

18 ITEM NO	20 SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
0001	(b)(7)(E) Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0002	(b)(7)(E) Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0003	(b)(7)(E) SOFTWARE Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0004	(b)(7)(E) SOFTWARE Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0005	(b)(7)(E) SOFTWARE Continued ...	(b)(7)(E)	EA	\$ _____	\$ _____

32a QUANTITY IN COLUMN 21 HAS BEEN

RECEIVED INSPECTED ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32c. DATE 32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33 SHIP NUMBER 34. VOUCHER NUMBER 35 AMOUNT VERIFIED CORRECT FOR 36. PAYMENT 37. CHECK NUMBER
PARTIAL FINAL COMPLETE PARTIAL FINAL

38 S/R ACCOUNT NUMBER 39. S/R VOUCHER NUMBER 40. PAID BY

41a I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT 42a. RECEIVED BY (Print)
41b SIGNATURE AND TITLE OF CERTIFYING OFFICER 41c. DATE 42b RECEIVED AT (Location)
42c. DATE REC'D (YY/MM/DD) 42d. TOTAL CONTAINERS

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

HSCEMD-14-Q-00028

PAGE OF

3 18

NAME OF OFFEROR OR CONTRACTOR

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT				
0006	(b)(7)(E) SOFTWARE Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0007	(b)(7)(E) Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0008	(b)(7)(E) Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0009	LAPTOP PC Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND QUICK REACTION CAPABILITY EQUIPMENT	(b)(7)(E)	EA	\$ _____	\$ _____
0010	EQUIPMENT FAMILIARIZATION - MELBOURNE, FLORIDA Each (b)(7)(E) requires two days of work on each of the four protocols, four students per session. Therefore listed pricing should reflect 20 complete sessions X 4 students per session, for complete familiarization for a total quantity of 80 students. Travel and TDY expenditures are handled separately from this CLIN. Product/Service Code: (b)(7)(E) Product/Service Description: ELECTRONIC COUNTERMEASURES, COUNTER-COUNTERMEASURES AND Continued ...	(b)(7)(E)	EA	\$ _____	\$ _____

CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED
HSCEMD-14-Q-00028

PAGE OF
4 18

NAME OF OFFEROR OR CONTRACTOR

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
----------------	--------------------------	-----------------	-------------	-------------------	---------------

QUICK REACTION CAPABILITY EQUIPMENT

See attached Addenda pages for applicable clauses and provisions.

From: (b)(6); (b)(7)(C)
Sent: 20 Dec 2016 13:56:28 -0500
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: Harris Stingray cell phone tracker/House Oversight and Government Reform Committee report

<http://www.washingtontimes.com/news/2016/dec/19/house-oversight-doj-dhs-have-more-than-400-cell-si/>

(b)(6); (b)(7)(C)

Investigations & Operations Support Dallas | Section Chief
DHS | ICE | Office of Acquisition Management (OAQ)
Phone: 214-(b)(6);
Blackberry: 202-(b)(6);
Email: (b)(6); (b)(7)(C)@dhs.gov

Your First Partner in Acquisition!

Information contained in this email and any attachments may include "source selection information." Unauthorized disclosure of source selection information is prohibited by Subsection 27(a) of the Office of Federal Procurement Policy Act (the Procurement Integrity Act)(41 U.S.C. § 2102). Release of information both before and after award may also be prohibited by the Privacy Act (5 U.S.C. § 552(a), the Trade Secrets Act (18 U.S.C. § 1905), and other laws (together referred to as "Acts"). Criminal and civil penalties, and administrative remedies, may apply to conduct that violates these Acts. Contact the contracting officer prior to sharing the contents of this e-mail, or any attachments, with any non-recipient.

Cell-Site Simulator Policy

Exigent Circumstances

May nullify the Fourth Amendment warrant requirement when the needs of law enforcement are so compelling that it renders a warrantless search objectively reasonable.



Cell-Site Simulator Policy

Exigent Circumstances (cont.)

- In exigent circumstances, still must comply with the Pen Register Statute (18 U.S.C. 3121, et seq); and
- Must receive judicial authorization based on the government's certification that the information sought is ***relevant to an ongoing criminal investigation***. See 18 U.S.C. 3123(a).

UNLESS – the situation necessitates an emergency pen register.



