes. To conduct their investigations, CBP, ICE, and Secret Service have used commercially available geolocation data that provides historical mobile device locations related to criminal activity.

CBP, ICE, and Secret Service purchased access to commercial telemetry data (CTD) collected from mobile devices that included, among other things, historical device location.[1] Applications running on mobile devices use an Advertising Identifier (AdID)[2] unique to each device that can be used to track and record the device's historical location data and device information. The information collected may include time stamps, device type, operating system, and Global Positioning System coordinates. Commercial aggregators of AdID data sell access to users through licenses to the platforms. Subscribers access the data using the vendor's web-based portal. AdID data allows subscribers to historically identify a device's general location, which can be displayed on the vendor's website map. Subscribers can subsequently isolate a device of interest and analyze the device's historical locations over an extended period.

CBP, ICE, and Secret Service cited different uses of CTD for law enforcement intelligence purposes, [redacted]

[1] For this report, CTD refers only to commercial data that includes mobile device geolocation information derived from AdID data.
[2] The AdID is a unique identifier created and maintained by the mobile device's operating system and, as its name implies, is typically sent to advertisers, vendors, and other third parties for advertising purposes.

[redacted]

## *E-Government Act of 2002* and DHS Privacy Policies

Use of information technology (IT) or data obtained from that technology, such as CTD, within the Federal Government is controlled by the *E-Government Act of 2002* (the 2002 Act).[4] Congress passed the 2002 Act to, among other reasons, ensure sufficient protections for the privacy of personal information. Under Section 208 of the 2002 Act, agencies are required to conduct a Privacy

[3] *United States Constitution, 4th Amendment*: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[4] Public Law 107–347.

Impact Assessment (PIA) before developing or procuring IT that collects, maintains, or disseminates information in an identifiable form.[5]

A PIA provides an analysis of the privacy considerations posed and the steps an agency has taken to mitigate any impact on privacy.

The DHS Privacy Office (DHS Privacy) issued policies that provide guidance for preparing a PIA. A PIA describes what information an agency is collecting and why the information is collected; how the information will be used, stored, and shared; how the information may be accessed; how the information will be protected from unauthorized use or disclosure; and how long the information will be retained. A PIA also provides an analysis of the privacy considerations posed and the steps an agency has taken to mitigate any impact on privacy. DHS Privacy requires, reviews, and approves PIAs on technologies, rulemakings, programs, and activities, regardless of their type or classification, to ensure that privacy considerations and protections are incorporated into all activities of the Department under Section 208 of the 2002 Act, the *Homeland Security Act of 2002*,[6] and other statutes, as applicable.

DHS Privacy's *Privacy Policy and Compliance* instruction and included references[7] (DHS privacy policies) apply throughout DHS regarding the collection, use, maintenance, disclosure, deletion, and destruction of PII[8] and any other activity that impacts the privacy of individuals as determined by the DHS Chief Privacy Officer. DHS privacy policies describe the policies, procedures, and responsibilities to ensure PII is protected from unauthorized use or disclosure, including completion of the Privacy Threshold Analysis (PTA) and PIA, when required.

DHS Privacy developed the PTA form to help identify when an IT system, technology, rulemaking, program, or pilot project involves PII and to determine whether additional privacy compliance documentation is necessary. A PTA includes a general description of the IT system, technology, rulemaking,

---

[5] Office of Management and Budget M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, defines information in identifiable form as "information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."
[6] Public Law 107-296.
[7] DHS Instruction 047-01-001, *Privacy Policy and Compliance,* Revision 00, July 25, 2011.
[8] DHS Privacy defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

program, pilot project, or other Department activity and describes what PII is collected (and from whom) and how that information is used. In completed PTAs, DHS Privacy generally indicates whether the technology is privacy sensitive; whether PIA coverage is required, and if so, whether an existing PIA provides the requisite coverage or a new or updated PIA is required; and whether System of Records Notice (SORN) coverage is required, and if so, whether an existing SORN provides the requisite coverage or a new or updated SORN is required.

DHS privacy policies also clarify that pilot testing of a technology does not provide an exemption to the PIA requirement if DHS Privacy initially determines that a new or updated one is required. If a new or updated PIA is required for a technology, any testing of that technology must have the new or updated PIA completed prior to the pilot launch. This applies even if the pilot project will not initially use PII but may use PII as it moves out of the pilot phase. Completion of a new or updated PIA prior to launch of a pilot project ensures that privacy protections are considered during the development process instead of after the testing has concluded when changes would likely be more costly and time-consuming.

If a new or updated PIA is required for a technology, any testing of that technology must have the new or updated PIA completed prior to the pilot launch.

The objective of our audit was to determine whether DHS and its components have developed, updated, and adhered to policies related to the use of CTD.

## Results of Audit

CBP, ICE, and Secret Service did not adhere to Department privacy policies or develop sufficient policies before procuring and using CTD. Specifically, the components did not adhere to DHS' privacy policies and the 2002 Act by ensuring they had approved CTD PIAs. When DHS Privacy determines that a privacy-sensitive technology or data obtained from that technology, such as CTD, is required to have an approved PIA in place, the PIA must either already exist, or a new or updated PIA must be drafted and approved before such technology is developed or procured. This failure to adhere occurred because the components did not have sufficient internal controls to ensure compliance with DHS privacy policies, and because DHS Privacy did not follow or enforce its own privacy policies and guidance. Without a PIA, CBP, ICE, and Secret Service may not have identified and mitigated the privacy risks associated with CTD use.

Additionally, the components did not have sufficient policies and procedures to ensure appropriate use of CTD. According to CBP, its CTD rules of behavior were interim policies and procedures until complete policies and procedures were developed. An ICE official stated the component had not yet developed CTD-specific policies and procedures. According to a Secret Service official, the component did not believe CTD-specific policies and procedures were needed. PIAs are intended to identify privacy risks and mitigation strategies that may facilitate developing policies and procedures for ensuring proper use and oversight of CTD.

We also noted that the Department does not have a DHS-wide policy governing component use of CTD. Given the number of components using CTD and the significant congressional and public interest in the potential privacy implications with law enforcement use of CTD for investigative purposes, the Department should take a proactive approach to providing DHS-wide guidance.

## CBP, ICE, and Secret Service Did Not Adhere to Department Privacy Policies and the *E-Government Act of 2002* Before Procuring and Using CTD

Through our review of CBP, ICE, and Secret Service's procurement and use of CTD during fiscal years 2019 and 2020, we determined CBP had an approved PIA that included the use of CTD. However, the PIA did not include using CTD with other data to match an AdID to a specific person. ICE and Secret Service did not have approved PIAs for procuring and using CTD. Without approved PIAs, CBP, ICE, and Secret Service may not have identified and mitigated the privacy risks associated with CTD use.

DHS privacy policies provide guidance to ensure DHS complies with Section 208 of the 2002 Act for PIA requirements when PIA coverage is required. DHS' privacy compliance process begins with the drafting, reviewing, and adjudication of a PTA.[9] DHS Privacy uses PTAs to determine whether a technology is privacy sensitive, and whether the technology requires, among other things, new, existing, or updated PIA coverage. Once approved by DHS Privacy, the PTA includes an expiration date for the PTA. An official with DHS Privacy stated that although the approved PTA has an expiration date, this does not authorize components to use the technology before a new or updated PIA is approved, if one is required.

