(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E) AREAS OF INTEREST

Background: (b) (7)(E) request for information dated (b) (7)(E). Named areas of interest in (b) (7)(E) associated to illicit alien operations with impacts to CBP operations.

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

~~FOR OFFICIAL USE ONLY// LAW ENFORCEMENT SENSITIVE// SENSITIVE SECURITY INFORMATION~~

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E) (b)(7)(E)

(b) (7)(E)

[redacted]

Issue:

(b) (7)(E) research into an alleged (b) (7)(E) migrant stash house (b) (7)(E) (b) (7)(E)

Synopsis:

(b) (7)(E)

Key Findings:

(b) (7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E)

[redacted]

(b)(7)(E)

[redacted]

(b)(7)(E)

[redacted]

U.S. Department of Homeland Security
U.S. Customs and Border Protection

[redacted] (b)(7)(E)

[redacted] (b)(7)(E)

[redacted] (b)(7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Field Operations
National Targeting Center

Device Research into Marijuana Seizure

(b) (7)(E)

Issue:

(b) (7)(E) According to the requestor, (b) (7)(E) packages of marijuana (b) (7)(E)

Synopsis:

(b) (7)(E)

(b) (7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Field Operations

National Targeting Center

(b) (7)(E)

[redacted]

U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Field Operations
National Targeting Center

(b) (7)(E)

[redacted]

U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Field Operations

National Targeting Center

(b) (7)(E)

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether
a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**AdID Efficacy Pilot**		
Component:	Customs and Border Protection (CBP)	**Office or Program:**	OFO/NTC
Xacta FISMA Name (if applicable):	**Automated Targeting System (ATS)**	**Xacta FISMA Number (if applicable):**	**CBP-00006-MAJ-00006**
Type of Project or Program:	**Pilot**	**Project or program status:**	**Pilot**
Date first developed:	**December 1, 2018**	**Pilot launch date:**	**May 1, 2019**
Date of last PTA update	**N/A**	**Pilot end date:**	**May 1, 2021**
ATO Status (if applicable)	**Not started**	**ATO expiration date (if applicable):**	**N/A**

PROJECT OR PROGRAM MANAGER

Name:	(b) (6), (b) (7)(C)		
Office:	**OFO**	**Title:**	Assistant Director NTC PAIG
Phone:	(b) (6), (b) (7)(C)	**Email:**	(b) (6), (b) (7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:			
Phone:		**Email:**	

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

(U) Background

(U//FOUO) U.S. Customs and Border Protection (CBP) is generally responsible for preventing the entry of terrorists, securing the borders of the United States, and enforcing customs, immigration, and other U.S. laws at the border. CBP's authorities require it to detect, respond to, and interdict persons who may undermine the security of the United States, in cases in which such persons are seeking to enter, or have entered, the United States. To aid in CBP's (b) (7)(E) processes, CBP is entering a testing and evaluation phase to assess the efficacy of using commercially available marketing location data associated with Advertising IDs (AdIDs).

(U) Traditional computers and laptops use internet cookies to track consumers' activities, which is then largely sold to marketers and advertisers. While still in use today, internet cookies grew less effective over time to marketers due to the emergence of mobile smart devices and mobile applications (apps). To continue to monetize consumers' activities, mobile app developers first began to link app activity to the mobile device's Unique Device ID (UDID) that is hardcoded to the device. However, due to privacy concerns, the Advertising ID (AdID) was created in 2013 to provide an alternative for app developers to use instead of the UDID that gave device users more control over their privacy. In 2013, Apple stopped accepting new apps to the Apple Store that accessed iOS device's UDID and required app developers to use Apple's version of an AdID called ID for Advertisers (IDFA). Android soon followed with their own version called Google Advertising ID with Google Play Services version 4.0 on devices running Android software.

(U) The AdID is a hashed identifier that is temporarily associated with a device for a period of time and not hardcoded to the device like the UDID. This allows app developers to still track and report a device's consumer activity, to include date/time and locational information, without connecting to or using any personally identifiable information (PII) associated with the device such as the UDID, or the device user, such as names, phone numbers, emails, usernames, etc. AdIDs can be reset by the device owner at any time. Device users can also opt-out of or limit the location information used by an app or delete the app altogether. Location data associated with AdIDs is available from devices and apps where users have consented to and have opted-in to share their locational information. Data is available from when a device is in use and never when a device is idle or turned off.

(U) CBP Pilot

(U//FOUO) CBP has identified and seeks to pilot and review several commercially available AdID platforms (b) (7)(E). Analysis during this testing and evaluation will be focused on AdIDs associated with cross border criminal activity and/or activity with an identified terrorist/criminal predicate. (b) (7)(E). The pilot will last for twelve months, with possible extensions as required. Information collected as part of the pilot will continue to be retained after the pilot until CBP can establish an appropriate retention schedule. As part of the pilot, CBP will provide proprietary, commercially available AdID platforms to (b) (7)(E) . CBP will track requests for AdID research, analysis, and response sent to requester. (b) (7)(E)

(b) (7)(E) .

(U) An Evaluation Committee, consisting of (b) (7)(E) and Privacy and Diversity (PDO) representatives, will establish user guidelines, account issuance protocols, tracking and monitoring of user activity, account maintenance and will consolidate the evaluation results across platforms.