Cell-Site Simulator Policy

Exigent Circumstances (cont.)

- § If justifying use of a cell-site simulator in an exigent circumstance, under the emergency pen register statute:
- w The case agent/operator must get the requisite internal approval to use a pen register;
 - w Case agent/operator must contact the AUSA;
 - w AUSA must apply for a court order within 48 hours; and
 - w Any use under an emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours has passed, whichever comes first.



Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 27, 2018

December 21, 2018-December 27, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

104

0

56

13

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 31, 2018

December 28, 2018-December 31, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

109

5

57

14

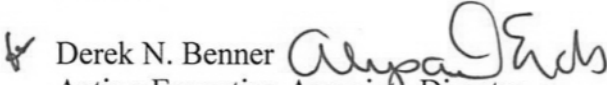
(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

AUG 31 2017

MEMORANDUM FOR: Assistant Directors
Deputy Assistant Directors
Special Agents in Charge
Attachés

FROM:  Derek N. Benner
Acting Executive Associate Director

SUBJECT: Use of Cell-Site Simulator Technology

Purpose:

Cell-site simulators are invaluable law enforcement tools that locate or identify mobile devices during active criminal investigations. They allow law enforcement to locate both subjects of an investigation and victims of ongoing criminal activity. U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents (SAs), Technical Enforcement Officers (TEOs), and Task Force Officers (TFOs) may use cell-site simulators in accordance with the Department of Homeland Security (DHS) Policy Directive 047-02, "Department Policy Regarding the Use of Cell-Site Simulator Technology," dated October 19, 2015.

As with any law enforcement capability, HSI must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment and applicable statutory authorities, including the Pen Register Statute (Title 18, United States Code (U.S.C.), Section 3121 *et seq.*). Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with applicable statutes, regulations, and policies that guide HSI data collection, retention, and disclosure.

By this memorandum, I am directing the immediate implementation of this HSI policy on the use of cell-site simulator technology. This policy provides guidance for the use of cell-site simulators by HSI SAs, TEOs, and TFOs. This policy applies solely to the use of cell-site simulator technology inside the United States, as well as inside its Commonwealths, Territories, and Possessions, in furtherance of criminal investigations.

Background:

HSI SAs, TEOs, and TFOs may use cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity.

Cell-site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the cell-site device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the cellular device in the same way that they would with a networked tower.

A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular device. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. Cell-site simulators provide only the relative signal strength and general direction of the subject cellular device; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Cell-site simulators used by HSI SAs, TEOs, and TFOs must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes contents of any communication stored on the device itself; cell-site simulators do not remotely capture emails, text messages, contact lists, or images. Moreover, cell-site simulators used by HSI SAs, TEOs, and TFOs do not provide subscriber account information (for example, an account holder's name, address, or telephone number). Nothing in this policy prohibits the use of other appropriate legal authorities to acquire that information.

Management Controls and Accountability

The following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. The HSI Assistant Director (AD), Information Management Directorate (IMD), will be responsible for the implementation of this policy and for ensuring compliance with its provisions within HSI. The AD, IMD, will also serve as the ICE executive level point of contact.
2. Prior to the court order application for the deployment of this technology, the use of a cell-site simulator must be approved by a first-level supervisor. Any exigent or

emergency use of a cell-site simulator must also be approved by an appropriate second-level supervisor prior to its use. If the circumstances permit, these approvals should be granted in writing (an email fulfills this requirement). When circumstances do not permit, approval should be documented in writing at the soonest practicable moment.

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

Legal Process and Court Orders

The use of cell-site simulators is permitted only as authorized by law and policy. While HSI SAs, TEOs, and TFOs have, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute, as a matter of policy, HSI SAs, TEOs, and TFOs must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent), except as provided below.

HSI SAs, TEOs, and TFOs will need to seek authority pursuant to Rule 41 *and* the Pen Register Statute, depending on the rules in their jurisdiction, prior to using a cell-site simulator. They must therefore consult with the Assistant United States Attorney (AUSA) or the appropriate state or local prosecutor, depending on the jurisdiction in which the cell-site simulator is being utilized, to either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit must also reflect the information noted below under “Applications for Use of Cell Site Simulators.” In addition to consulting with the appropriate prosecuting attorney, HSI SAs, TEOs, and TFOs shall coordinate with their local Office of the Principal Legal Advisor (OPLA) prior to beginning the legal process or, in the case of exigent circumstances, as soon as practicable thereafter.