[9] The DHS privacy compliance process includes four steps: PTA, PIA, SORN, and periodic review.

Under Section 208 of the 2002 Act, and DHS privacy policies, if PIA coverage is required, agencies must conduct the PIA before developing or procuring IT that collects, maintains, or disseminates information in an identifiable form. The PIA includes an overview of the project's purpose, mission, and justification for operating a privacy-sensitive project. It should also include legal authorities for collecting the information, characterization and uses of the information, additional notice requirements and data retention, information sharing, redress and correction actions, and auditing and accountability processes and procedures. The PIA also identifies privacy risks and mitigation strategies to address those risks and ensures compliance with Federal privacy laws. Finally, DHS privacy policies do not exempt components from the requirement of having an approved PIA before pilot testing a technology.

> Agencies are required to conduct the PIA before developing or procuring IT that collects, maintains, or disseminates information in an identifiable form.

**CBP's CTD Related PIA Was Missing Information Related to CTD Use**

CBP's approved CTD-related PIA did not include the capability to associate CTD with other CBP technologies and open-source information to identify a user associated with a particular AdID. On August 21, 2018, CBP published an update to its Border Surveillance Systems (BSS) PIA. The updated BSS PIA incorporated several surveillance technologies, including commercially available location data. The PIA indicated that CBP planned to use commercially available data to "detect presence of individuals in areas between ports of entry where such presence is indicative of potential illicit or illegal activity." However, the PIA did not include [redacted]

> CBP's approved PIA did not include the capability to associate CTD with other CBP technologies and open-source information to identify a user associated with a particular AdID.

On December 1, 2018, CBP developed the PTA for its AdID Efficacy Pilot program, indicating that it planned to start the pilot program on May 1, 2019. CBP did not submit the PTA to DHS Privacy until August 16, 2019. In contrast to the BSS PIA, the AdID Efficacy Pilot PTA stated that the pilot program would review several commercially available AdID platforms to identify devices in locations of interest and, where necessary, analyze patterns of device movement on suspect devices. Also, according to the PTA, CBP intended to analyze and correlate suspect devices against both open-source and CBP data

to match the AdID to a specific person. DHS Privacy approved the AdID Efficacy Pilot PTA on September 30, 2020, with an expiration date of September 30, 2021. DHS Privacy indicated in the approved PTA that CBP's use of AdID was privacy sensitive and required a new PIA. Specifically, DHS Privacy noted:

> [DHS Privacy] agrees this is a privacy sensitive system that requires PIA coverage. A new PIA is required to discuss CBP's use of AdID. Because Components will have unique applications of this type of data, Component-specific PIA coverage is necessary. The DHS Privacy Office recommends that, in addition to the compliance coverage, Components develop Rules of Behavior and/or SOP/guidance for the use of AdID data. CBP should address how AdIDs become linked to an individual during the CBP analysis process, as well as the retention of AdID in the vendor system and within CBP systems with the associated linked PII. In addition, CBP should discuss the process of searching the platforms for a known AdID that CBP has previously identified outside of the platform, and the use of AdID for activity with identified terrorist predicate.

According to CBP officials, DHS Privacy's actions led them to believe that they could purchase and use CTD for the AdID Efficacy Pilot before completing a PIA. CBP believed it could use CTD while developing the PIA because the approved PTA had a 1-year expiration date and did not specifically prohibit CTD use before a new PIA was approved. According to CBP officials, DHS Privacy allows components 1 year to complete a PIA. During our review of PTAs, we noted on a separate PTA not associated with CTD that DHS Privacy explicitly stated, "CBP may proceed with the first phase of this initiative while the PIA is in development. *However, before any data is used operationally, the PIA must be completed* [emphasis added]," which supports CBP's assertion. Finally, CBP noted that DHS' Chief Information Officer approved CBP's FY 2020 CTD acquisition.

Although CBP acknowledged that the PTA expired in 1 year, the component continued to use CTD after the PTA expired. CBP was working on a CTD-related PIA as early as July 23, 2021, but at the time of our audit, this PIA had not been approved by DHS Privacy. As a result, CBP has used CTD since May 1, 2019, without an approved PIA that includes matching AdIDs to individuals.

Through our review, we found that CBP had six contracts for access to two CTD databases during FYs 2019 and 2020[10] and conducted over 55,000 queries[11] during this time.[12]

**ICE Used CTD Without Approved PIAs**

ICE used CTD during FYs 2019 and 2020 without approved PTAs and PIAs.

ICE Homeland Security Investigations (HSI), Enforcement and Removal Office, and Office of Professional Responsibility collectively purchased and used CTD during FYs 2019 and 2020 without approved PTAs and PIAs. Despite initially obtaining access to CTD in September 2018, ICE submitted its first two CTD-related PTAs to DHS Privacy on September 30, 2020. These PTAs were approved on November 17, 2020, and expired one year later. DHS Privacy noted on both PTAs that:

> [DHS Privacy] finds that a new ICE-specific PIA is required to provide a privacy analysis of ICE's use of geolocation data. The PIA must address how AdIDs become linked to an individual during the ICE analysis process, as well as the retention of AdID in the vendor system and within ICE systems with the associated linked PII. In addition, ICE should discuss the process of searching the platforms for a known AdID that ICE has previously identified outside of the platform, and the use of AdID for activity with identified terrorist/criminal predicate. ICE should prioritize completion of this PIA.

According to ICE officials, gaps in the procurement and privacy review process enabled program offices to use CTD without completing the PTA and PIA. DHS' *Homeland Security Acquisition Manual*, *Appendix G — Checklist for Sensitive Information* (checklist), is intended, in part, to determine whether a contractor requires access to sensitive information. The completed checklist is one of the required procurement documents associated with any DHS acquisition. Depending on the responses provided in the checklist by the requiring office, the procurement request is routed to various component officials for review. If a contractor requires access to particular categories of sensitive information,

[10] *See* Appendix C for details on CBP, ICE, and Secret Service contracts for CTD use in FYs 2019 and 2020.
[11] This represents the number of queries maintained in the audit logs provided by one database provider for FYs 2019 and 2020. The logs may contain duplicate queries of the same location and queries of multiple locations or device identifiers that are counted as a single query.
[12] CBP was not able to provide audit logs from one CTD database provider. A CBP official stated that the provider did not respond to the request.

DHS information systems, or Government facilities, the checklist may be routed to the component Privacy Officer who may determine what privacy-related language to include in the contract. If such access is not required, the component Privacy Officer does not have to review the procurement. Although the process is designed to ensure appropriate language is included in contracts, it does not always require review by the component Privacy Officer. If the component Privacy Officer does not review the procurement, the component Privacy Officer may not be aware of the acquisition of privacy-sensitive technology.