(b) (7)(E)

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]:

[redacted]

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	□ Closed Circuit Television (CCTV) □ Social Media □ Web portal[1] (e.g., SharePoint) □ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☒ This program does not collect any personally identifiable information[2] □ Members of the public □ DHS employees/contractors (list components): □ Contractors working on behalf of DHS □ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?
(U//FOUO) AdIDs were created to protect the identity and privacy of a device owner. All information acquired from this AdID data is specific to a mobile smart device for the duration the device is linked to the AdID, and is not linked to nor does it provide any PII of the device owner, such as device owner's name, phone numbers, social security numbers, email addresses, social media and app usernames, device Unique Device ID (UDID), device International Mobile Equipment Identity (IMEI), or device International Mobile Subscriber Identity (IMSI).

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

(U//FOUO) This AdID data is acquired directly from a data provider's platform and indirectly through two other commercial platforms accessing the same data. The data vendor ingests and aggregates location adID data from data providers [redacted] (b) (4), (b) (7)(E) This AdID data is only available from devices and apps that have opted-in to share location data and only when a device is in use, never when a device is idle or turned off. AdIDs are resettable at any time by a device owner. Location data collected by a wireless carrier and/or device manufacture is never used. SDK-sourced location data is recorded by applications and is embedded within tens of thousands of apps. Not all location enabled apps include an SDK that shares location data. RTB-sourced location data is recorded when an advertisement is served.

(U//FOUO) The data provider takes (b) (7)(E) [redacted] to process all data collected to help flag and filter valid location data by signal origin and key characteristics. Data is also filtered to remove duplicate, inaccurate, and fraudulent data. No real-time tracking of data is available.

(U//FOUO) For further security, the AdID data provider further anonymizes the original AdID by generating a new, hashed AdID for use by vendor platforms. This new hashed ID is called the Provider ID. This allows platform users to see only the provider generated AdID and its associated geolocation data, and timestamps of activity. Vendor platforms (b) (7)(E) [redacted].

(U//FOUO) As noted in section 1, two vendor platforms provide an enhanced version where a user can see and search by the original AdID. In addition to search, the enhanced version provides metadata associated with the device. This metadata includes:

- the AdID number,
- device geolocation data (latitude/longitude & timestamp),
- [redacted] (b) (7)(E)
- Below is an example of what some of the information looks like:

[redacted] (b) (7)(E)

(b) (7)(E)

(U//FOUO) As noted in section 1, testing and evaluation will be focused on AdIDs associated with (b) (7)(E) [redacted]. Platform user queries and associated search results with (b) (7)(E) may be saved by CBP users in the vendor platform for further analysis, consistent with applicable policies. The vendor cannot access or view anything CBP saves on the platform without CBP permission. Subsequent analysis and any relevant findings will be captured in standard CBP reporting.

4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.

4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list:
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item.
7. Does the project, program, or system provide role-based training for personnel who have access in addition	☐ No. ☒ Yes. If yes, please list:

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

to annual privacy training required of all DHS personnel?	Training will incorporate an overview of responsible use, to include necessity for a border-related predicate pursuant to CBP's existent law enforcement authorities. Training will highlight that the platform and data must be used with existent CBP and individual component and division or job series authorities, and reasons for retaining data will be clearly documented consistent with applicable policy.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: No PII will be collected during the use of this too. ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

FOUO/LAW ENFORCEMENT SENSITIVE

PRIVACY THRESHOLD REVIEW

(To be Completed by COMPONENT PRIVACY OFFICE) Component Privacy Office Reviewer:	(b) (6), (b) (7)(C)
Date submitted to Component Privacy Office:	**June 6, 2019**
Date submitted to DHS Privacy Office:	August 16, 2019

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed.

(b) (5), (b) (7)(E)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	September 30, 2020
PTA Expiration Date	September 30, 2021

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.

FOUO/LAW ENFORCEMENT SENSITIVE

Category of System:	IT System If "other" is selected, please describe: Click here to enter text.

Determination:

☐ PTA sufficient at this time.

☐ Privacy compliance documentation determination in progress.

☐ New information sharing arrangement is required.

☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.

☐ Privacy Act Statement required.

☒ Privacy Impact Assessment (PIA) required.

☒ System of Records Notice (SORN) required.

☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

☐ A Records Schedule may be required. Contact your component Records Officer.

PIA:	**New PIA is required.** If covered by existing PIA, please list: Forthcoming AdID PIA
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

CBP is submitting this PTA to discuss the use of commercially-acquired marketing location data associated with Advertising ID (AdID) for law enforcement intelligence purposes. All information acquired during the testing and evaluation phase will be focused on AdIDs associated with (b) (7)(E) [redacted]

The AdID was created to provide an alternative for app developers to use as an identifier. It is a hashed identifier that is temporarily associated with a device for a period of time, but is not hardcoded to the device like the previously used identifier (Unique Device ID). Use of AdID allows app developers to track and report a device's consumer activity, including date/time and location information, without connecting to or using any PII associated with the device/device user. Location data associated with AdIDs is available only when users have consented to/opted-in to share location information; users can choose to opt out of or limit the location information collected by a certain app.

AdIDs are available via commercially available platforms. (b) (7)(E) [redacted]

Platform user queries and associated search results (b) (7)(E) may be saved by CBP users in the vendor platform for further analysis. Subsequent analysis and any relevant findings will be captured in standard CBP reporting (b) (7)(E)

The DHS Privacy Office 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, (b) (7)(E).

SORN coverage comes from DHS/CBP-024 CBP Intelligence Records System, which permits the collection of location information from public source data, metadata, as well as commercial data providers. This SORN permits the collection of information about individuals associated with law enforcement activities where CBP is responsible for upholding the law.