There are two circumstances in which this policy does not require a warrant prior to the use of a cell-site simulator.

1. Exigent Circumstances under the Fourth Amendment

Exigent circumstances can vitiate a Fourth Amendment warrant requirement, but cell-site simulators still require court approval – consistent with the circumstances delineated in the Pen Register Statute’s emergency provisions – in order to be lawfully deployed. An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an officer has the requisite probable cause, a variety of types of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; the prevention of

the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition, in the subset of exigent situations where circumstances necessitate emergency pen register authority pursuant to 18 U.S.C. § 3125 (or the state equivalent), the emergency must be among those listed in Section 3125: immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year. Further, this policy requires that the case agent or operator first obtain the requisite supervisory approval to use a pen register before using a cell-site simulator.¹ In order to comply with the terms of this policy and with 18 U.S.C. § 3125, the case agent or operator must contact the duty AUSA in the local U.S. Attorney's Office, who will coordinate approval within the Department of Justice (DOJ).² Upon approval, the AUSA or the state or local prosecutor must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125.³ Under the provisions of the Pen Register Statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours have passed, whichever comes first.

2. Training and Function Testing

All HSI SAs, TEOs, and TFOs who operate cell-site simulator equipment must have attended formal training provided by the equipment vendor and any other training determined necessary by the AD, IMD. These operators are required to take an annual refresher course on the requirements of this policy, including training on privacy and civil liberties, which will be furnished by the HSI Technical Operations Unit.

During practical training scenarios, HSI personnel are permitted to target specified government- or vendor-provided equipment intended for use in training purposes. Non-approved devices and civilian devices will not be used as targets during training scenarios.

As part of the pre-deployment of cell site simulator equipment, HSI operators should verify that the equipment is in proper working condition and confirm that the equipment has been cleared of all previous operational data, if it pertains to an unrelated mission, prior to deploying the equipment.

¹(b)(7)(E)

²In non-federal cases, the case agent or operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

³The knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).

Applications for Use of Cell-Site Simulators

In all circumstances, candor to the court is of paramount importance. When making any application to a court, HSI SAs, TEOs, and TFOs must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. HSI SAs, TEOs, and TFOs must consult with the AUSA or appropriate prosecuting attorney in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.⁴

1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that SAs, TEOs, or TFOs plan to send signals to the cellular device that will cause both the cellular device and non-target devices on the same provider network in close physical proximity to emit unique identifiers, which will be obtained by the technology. The description should also indicate that SAs, TEOs, and TFOs will use the information to determine the physical location of the target device or to determine the currently unknown identifiers of the target device. If SAs, TEOs, or TFOs will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.
2. An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area of influence of the cell-site simulator might experience a temporary disruption of service from the service provider. Generally, in a majority of cases, any disruptions are exceptionally minor in nature and virtually undetectable to end users. The application may also note, if accurate, that any potential service disruption would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.⁵
3. An application for the use of a cell-site simulator should inform the court about how HSI intends to address deletion of data not associated with the target device. The application should also indicate that HSI will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

⁴ Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (e.g., tradecraft, capabilities, limitations, or specifications). Sample applications containing such technical information are available from the Computer Crime and Intellectual Property Section (CCIPS) of the DOJ's Criminal Division. To ensure that courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, SAs, TEOs, TFOs, or the prosecuting attorney must contact CCIPS, as well as consult with the local OPLA office for compliance with DHS policies.

⁵ Despite any disruption in service, cell phones being disrupted will still be able to conduct emergency calls, i.e., 911.

Data Collection, Recordkeeping, and Disposal

HSI is committed to ensuring that law enforcement practices concerning the collection or retention⁶ of data are lawful and respect the important privacy interests of individuals. As part of this commitment, HSI will operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence,⁷ HSI's use of cell-site simulators shall include the following practices:

1. Immediately following the completion of a mission, an operator of a cell-site simulator must delete all data.⁸
2. When the equipment is used to locate a target, data must be deleted as soon as the target is located.
3. When the equipment is used to identify a target, data must be deleted as soon as the target is identified, and no less than once every 30 days.
4. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.
5. If the deployment of the device results in the positive identification or location of a target person (or target telephone number), the said pertinent results will be documented in an ROI. The ROI will be stored in the relevant investigative case file and retained in accordance with the applicable Federal records schedule.