According to ICE, CTD contractors do not collect sensitive data or need to access facilities. Therefore, the ICE Privacy Office (ICE Privacy) did not see the checklist and the procurement request was sent directly to the ICE Office of Acquisition. Although the process associated with completing the checklist only ensures the necessary language is included in a contract, ICE program office personnel mistakenly assumed that operational use of CTD was permitted because ICE Privacy did not contact them or inform them that additional documentation was required. According to one ICE Privacy official, because the AdID geolocation data was "anonymized" it did not constitute PII. Thus, these program offices determined that their acquisition was "not privacy sensitive," and ICE Privacy did not need to be engaged.

Similar to CBP, ICE officials stated it was their understanding that if an approved PTA indicates a new or updated PIA is required, components may begin using the technology operationally as long as they submit a PIA to DHS Privacy within the time period of the PTA or request an extension. According to ICE, if DHS Privacy determines ICE does not have an existing PIA that addresses a new technology, it may require, at its discretion, that a PIA be published prior to operational use of the technology. Otherwise, ICE assumes DHS Privacy allows operations while a component develops its PIA. ICE has an undated draft CTD-related PIA, but at the time of our audit it had not been approved by DHS Privacy. As a result, ICE has used CTD since September 2018 without an approved PIA.

In our review, we found that ICE had nine contracts for access to two CTD databases during FYs 2019 and 2020 and conducted over 16,000 queries[13] during FY 2020.[14]

[13] This represents the number of queries maintained in the audit logs from one database provider for FY 2020. The logs may contain duplicate queries of the same location and queries of multiple locations or device identifiers that are counted as a single query.
[14] ICE's FY 2019 and 2020 CTD contracts included different CTD database providers. The FY 2020 database provider supplied complete audit logs. However, the FY 2019 database provider

**Secret Service Procured Licenses to Use CTD Without a PTA or PIA**

In September 2018, Secret Service procured 25 licenses to use CTD but did not have a PTA or PIA prepared or approved. Secret Service officials could not provide a reason for not completing a PTA or PIA because the personnel responsible for completing and submitting these documents during procurement are no longer with the component. Secret Service suspended CTD use during FY 2021 but procured the technology again in September 2021 for licensing in FY 2022. Prior to this procurement, the Secret Service Office of Investigations updated an existing Field Investigative Reporting System PTA to incorporate use of commercially and publicly available data services. DHS Privacy approved the updated PTA on July 13, 2021, indicating that the system was privacy sensitive.

Secret Service procured 25 licenses to use CTD but did not have a PTA or PIA prepared or approved.

To fully comply with the PIA requirements of the 2002 Act, Secret Service should have updated the existing Field Investigative Reporting System PIA before using CTD. According to an official in the Secret Service Office of Intergovernmental and Legislative Affairs, Secret Service submitted an updated PIA to DHS Privacy on December 3, 2021. The official stated that after waiting 6 months following the FY 2022 procurement for DHS Privacy to approve the PIA, Secret Service decided the operational need to use CTD superseded the requirement to have an approved PIA. On February 23, 2023, DHS Privacy approved Secret Service's Field Investigative Reporting System PIA update that included CTD use. Although the PIA was ultimately updated and approved, Secret Service used CTD from September 28, 2018, through September 29, 2020, and from September 27, 2021, until September 23, 2022, without an approved PIA.

[redacted]

did not. According to ICE officials, the provider indicated that the audit logs could not be produced in the structure requested. Therefore, we were not able to determine the number of queries conducted in FY 2019.

[redacted]

## DHS Privacy Office Did Not Follow or Enforce Its Privacy Policies and Guidance

DHS Privacy did not follow or enforce its own privacy policies and guidance. The 2002 Act; Office of Management and Budget, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*; and DHS privacy policies require PIAs to be completed before technology is procured, when it is determined that new or updated PIA coverage is required for the system or technology. According to *Privacy Impact Assessments, The Privacy Office Official Guidance,* June 2010:

> If a PIA is ultimately required for a system, any pilot of that system must have the PIA completed prior to the pilot launch. This applies even if the pilot initially plans to use anonymous data but will use personally identifiable information as it moves out of pilot. This is because the decisions affecting privacy are made leading up to the initiation of a pilot. Completion of a PIA prior to launch of a pilot ensures that privacy protections are considered during the development process instead of after a pilot has concluded when changes are potentially more costly and time-consuming.

Although this guidance requires a PIA before procurement, according to DHS Privacy, some technologies need to be procured and used to gather information necessary to complete PIAs. DHS Privacy clarified that once the PTA is approved and it is determined a new or updated PIA is needed, the component is expected to procure the technology for non-operational, limited-use testing to gain an understanding of the limitations and risks associated with the technology needed to create a PIA. In these instances, the component can only use the technology operationally after the PIA is approved. on-operational piloting of technologies prior to PIA approval is inconsistent with DHS' privacy policy.

According to DHS Privacy, some technologies need to be procured and used to gather information necessary to complete PIAs.

Our review of DHS Privacy-approved CBP and ICE PTAs showed the components intended to use CTD operationally and did not limit themselves to non-operational use prior to completing a PIA. For example, although CBP's AdID Efficacy Pilot PTA was characterized as a "pilot," the PTA indicated that "[a]ll information acquired during the testing and evaluation phase will be focused on AdIDs associated with cross border criminal activity and/or activity with an identified terrorist/criminal predicate." DHS Privacy approved CBP's FY 2020 CTD acquisition, which was signed by the DHS Chief Information

Officer on September 12, 2019.

ICE's PTAs provided examples of how the CTD would be used. [redacted] ICE's PTAs submitted to DHS Privacy indicated ICE had already procured 42 licenses for query-based access to a vendor-owned commercial geolocation data service. Based on CBP's and ICE's own language, DHS Privacy was aware when it approved the CBP and ICE PTAs that the components had already procured access to CTD without approved PIAs and that they intended to use it operationally.

## CBP, ICE, and Secret Service Did Not Develop Sufficient Policies and Procedures for CTD Use

Through our review of CBP's, ICE's, and Secret Service's use of CTD during FYs 2019 and 2020, we determined the components did not develop sufficient policies and procedures to govern the use of CTD. The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* provides Federal agencies with the criteria for designing, implementing, and operating an effective internal control system. Internal controls are processes that provide reasonable assurance that the objectives of a program will be achieved. For example, management should identify, analyze, and respond to risks and establish and operate monitoring activities.

[redacted]

CBP developed CTD-specific rules of behavior that provided guidance for various aspects of use, such as linking of queries to ongoing investigations, user access levels, and data storage, but CBP did not develop policies or procedures to ensure compliance with those rules of behavior and sufficient oversight of CTD use. According to a CBP official, the rules of behavior were interim CTD policies and procedures until complete policies and procedures were developed. ICE developed general IT rules of behavior that provided broad guidance such as requiring users to protect PII, not manipulate software applications, and lock workstations when not in use. However, ICE did not develop policies or procedures for the use of CTD and oversight of that use. Secret Service did not develop any policies or procedures specific to using CTD.

We interviewed 13 CBP CTD users, 7 ICE CTD users, and 5 Secret Service CTD users. Our interviews revealed CTD oversight gaps at CBP, ICE, and Secret Service such as:

- shared accounts and passwords;
- ad hoc methods for maintaining records; and
- no supervisory review to ensure proper use of the technology.

In addition to these oversight gaps, we identified one instance in which, unrelated to an investigation, a CBP employee used CTD inappropriately to track coworkers. The individual told the coworkers they had tracked their location using CTD. According to CBP, the complaint was reported by an ICE employee on August 20, 2020. The incident was reported to CBP's Joint Intake Center and Office of Professional Responsibility and was resolved administratively.

It is unlikely the inappropriate use of CTD would have been discovered due to the lack of policies and procedures governing CTD oversight requirements.

Procedures such as supervisory review of audit logs, which provide details of each CTD query, could deter and detect misuse of the technology. For example, the audit logs can include information such as user log-in names, time stamps, "hashed identifier," and Global Positioning System coordinates. CBP officials stated that although CTD vendors can provide audit logs associated with queries, no CBP supervisors have requested the logs. ICE program office officials who manage access for many CTD users believed supervision requirements were the responsibility of each CTD user's supervisor. None of the supervisors we interviewed mentioned using audit logs, evaluating CTD queries, or providing any other supervisory review of CTD use. A Secret Service official was unaware of audit logs.

CBP, ICE, and Secret Service noted various reasons for not having policies and procedures governing CTD use. According to CBP officials, CBP's rules of behavior are temporary guidance until the AdID Efficacy Pilot program is completed.[17] At that point CBP intends to develop comprehensive policies and procedures as a general control activity. ICE HSI officials stated they were only responsible for access to CTD. They said the ICE Office of Information Governance and Privacy was responsible for designing control activities, and the field offices were responsible for monitoring and supervising through

[17] According to CBP's AdID Efficacy Pilot PTA, dated December 1, 2018, and approved by DHS Privacy on September 30, 2020, CBP planned to pilot AdID from May 1, 2019, through May 1, 2021.

enforcement of these control activities. According to ICE Information Governance and Privacy, ICE is developing Geolocation Services rules of behavior. Secret Service officials stated that, with their limited use of CTD, they did not believe developing CTD-specific policies or procedures was necessary. Despite the components' reasons for not developing and implementing CTD policies and procedures, they also did not complete the PIA, as previously discussed. PIAs are intended to identify privacy risks and mitigation strategies that may facilitate developing policies and procedures for ensuring proper use and oversight of CTD.

We also noted that the Department does not have a DHS-wide policy governing component use of CTD. Given the number of components using CTD and the significant congressional and public interest in the potential privacy implications with law enforcement use of CTD for investigative purposes, the Department should take a proactive approach to providing DHS-wide guidance. Additionally, other DHS component offices may be using CTD without DHS Privacy's knowledge and without an approved PTA and PIA. This could occur if a component procures the technology through a different means, such as a vendor's free trial or a local acquisition process and does not notify DHS Privacy or submit a PTA. A department-wide CTD policy could help ensure consistent CTD use and proper oversight to protect privacy and reduce litigation exposure. In 2022, the Department created a commercial data working group to review the use of commercial data use throughout the Department. As of April 2023, the DHS commercial data working group has not issued a policy for commercial data use.

## Recommendations

**Recommendation 1:** We recommend that the Commissioner, U.S. Customs and Border Protection discontinue use of commercial telemetry data until the Privacy Impact Assessments are completed and approved.

**Recommendation 2:** We recommend that the Commissioner, U.S. Customs and Border Protection develop and implement controls to ensure compliance with DHS privacy policies, specifically approval of Privacy Impact Assessments, when required, before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.

**Recommendation 3:** We recommend that the Director, U.S. Immigration and Customs Enforcement discontinue use of commercial telemetry data until the Privacy Impact Assessments are completed and approved.

**Recommendation 4:** We recommend that the Director, U.S. Immigration and Customs Enforcement develop and implement controls to ensure compliance with DHS privacy policies, specifically approval of Privacy Impact Assessments, when required, before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.

**Recommendation 5:** We recommend that the Director, United States Secret Service develop and implement controls to ensure compliance with DHS privacy policies, specifically approval of Privacy Impact Assessments, when required, before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.

**Recommendation 6:** We recommend that the Chief Privacy Officer, DHS Privacy Office include a statement on approved Privacy Threshold Analyses that use of the project, program, or system determined to be privacy sensitive is not authorized for operational use until approval of the required Privacy Impact Assessment.

**Recommendation 7:** We recommend that the Chief Privacy Officer, DHS Privacy Office ensure compliance with its privacy policies or revise them to include the guidance necessary for program offices to meet the intent of the privacy requirements when, with due diligence, the technology needs to be procured and tested to complete the Privacy Impact Assessment process. The additional guidance, if developed, should address justification for deviating from Privacy Impact Assessment–related privacy policies and restrictions on the operational use of privacy-sensitive information; the guidance should also ensure Privacy Impact Assessments are completed before privacy-sensitive information is collected and used operationally.

**Recommendation 8:** We recommend that the Chief Data Officer, Office of Chief Information Officer, Management Directorate develop and implement a department-wide commercial telemetry data policy, including component policy requirements, to ensure oversight of commercial telemetry data use, privacy protection, and applicable legal standards.

## Management Comments and OIG Analysis

The Department provided written comments in response to a draft of this report. We reviewed the Department's comments, as well as technical comments received separately, and revised the report as appropriate. We have included a copy of the comments in their entirety in Appendix B. A summary of DHS' response to each recommendation with our analysis follows.

**DHS Response to Recommendation 1:** Concur. CBP's Office of Field Operations National Targeting Center does not intend to renew existing contracts for the use of CTD, which are set to expire September 21, 2023, but will use existing CTD until such contracts lapse. However, the CBP Privacy and Diversity Office is currently drafting a PIA detailing the privacy risks and mitigations associated with the past limited use of CTD by select CBP users during the time period for which CBP contracted access to this information.

Estimated Completion Date: March 29, 2024.

**OIG Analysis:** CBP's actions meet the intent of the recommendation. The recommendation will remain open and resolved until support for the contract expiration dates is provided and CBP confirms that the CTD contracts were not renewed.

**DHS Response to Recommendation 2:** Concur. CBP's Privacy and Diversity Office will assess compliance with CBP Directive 2120-010A, *Privacy Policy, Compliance, and Implementation,* dated June 29, 2022. The office will also assess compliance with the following DHS documents and determine whether additional guidance is required for CBP procurement of privacy-sensitive technologies:

- CBP Directive 2120-010A, *Privacy Policy, Compliance, and Implementation*, dated June 29, 2022
- DHS Directive 047-01, *Privacy Policy and Compliance*, dated July 7, 2011
- DHS Instruction 047-01-001, *Privacy Policy and Compliance*, Revision 00, dated July 25, 2011

Estimated Completion Date: March 29, 2024.

**OIG Analysis:** CBP's planned corrective actions meet the intent of the recommendation. This recommendation will remain open and resolved until CBP provides the results of its assessments and any operational changes it incorporated to prevent a recurrence of CBP noncompliance with privacy policies.