State and Local Partners

HSI often works closely with its state and local law enforcement partners and provides technological assistance under a variety of circumstances. In all cases, law enforcement authorities in the United States must conduct their missions lawfully and in a manner that respects the rights of the citizens they serve. This policy applies to all instances in which HSI uses cell-site simulators in support of other Federal agencies and/or state and local law enforcement agencies.

⁶ In the context of this policy, the terms "collection" and "retention" are used to address only the unique technical process of identifying, dialing, routing, addressing, or signaling information, as described by 18 U.S.C. § 3127(3), emitted by cellular devices. "Collection" means the process by which unique identifier signals are obtained; "retention" refers to the period during which the dialing, routing, addressing, or signaling information is utilized to locate or identify a target device, continuing until the point at which such information is deleted.

⁷ It is not likely, given the limited type of data cell-site simulators collect (as discussed above), that exculpatory evidence would be obtained by a cell-site simulator in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent that investigators know or have reason to believe that information is exculpatory or impeaching, they have a duty to memorialize that information.

⁸ A typical mission may last anywhere from less than one day up to several days.

Coordination and Ongoing Management

Each Special Agent in Charge office shall send monthly records to the Technical Operations Unit reflecting the total number of times a cell-site simulator is deployed, and by whom, in its area of responsibility; the number of deployments at the request of other agencies, including state or local law enforcement agencies; and the number of times the technology is deployed in exigent circumstances.⁹ In these monthly records, confirmation that the equipment had been cleared of any previous operational data must also be included. The Technical Operations Unit will be responsible for monitoring and maintaining the monthly records.

Improper Use of Cell-Site Simulators

Accountability is an essential element in maintaining the integrity of HSI. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the Joint Intake Center and/or the ICE Office of Professional Responsibility.

No Private Right

This policy guidance is not intended to and does not create any right, benefit, trust or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding.

⁹ Records reflecting the number of times the cell-site simulators were used may also be required for ongoing oversight by the DHS oversight offices.



HSI

POLICY GUIDANCE REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY



Basic Uses

- A cell-site simulator is a mobile device that law-enforcement can use to locate a cell phone whose identifiers are already known to law enforcement, or to determine the identifiers of an unknown phone by collecting (“canvassing”) identifying signals from cell phones in the cell-phone user’s vicinity.



How They Function

Cell-site simulators function by transmitting as a cellular tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and transmit signals to the simulator, which identify the device similar to the way that they would a networked tower.





How They Function

A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator.



How They Function

Once the Cell Site Simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular device. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.





HSI Cell-Site Simulators Obtain....

- Limited identifying information Only the relative signal strength and general direction of a subject telephone



HSI Cell-Site Simulators DO NOT....

- Function as a GPS locator, as they do not obtain or download any location information from the device or its applications
- Remotely capture emails, texts, contact lists, images or any other data from the phone
- Provide subscriber account information, such as an account holder's name or address



PEN Register Configuration

Cell-site simulators used by HSI must be configured as pen registers and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). The term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purpose the ordinary course of its business



Management and Accountability

- Cell-site simulators may only be operated by trained personnel who have been authorized by HSI to use the technology and whose training has been administered by a qualified agency component, expert or approved vendor. Prior to the deployment of the technology, use of a cell-site simulator by HSI personnel must be approved by a first-line supervisor. Emergency (or exigent) use of a cell-site simulator must be approved by a second-line supervisor. Any use of a cell-site simulator on an aircraft must be approved either by the Special Agent in Charge for the jurisdiction or by the Assistant Director, Information Management Directorate.



Legal Process

The use of cell-site simulators is permitted only as authorized by law and policy. Law enforcement agencies must obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure; Search and Seizure (or the applicable state equivalent), except as follows...



Legal Process

Pursuant to HSI policy, the only circumstance in which HSI law enforcement personnel do not require a warrant prior to the use of a cell-site simulator is Exigent (emergency) Circumstances under the Fourth Amendment.

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.