**DHS Response to Recommendation 3:** Non-concur. CTD is an important mission contributor to the ICE investigative process as, in combination with other information and investigative methods, it can fill knowledge gaps and produce investigative leads that might otherwise remain hidden. Accordingly, continued use of CTD enables ICE HSI to successfully accomplish its law enforcement mission.

ICE Privacy is currently working to finalize its Geolocation Services PIA in quarter 1 of FY 2024, subject to DHS Chief Privacy Officer review and approval, to provide appropriate transparency to the public regarding ICE CTD use. Additionally, ICE Privacy worked with ICE HSI to develop formal privacy-focused geolocation training and rules of behavior, both of which ICE anticipates finalizing before the end of FY 2023. Finally, ICE HSI has implemented privacy risk mitigation strategies at the individual user level, which will be documented in the draft Geolocation Services PIA.

ICE also notes that the CTD technologies HSI uses do not directly correlate an individual to a device. All devices are masked by vendor-generated device numbers, and no information in identifiable form (i.e., PII) is contained in the tool. To correlate a device with an individual, HSI must use other law enforcement techniques or procedures. In summary, CTD technologies are used as one mechanism for developing investigative leads. Traditional investigative techniques and legal process are required for further evidence gathering.

Estimated Completion Date: December 29, 2023.

**OIG Analysis:** ICE's response does not meet the intent of the recommendation, which is to ensure ICE complies with privacy requirements for a technology that DHS Privacy determined was privacy sensitive and required a PIA. ICE noted its progress in finalizing its Geolocation Services PIA, developing formal privacy-focused geolocation training and rules of behavior, and implementing privacy risk mitigation strategies at the individual user level, which will be documented in the draft Geolocation Services PIA. All of these actions are positive steps toward complying with privacy requirements.

However, these efforts do not negate that DHS Privacy determined on November 17, 2020, that using geolocation data is privacy sensitive and requires a PIA. Continued use of the geolocation data without an approved PIA violates DHS privacy policies, which ensure DHS complies with privacy considerations and incorporates protections into all activities of the Department under Section 208 of the 2002 Act, the *Homeland Security Act of 2002*, and other statutes, as applicable. This recommendation will remain open and unresolved until ICE completes PIA requirements or discontinues its non-compliant use of CTD.

**DHS Response to Recommendation 4:** Concur. ICE has already implemented controls to ensure it considered and addressed privacy impacts before acquiring CTD capabilities. Specifically, under ICE's procurement procedures, ICE Privacy is a key stakeholder in the pre-acquisition process. ICE components must also include in their procurement packages a completed

"ICE Privacy and Information Assurance Division Checklist" and a DHS Acquisition Manual Appendix G form, *Individual or Class Checklist for Controlled Unclassified Information*. Both of these forms require ICE Privacy review, in conjunction with proposed statements of work/performance work statements or other procurement documents (e.g., licensing agreements), as applicable.

In situations where ICE procurement involves access to or handling of sensitive information, including commercial data, the DHS Acquisition Manual Appendix G form also requires ICE Privacy Officer signature. In 2022, ICE Privacy updated both forms to specifically identify procurements involving commercial data as sensitive procurements requiring ICE Privacy review and, with respect to the Appendix G form, ICE Privacy Officer approval. These updates closed a gap in the procurement process that previously enabled some CTD capabilities to be procured without ICE Privacy Officer approval.

Additionally, in January 2021, ICE instituted a "commercial data pause" that required ICE operational components to obtain ICE Deputy Director approval before acquiring access to commercial data, which includes CTD. This pause remains in effect, pending any related forthcoming DHS-wide CTD policy recommended in our report.

ICE requests that we consider the recommendation closed and resolved, as implemented.

**OIG Analysis:** ICE's corrective actions appear to meet the intent of the recommendation, which ICE requested we consider closed and resolved. However, before closing the recommendation, we will assess support ICE provides for its implemented corrective actions. Without an estimated completion date, this recommendation will remain open and unresolved. Additionally, ICE must provide support that its procurement process cannot bypass ICE Privacy review, including the updated checklist ICE noted in its response.

**DHS Response to Recommendation 5:** Concur. In June 2022, Secret Service's Office of Intergovernmental and Legislative Affairs, Privacy Program, issued an internal privacy compliance policy outlining privacy requirements within Secret Service operations. Specifically, the policy describes the approval process for PTAs and PIAs required before the development or procurement of IT that collects, maintains, or disseminates information in an identifiable form. As part of the privacy compliance review process, the Secret Service Privacy Program works with the DHS Privacy Office, which subsequently determines whether additional privacy compliance documentation is required based on the

use, storage, or access to PII or sensitive PII. Secret Service requests that we consider the recommendation closed and resolved, as implemented.

**OIG Analysis:** Secret Service's corrective actions meet the intent of the recommendation. On July 25, 2023, Secret Service provided support that it issued IGL-04 USSS [Secret Service] *Privacy Compliance Policy,* dated June 28, 2022. The policy set forth an approval process for PTAs and PIAs required before the development or procurement of IT that collects, maintains, or disseminates information in an identifiable form. We consider this recommendation closed and resolved.

**DHS Response to Recommendation 6:** Concur. In June 2020, DHS Privacy added a section to the PTA template to specifically indicate whether a program or system is compliant. DHS Privacy revised this section in July 2023. DHS Privacy will provide us the updated PTA template under a separate cover.

Estimated Completion Date: September 29, 2023.

**OIG Analysis:** DHS Privacy's actions do not fully address this recommendation. On September 5, 2023, DHS Privacy provided a revised PTA template that specifically indicates whether a program or system is compliant. However, DHS Privacy's response and revised PTA template did not include language that the project, program, or system determined to be privacy sensitive is not authorized for operational use until the required PIA is approved. As indicated in our report, both CBP and ICE noted that they believed they could use CTD while developing the PIA because the approved PTAs had 1-year expiration dates and did not specifically prohibit CTD use before a PIA was approved. Additionally, DHS Privacy indicated that some technologies need to be procured and used to gather information necessary to complete PIAs. This recommendation will remain open and unresolved until DHS Privacy provides a corrective action plan, including an estimated completion date, to ensure components are aware that operational use of the project, program, or system is not authorized until approval of the required PIA.

**DHS Response to Recommendation 7:** Non-concur. DHS stated that OIG's recommendation that DHS privacy policies should allow for deviations from PIA-related policies when information in identifiable form is collected in a technology used by or on behalf of DHS. Doing so contradicts the legal requirements of the 2002 Act, which requires agencies to conduct a PIA before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public. DHS Instruction 047-01-001 is explicit that program managers and

system managers are responsible for coordinating with the Chief Privacy Officer and the Component Privacy Officer or Privacy Point of Contact to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any IT system, technology, regulation, rulemaking, program, or other activity, including pilot activities.

In addition, DHS Privacy implements the requirements established by Office of Management and Budget M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003, as well as the Chief Privacy Officer's statutory authority pursuant to 6 United States Code § 142, "Privacy officer," for PIAs to be completed before a system, program, or new technology is procured. DHS requests that we consider this recommendation closed and resolved.