Legal Process

As a practical matter, because prosecutors will need to seek authority pursuant to Rule 41 and the Pen register Statute, prosecutors should, depending upon the rule of their jurisdiction, either...Obtain a warrant that contains all information required to be included in a pen register order, pursuant to 18 U.S.C. § 3123 (or the state equivalent), or Seek a warrant and pen register order concurrently.



Exigent Circumstances under the Fourth Amendment

An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an agent has the requisite probable cause, a variety of circumstances may justify dispensing with a warrant. These include...the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.



Exigent Circumstances under the Fourth Amendment

When circumstances necessitate emergency pen register authority, the operator must obtain the requisite internal approval to use a pen register, before using a cell-site simulator, and contact the duty Assistant United States Attorney (AUSA) in the local U.S. Attorney's Office. Once the AUSA receives verbal authorization from the DOJ Office of Enforcement Operations, Electronic Surveillance Unit, they must apply for a court order within 48 hours as required by 18 U.S.C. § 3125. Under the provisions of the Pen Register Statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours has passed, whichever comes first.



Applications for Use of Cell-Site Simulators

When making any application to a court, law enforcement personnel must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. HSI agents must consult with the government prosecutor in advance of using a cell-site simulator and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.



Applications for Use of Cell-Site Simulators

Regardless of the legal authority relied upon, at the time of making an application for the use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that law enforcement officers...Plan to send signals to the cellular phone that will cause it, and non-targeted devices on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology and Will use the information to determine the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If law enforcement personnel will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this as well.



Applications for Use of Cell-Site Simulators

An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area of influence of the cell-site simulator might experience a temporary disruption of service from the service provider. Generally, in a majority of cases, any disruptions are exceptionally minor in nature and virtually undetectable to end users. The application may also note, if accurate, that any potential service disruption would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.



Applications for Use of Cell-Site Simulators

An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target device. The application should also indicate that law enforcement will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.



Data Collection & Disposal

HSI is committed to ensuring that law enforcement practices concerning the collection or retention of data are lawful and respect the important privacy interests of individuals. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence, HSI's use of cell-site simulators shall include the following practices...Immediately following the completion of a mission, an operator of a cell-site simulator must delete all data. When the equipment is used to locate a target, data must be deleted as soon as the target is located. When the equipment is used to identify a target, data must be deleted as soon as the target is identified, and no less than once every 30 days. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data. If the deployment of the device results in the positive identification or location of a target person (or target telephone number), the said pertinent results will be documented in an ROI. The ROI will be stored in the relevant investigative case file and retained in accordance with the applicable Federal records schedule.



Auditing

HSI Technical Operations will be responsible for auditing the use of cell-site simulators, to ensure that the data is deleted in the manners previously described. This auditing program will include an equipment sign-in process that will comprise of the operator User Name and an affirmative acknowledgement by the operator that they have the proper legal authority to collect and view data non-target date and monthly reporting on the use of these devices.



Auditing

- Each field office is required to report to the Technical Operations Unit, on a monthly basis, statistics reflecting the total number of times a cell-site simulator is deployed in the jurisdiction, the number of deployments at the request of other agencies (including state or local law enforcement), and the number of times the technology is deployed pursuant to emergency circumstances. In addition to monthly statistics, operators must complete a utilization log that can be accessed and updated online via a SharePoint site. Access to the site will automatically be granted to those authorized to operate a cell-site simulator; however they will only be able to access information pertaining to their own Area of Responsibility (AOR). Log entries and submissions must be completed at the soonest practicable moment once the mission is concluded.



State and Local Partners

HSI often works closely with its state and local law enforcement partners and provides technological assistance under a variety of circumstances. In all cases, law enforcement authorities in the United States must conduct their missions lawfully and in a manner that respects the rights of the citizens they serve. HSI's policy regarding the use of cell-site simulators applies to all instances in which a cell-site simulator is used to support other federal agencies and/or state and local law enforcement agencies.



Training and Coordination

- All HSI personnel who operate cell-site simulators must have successfully completed a formal training session provided by the equipment vendor and any other training determined mandatory by the Assistant Director, Information Management Directorate. During practical training scenarios, HSI personnel are only permitted to target specified government or vendor equipment. As part of the pre-deployment checks for cell-site simulator equipment, operators should verify that the equipment is functioning properly. During testing, HSI personnel are only permitted to target specified government or vendor equipment.