**OIG Analysis:** DHS Privacy misinterpreted our recommendation. The intent of the recommendation was to provide DHS the option to either follow its privacy policies or implement controls that would permit non-operational testing of a technology by restricting the collection, maintenance, or dissemination of information in an identifiable form. As noted in our report, DHS Privacy indicated that some technologies need to be procured and used to gather information necessary to complete PIAs and that limited-use testing is used to gain an understanding of the limitations and risks associated with the technology needed to create a PIA. Nonetheless, DHS Privacy cited current privacy policies that require a PIA before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public, which is consistent with our recommendation. We consider this recommendation closed and resolved.

**DHS Response to Recommendation 8:** Concur. The DHS Office of the Chief Information Officer, in coordination with DHS Privacy, will lead a DHS-wide effort to develop a department-level CTD policy.

Estimated Completion Date: June 28, 2024.

**OIG Analysis:** DHS' corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved until DHS completes and issues the department-level CTD policy.

# Appendix A
# Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

Our original objective was to determine whether DHS and its components developed, updated, and adhered to policies related to the use of cell phone surveillance devices and commercial location-sharing databases. Our objective referenced two separate technologies: cell phone surveillance devices and commercial location-sharing databases. As a result, we are reporting our audit results separately based on the technologies. For this report, our objective was to determine whether DHS and its components have developed, updated, and adhered to policies related to the use of CTD. Our report, *Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators* (OIG-23-17), which addressed the Department's use of cell-site simulators, was issued on February 23, 2023.

The scope of this audit was the use of CTD during FYs 2019 and 2020. This review included only CTD that provides the geolocation of mobile devices derived from AdID. Other types of commercial data were not included in this review. To accomplish our objective, we surveyed 22 DHS headquarters offices and components and reviewed CTD procurement documents. Based on our survey, we determined that only CBP, ICE, and Secret Service used CTD within our scope period. However, a risk remains that other component offices were using CTD during FYs 2019 and 2020 without DHS Privacy's knowledge and without an approved PTA and PIA. DHS Privacy may be unaware of CTD use if a component procured the technology through a different means, such as a vendor's free trial or through its local acquisition process, and failed to notify DHS Privacy or submit a PTA.

We evaluated relevant Federal laws and regulations, as well as DHS guidance, policies, and procedures related to CTD; privacy requirements; and legal analysis. Specifically, we reviewed:

- *E-Government Act of 2002,* Section 208
- U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*, September 2014
- Office of Management and Budget, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*

- DHS Instruction 047-01-001, *Privacy Policy and Compliance*, Revision 00, July 25, 2011
- *Department of Homeland Security Acquisition Manual*, October 2009
- DHS Privacy Office, *Privacy Policy Guidance Memorandum*, Memorandum Number: 2008-02, December 30, 2008
- *DHS Privacy Impact Assessments, The Privacy Office Official Guidance, June 2010*

Due to COVID-19–related travel restrictions, we observed virtual demonstrations of two CTD platforms to understand the capabilities and limitations of the technology. Although travel was restricted, we accomplished our objective by reviewing CTD search query audit logs; interviewing CBP, ICE, and Secret Service officials; and corroborating evidence to support our findings.

To understand how DHS and components used CTD and adhered to Federal laws and DHS regulations, we interviewed officials from the DHS Offices of Strategy, Policy, and Plans; Privacy; Chief Security Officer; Civil Rights and Civil Liberties; and General Counsel. We also interviewed officials from the following operational components:

- Science and Technology Directorate
- United States Coast Guard
- CBP National Targeting Center and CBP Privacy and Diversity Office
- ICE HSI, Enforcement and Removal Operations, and Office of Information Governance and Privacy
- Secret Service Criminal Investigative Division, Investigative Support Division, and Office of Intergovernmental and Legislative Affairs

To determine compliance with Federal and DHS privacy requirements for privacy-sensitive technology or data obtained from that technology such as CTD, we analyzed the requirements and applied them to approved CBP, ICE, and Secret Service privacy documents.

We interviewed 13 CBP users of CTD, 7 ICE users, and 5 Secret Service users to assess the process for conducting queries and determine whether there were adequate controls in place to prevent CTD misuse. We reviewed partial vendor audit logs of queries conducted by CBP and ICE during June and July 2021. We judgmentally selected a sample of 84 queries conducted by ICE users out of a population of 2,853 and 243 queries conducted by CBP users out of a population of 7,221. We then contacted the CTD users to determine the purpose of the queries, reporting, and record keeping. We learned during these interviews that multiple queries can be associated with a single investigation.

We did not select a sample of queries for Secret Service because it did not procure licensing for the technology for FY 2021.

To assess the reliability of the audit logs, we conducted limited testing that included: (1) tracing audit search query data to the identified CTD users; (2) verifying that CTD user names matched the user names on the audit logs for the time period provided; (3) ensuring audit log entries matched the time periods of conducted queries reported by CBP, ICE, and Secret Service; and (4) discussing the purpose of the queries with CTD users to understand the intent of the queries.

Additionally, according to a CBP official, one vendor had never previously received a request for audit logs and therefore had to develop a process to create the logs we requested. The created audit logs were provided to CBP. However, CBP was unable to obtain audit logs from the second vendor. According to a CBP official, the second vendor did not respond to the request. ICE provided audit logs from the vendor it used in FY 2020. However, an ICE official stated that the vendor used during FY 2019 could not produce the audit logs we requested. Secret Service contracted with one vendor and provided complete audit logs for FYs 2019 and 2020. Overall, we determined the audit logs were sufficiently reliable to support conclusions presented in the report.

In planning and performing our audit, we identified the four internal control components and six underlying internal control principles significant to the audit objective. We planned and performed audit procedures necessary to assess the control environment, audit risk, control activities, and monitoring internal control components to address our audit objective. We identified internal control deficiencies that affected CBP, ICE, and Secret Service's compliance with Federal laws and DHS Privacy policies, which we included in the report.

We assessed the reliability of the information we received pertaining to CBP's, ICE's, and Secret Service's CTD use. Specifically, we:

- observed CBP and ICE demonstrations of CTD queries;
- reviewed vendor audit logs of CBP, ICE, and Secret Service queries conducted during FYs 2019 and 2020;
- compared procurement information obtained from the DHS components to publicly available Government procurement websites to ensure all contracts had been provided;
- conducted multiple interviews and communicated with the components to ensure we had adequate information to clarify and corroborate the evidence; and

- verified analysis with the component officials to ensure our findings were accurate.

We conducted this performance audit between February 2021 and April 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

**DHS OIG's Access to DHS Information**

During this audit, DHS provided timely responses to our requests for data, records, and information and did not deny or delay access to the data, records, and information we requested.

# Appendix B
# DHS Comments to the Draft Report

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

Homeland Security

September 7, 2023

MEMORANDUM FOR: Joseph V. Cuffari, PhD
Inspector General

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

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.09.07 13:30:04 -04'00'

SUBJECT: Management Response to Draft Report: "CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data" (Project No. 21-008-AUD-DHS(a))

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

DHS leadership is pleased to note OIG's recognition of the importance of geolocation data that U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE) and the U.S. Secret Service (USSS) use to accomplish their collective law enforcement missions, including investigations related to countering terrorism, securing the border, and combatting transnational crime, narcotics smuggling, human trafficking, gang activity, money laundering, and other financial crimes. DHS remains committed to assessing the privacy risk of DHS systems and programs, and developing and implementing mitigation strategies to safeguard individual privacy, as appropriate.

The draft report contained eight recommendations, including six with which the Department concurs (Recommendations 1, 2, 4, 5, 6 and 8) and two with which the Department non-concurs (Recommendations 3 and 7). Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity, and editorial issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Enclosure

**Enclosure: Management Response to Recommendations Contained in 21-008-AUD-DHS(a)**

OIG recommended that the CBP Commissioner:

**Recommendation 1:** Discontinue use of commercial telemetry data until the Privacy Impact Assessments are completed and approved.

**Response:** Concur. CBP's Office of Field Operations National Targeting Center does not intend to renew existing contracts for the use of commercial telemetry data (CTD), which are set to expire September 21, 2023, but will use existing telemetry data until such contracts lapse. However, the CBP Privacy and Diversity Office (PDO) is currently drafting a Privacy Impact Assessment (PIA) detailing the privacy risks and mitigations associated with the past limited use of CTD by select CBP users during the time period for which CBP contracted access to this information. Estimated Completion Date (ECD): March 29, 2024.

**Recommendation 2:** Develop and implement controls to ensure compliance with DHS privacy policies, specifically approval of Privacy Impact Assessments, when required, before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.

**Response:** Concur. CBP's PDO will assess compliance with CBP Directive 2120-010A, "Privacy Policy, Compliance, and Implementation," dated June 29, 2022, which requires CBP to coordinate with the CBP Privacy Officer to "ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any information technology system, technology, or other activity, including pilot activities, before any personally identifiable information (PII) is collected, used, or disclosed (e.g., … efforts involving the collection, use, or sharing of cellular phone and location data…)."

CBP PDO will also assess compliance with the following DHS documents and determine whether additional guidance is required for CBP procurement of privacy sensitive technologies:

- CBP Directive 2120-010A, "Privacy Policy, Compliance, and Implementation," dated June 29, 2022;[1]
- DHS Directive 047-01, "Privacy Policy and Compliance," dated July 7, 2011;[2] and
- DHS "Instruction 047-01-001, "Privacy Policy and Compliance," dated July 25, 2011.[3]

[1] https://www.cbp.gov/document/directives/cbp-directive-privacy-policy-compliance-and-implementation.
[2] https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01.
[3] https://www.dhs.gov/publication/privacy-policy-and-compliance-instruction-047-01-001.

ECD: March 29, 2024.

OIG recommended that the Director of ICE:

**Recommendation 3:** Discontinue use of commercial telemetry data until the Privacy Impact Assessments are completed and approved.

**ICE Response:** Non-concur. CTD is an important mission contributor to the ICE investigative process as, in combination with other information and investigative methods, it can fill knowledge gaps and produce investigative leads that might otherwise remain hidden. Accordingly, continued use of CTD enables ICE Homeland Security Investigations (HSI) to successfully accomplish its law enforcement mission.

ICE's Privacy Unit (ICE Privacy) is currently working to finalize its Geolocation Services PIA in quarter 1 of fiscal year (FY) 2024, subject to DHS Chief Privacy Officer review and approval, to provide appropriate transparency to the public regarding ICE CTD use. Additionally, ICE Privacy worked with ICE HSI to develop formal privacy-focused geolocation training and Rules of Behavior, both of which ICE anticipates finalizing before the end of FY 2023. Finally, ICE HSI has implemented the following privacy risk mitigation strategies at the individual user level, which will be documented in the draft Geolocation Services PIA:

- Only individuals supporting investigations are given access to technologies using CTD;
- Users receive Rules of Behavior training prior to receiving access to tools using CTD;
- Users receive annual training on First and Fourth Amendment protections; and
- Locations "geofenced" in CTD tools are predicated on investigative data directly corresponding to a suspected crime being, or having been, committed that HSI is investigating pursuant to its statutory authorities.

It is also important to clarify that, while a published PIA is important for oversight, compliance, and public transparency, it is not the sole mechanism through which ICE identifies privacy risks and develops and implements risk mitigation techniques. ICE Privacy is continually engaged with ICE HSI to ensure their use of CTD is consistent with their authority to collect and use information and otherwise aligns with federal requirements governing the collection, use, and maintenance of information.

Further, ICE Privacy develops Privacy Threshold Analyses (PTAs), consistent with DHS privacy policy requirements, on CTD capabilities through which the office analyzes privacy impacts of the particular use, and advises ICE HSI on requirements for mitigating any identified privacy risks. ICE Privacy uses the PTA process as a platform through which ICE Privacy works with ICE programs to mitigate any identified privacy risks in

advance of operational use. Accordingly, a PTA provides an initial privacy analysis wherein privacy risks are identified. PTAs must be submitted to, and adjudicated by, the DHS Privacy Office (PRIV) to determine whether a PIA and/or a System of Records Notice (SORN) is needed. In some circumstances, PRIV may determine a PTA is the only privacy compliance document required.

ICE also notes that the CTD technologies used by HSI do not directly correlate an individual to a device. All devices are masked by vendor-generated device numbers, and no information in identifiable form (synonymous with PII) is located in the tool. To correlate a device with an individual, HSI must use other law enforcement techniques or procedures. In summary, CTD technologies are used as one mechanism for developing investigative leads. Traditional investigative techniques and legal process are required for further evidence gathering.

ECD: December 29, 2023.

**Recommendation 4**: Develop and implement controls to ensure compliance with DHS privacy policies, specifically approval of Privacy Impact Assessments, when required, before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.

**ICE Response:** Concur. ICE has already implemented controls to ensure privacy impacts are considered and addressed before CTD capabilities are acquired. Specifically, under ICE's procurement procedures, ICE Privacy is a key stakeholder in the pre-acquisition process. ICE components must also include in their procurement packages a completed "ICE Privacy and Information Assurance Division Checklist" and a Department of Homeland Security Acquisition Manual (HSAM)[4] Appendix G form – "Individual or Class Checklist for Controlled Unclassified Information." Both of these forms require ICE Privacy review, in conjunction with proposed statements of work/performance work statements or other procurement documents (e.g., licensing agreements), as applicable. During the review process, ICE Privacy considers whether existing privacy compliance documentation (e.g., PTAs, PIAs, SORNs, etc.) covers the procurement, and includes this information in a written summary document provided to the ICE program point of contact and the Contracting Officer's Representative. ICE Privacy then works with the program to develop any additional required documents, as appropriate.

In situations where ICE procurement involves access to or handling of sensitive information, including commercial data, the HSAM Appendix G form also requires ICE Privacy Officer signature. In 2022, ICE Privacy updated both checklists to specifically identify procurements involving commercial data as sensitive procurements requiring

[4] https://www.dhs.gov/sites/default/files/2023-08/homeland-security-acquisition-manual-full-0727_0.pdf

ICE Privacy review and, with respect to the Appendix G, ICE Privacy Officer approval. These updates closed a gap in the procurement process that previously enabled some CTD capabilities to be procured without ICE Privacy Officer approval.