Improper Use of Cell-Site Simulators

Accountability is an essential element in maintaining the integrity of HSI. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the Joint Intake Center and/or the ICE Office of Professional Responsibility.



Questions

For questions pertaining to the HSI Cell-Site Simulator Program, Please contact the Technical Operations Unit (TechOps)

(b)(7)(E)



Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 3, 2019

January 1, 2019 -January 3, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

0

0

0

0

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
January 10, 2019

January 4, 2019 -January 10, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

0

0

0

0

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 15, 2019

January 11, 2019 -January 15, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

1

1

1

0

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 24, 2019

January 16, 2019 -January 24, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

5

4

4

2

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 31, 2019

January 24, 2019 -January 31, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

9

4

6

3

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 7, 2019

February 1, 2019, -February 7, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

14

5

10

5

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 14, 2019

February 8, 2019, -February 14, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

18

4

13

6

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 21, 2019

February 15, 2019, -February 21, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total	22	4	14	6
--------------------	-----------	----------	-----------	----------

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 28, 2019

February 22, 2019, -February 28, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

25

3

16

6

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

March 7, 2019

March 1, -March 7, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

26

1

17

6

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
March 14, 2019

March 8, -March 14, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total	32	6	22	8
--------------------	-----------	----------	-----------	----------

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
March 21, 2019

March 15, -March 21, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

34

2

24

9

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

March 28, 2019

March 22, -March 28, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

37

3

26

10

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April
4, 2019

March 29, -April 4, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

49

12

35

10

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April

11, 2019

April 5, -April 11, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

54

5

40

13

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April
17, 2019

April 12, -April 17, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

62

7

44

15

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April
25, 2019

April 18, -April 25, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

64

2

45

15

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
2, 2019

April 26, -May 2, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total	64	0	45	15
--------------------	-----------	----------	-----------	-----------

SAC Atlanta, Kansas City, Nashville, Las Vegas and Hawaii do not have CSS equipment

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
9, 2019

May 3, -May 9, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

66

2

46

15

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
15, 2019

May 10, -May 15, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

71

5

49

16

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
23, 2019

May 16, -May 23, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total	71	0	49	16
--------------------	-----------	----------	-----------	-----------

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
30, 2019

May 24, -May 30, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

75

4

53

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June
6, 2019

May 31, -June 6, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

78

3

54

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June
12, 2019

June 7, -June 12, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

79

1

55

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June
20, 2019

June 13, -June 20, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

86

7

58

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June

26, 2019

June 21, -June 26, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

88

2

58

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 - July
5, 2019

June 27, -July 5, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

96

8

61

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -July
11, 2019

July 6, -July 11, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total	97	1	62	17
--------------------	-----------	----------	-----------	-----------

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -July
18, 2019

July 12, -July 18, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

101

4

63

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -July
25, 2019

July 19, -July 25, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

105

4

65

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

August 1, 2019

July 26, -August 1, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

105

0

65

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
August 7, 2019

August 2, -August 7, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total	107	2	67	17
--------------------	-----	---	----	----

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
August 15, 2019

August 8, -August 15, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

109

2

67

17

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
August 22, 2019

August 16, -August 22, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

118

9

70

19

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
August 28, 2019

August 23, -August 28, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

118

0

70

19

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
September 5, 2019

August 29, -September 5, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

118

0

70

19

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
September 12, 2019

September 6, -September 12, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

120

2

72

19

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
September 20, 2019

September 13, -September 20, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

123

3

74

20

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
September 26, 2019

September 21, -September 26, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

129

9

78

22

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
October 3, 2019

September 27, -October 3, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

134

5

80

22

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

October 4, 2019

October 4, -October 7, 2019

Target Located

Arrests

(b)(7)(E)

Grand Total

134

0

80

22

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 1, 2018

October 26, 2018-November 1, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

86

1

45

10

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 15, 2018

November 9, 2018-November 15, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

91

5

48

12

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 15, 2018

November 9, 2018-November 15, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

95

4

51

13

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 21, 2018

November 16, 2018-November 21, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

95

0

51

13

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 29, 2018

November 22, 2018-November 29, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

95

0

51

13

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 6, 2018

November 30, 2018-December 6, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

98

3

53

13

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 13, 2018

December 7, 2018-December 13, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

101

3

54

13

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 20, 2018

December 14, 2018-December 20, 2018

Target Located

Arrests

(b)(7)(E)

Grand Total

104

3

56

13

(b)(7)(E)



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

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.