Additionally, in January 2021, ICE instituted a "Commercial Data Pause" that required ICE operational components to obtain ICE Deputy Director approval before acquiring access to commercial data, which includes CTD. This pause remains in effect, pending any related forthcoming DHS-wide CTD policy recommended in this OIG report ICE further instituted a process in December 2022 wherein ICE components are required to complete a form describing in detail the commercial data to be acquired, the mission need warranting an exception to the pause, and the controls in place to ensure data is protected and used appropriately. This form, once completed, is reviewed and cleared by the ICE Office of Information Governance and Privacy at the Deputy Assistant Director level (after being reviewed by the ICE Privacy Officer), as well as by the ICE Office of the Principal Legal Advisor, as a condition precedent of ICE Deputy Director approval. This process further ensures ICE Privacy has visibility and is able to conduct a privacy analysis prior to procurement of CTD.

We request that OIG consider the recommendation resolved and closed, as implemented.

OIG recommended that the Director of the Secret Service:

**Recommendation 5:** Develop and implement controls to ensure compliance with DHS privacy policies, specifically approval of Privacy Impact Assessments, when required, before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.

**Response:** Concur. In June 2022, Secret Service's Office of Intergovernmental and Legislative Affairs, Privacy Program, issued an internal Privacy Compliance Policy outlining privacy requirements within Secret Service operations. Specifically, the policy describes the approval process for PTAs and PIAs required prior to the development or procurement of information technology that collects, maintains, or disseminates information in an identifiable form. Additionally, the Secret Service Privacy Program, along with the Secret Service Chief Information Security Officer and Chief Security Officer, is embedded within the Secret Service acquisition process, thereby reviewing all new information technology to be procured. Moreover, as part of the privacy compliance review process, the Secret Service Privacy Program works in conjunction with the DHS Privacy Office, which subsequently makes a determination as to whether additional privacy compliance documentation is required based upon the use, storage, or access to PII or sensitive PII.

We request that OIG consider the recommendation resolved and closed, as implemented.

5

OIG recommended that the Chief Privacy Officer, PRIV:

**Recommendation 6:** Include a statement on approved Privacy Threshold Analyses that use of the project, program, or system determined to be privacy sensitive is not authorized for operational use until approval of the required Privacy Impact Assessment.

**Response:** Concur. In June 2020 (and later revised in July 2023), PRIV added a section to the PTA Template to specifically indicate whether a program or system is in compliance. PRIV will provide this PTA template to OIG under a separate cover. ECD: September 29, 2023.

**Recommendation 7:** Ensure compliance with its privacy policies or revise them to include the guidance necessary for program offices to meet the intent of the privacy requirements when, with due diligence, the technology needs to be procured and tested to complete the Privacy Impact Assessment process. The additional guidance, if developed, should address justification for deviating from Privacy Impact Assessment-related privacy policies and restrictions on the operational use of privacy sensitive information; the guidance should also ensure Privacy Impact Assessments are completed before privacy sensitive information is collected and used operationally.

**Response:** Non-concur. OIG's recommendation that DHS privacy policies should allow for deviations from PIA-related policies when information in identifiable form is collected in a technology used by or on behalf of DHS contradicts the legal requirements of the E-Government Act of 2002, which requires agencies to conduct a PIA before developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public. DHS Instruction 047-01-001 is explicit that Program Managers and System Managers are responsible for coordinating with the Chief Privacy Officer and the Component Privacy Officer or Privacy Point of Contact to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any IT system, technology, regulation, rulemaking, program, or other activity, including pilot activities.

In addition, PRIV implements the requirements established by the Office of Management and Budget M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," dated September 26, 2003,[5] as well as the Chief Privacy Officer's statutory authority pursuant to 6 United States Code § 142, "Privacy officer," for PIAs to be completed before a system, program, or new technology is procured.

We request that OIG consider this recommendation resolved and closed.

[5] M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 | The White House (archives.gov)

OIG recommended that the Chief Data Officer, Office of the Chief Information Officer (OCIO), Management Directorate:

**Recommendation 8:** Develop and implement a department-wide commercial telemetry data policy, including component policy requirements, to ensure oversight of commercial telemetry data use, privacy protection, and applicable legal standards.

**Response:** Concur. The DHS OCIO, in coordination with PRIV, will lead a DHS-wide effort to develop a department-level CTD policy. ECD: June 28, 2024.

7

## Appendix C
## CBP, ICE, and Secret Service CTD Contracts, FYs 2019 and 2020

| Component | Contract/Order Number | Period of Performance | Number of User Licenses |
|---|---|---|---|
| CBP | 70B04C18F00001093 | 9/21/2018 - 9/20/2019 | 20 |
| | 70B04C18F00001214 | 9/27/2018 - 9/26/2019 | 8 |
| | 70B04C19F00000798 | 9/21/2019 - 9/20/2020 | 20 |
| | 70B04C19F00000802 | 9/27/2019 - 9/25/2020 | 18 |
| | 70B02C20P00000521 | 9/10/2020 - 9/9/2021 | 1 |
| | 70B04C20F00000914 | 9/25/2020 - 9/14/2021 | 25 |
| ICE | 70CMSD18P00000127 | 9/30/2018 - 9/29/2019 | 10 |
| | 70CMSD19P00000012 | 2/15/2019 - 2/15/2020 | 2 |
| | 70CMSD19P000043 | 5/24/2019 - 5/23/2020 | 1 |
| | 70CMSD19A00000007 Base Year | 9/30/2019 – 9/29/2020 | 13 |
| | 70CMSD19A00000007 Amendment P00003 | 9/30/2020 – 9/29/2021 | 40 |
| | 70CMSD20P0000089 | 7/1/2020 - 6/30/2021 | 1 |
| | 70CMSD20P00000159 | 9/4/2020 - 9/3/2021 | 1 |
| | 70CTD020P000016 | 9/11/2020 - 9/10/2021 | 2 |
| | 70CMSD19A00000007 Option Year 1 | 9/30/2020 – 9/29/2021 | 13 |
| Secret Service | HSSS01-15-C-0040 Amendment 000007 | 9/28/2018 – 11/27/2018 | 25 |
| | HSHQDC-12-D-00011 | 9/30/2018 – 9/29/2019 | 6 |
| | 70US0919C70090057 | 9/30/2019 - 9/29/2020 | 13 |

Source: DHS OIG analysis of contracts provided by CBP, ICE, and Secret Service

# Appendix D
# Report Distribution

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Deputy Chief Privacy Officer, DHS Privacy Office
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commissioner, U.S. Customs and Border Protection
Director, U.S. Immigration and Customs Enforcement
Director, United States Secret Service
U.S. Customs and Border Protection Audit Liaison
U.S. Immigration and Customs Enforcement Audit Liaison
United States Secret Service Audit Liaison
DHS Privacy Office Audit Liaison
Office of Strategy, Policy, and Plans, Audit Liaison
Chief Data Officer, Office of Chief Information Officer, Management Directorate

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

## ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

## OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" box. If you cannot access our website, call our hotline at (800) 323-8603, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305