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	Cell Site Simulator Technology and Log		
Component:	Immigration and Customs Enforcement (ICE)	Office or Program:	Homeland Security Investigations (HSI) - Technical Operations Unit (TechOps) Title III
Xacta FISMA Name (if applicable):	NA	Xacta FISMA Number (if applicable):	NA
Type of Project or Program:	IT System	Project or program status:	Existing
Date first developed:	January 4, 2005	Pilot launch date:	Click here to enter a date.
Date of last PTA update:	April 3, 2015	Pilot end date:	Click here to enter a date.
ATO Status (if applicable)	Choose an item.	ATO expiration date (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b)(6); (b)(7)(C)		
Office:	T-III	Title:	Section Chief- Communications Intercept
Phone:	703 (b)(6); (b)(7)(C)	Email:	(b)(6); (b)(7)(C) @ice.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6); (b)(7)(C)		
Phone:	703 (b)(6); (b)(7)(C)	Email:	(b)(6); (b)(7)(C) @ice.dhs.gov

—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) is renewing the Over the Air Technology PTA (last adjudicated April 3, 2015) and replacing it with this PTA for Cell Site Simulators (CSS).

HSI uses CSS to track mobile phones within the course of carrying out criminal investigations. (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~— LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE —~~

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

~~— LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE —~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

(b)(5); (b)(7)(E)

-

(b)(5); (b)(7)(E)

<p>2. Does this system employ any of the following technologies: <i>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.</i></p>	<p>(b)(5); (b)(7)(E)</p>
--	--------------------------

(b)(5); (b)(7)(E)

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



— LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE —

<p>3. From whom does the Project or Program collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p>	<p>(b)(5); (b)(7)(E)</p>
--	--------------------------

<p>4. What specific information about individuals is collected, generated or retained?</p>
<p>(b)(5); (b)(7)(E)</p>

⁵ 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.

— LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE —



—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—

(b)(5); (b)(7)(E)	
4(a) Does the project, program, or system retrieve information by personal identifier?	(b)(5); (b)(7)(E)
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?	
<i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	
4(f) If header or payload data⁶ is stored in the communication traffic log, please detail the data elements stored.	
N/A	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems?⁷	(b)(5); (b)(7)(E)
--	-------------------

(b)(5); (b)(7)(E)

—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—



—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—

<p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p>	<p>(b)(5); (b)(7)(E)</p>
<p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p>	
<p>7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?</p>	
<p>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 who have requested access to their PII?</p>	
<p>9. Is there a FIPS 199 determination?⁸</p>	

⁸ 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.

—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

	(b)(5); (b)(7)(E)
--	-------------------

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:	May 29, 2019
Date submitted to DHS Privacy Office:	Click here to enter a date.
Component Privacy Office Recommendation:	
<i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
ICE is submitting this PTA to renew and update the information provided in the 2015 Over the Air Tracking Technology PTA. The ICE Privacy Division recognizes that (b)(5); (b)(7)(E)	
(b)(5); (b)(7)(E) and	
recommends (b)(5); (b)(7)(E)	As such, a PIA is required. ICE
recommends (b)(5); (b)(7)(E)	SORN coverage
is provided under DHS/ICE-009 - External Investigations (Jan. 5, 2010, 75 FR 404).	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6); (b)(7)(C)
-------------------------------------	-------------------

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—

PCTS Workflow Number:	1181415
Date approved by DHS Privacy Office:	July 18, 2019
PTA Expiration Date	July 18, 2020

DESIGNATION

Privacy Sensitive System:	Yes If “no” PTA adjudication is complete.
Category of System:	IT System If “other” is selected, please describe: Click here to enter text.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.
PIA:	New PIA is required. If covered by existing PIA, please list: Forthcoming ICE Surveillance Technologies PIA
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ICE-009 External Investigations January 5, 2010 75 FR 404
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
ICE is submitting this PTA to discuss the use of Cell Site Simulators (CSS), which are used to track mobile phones within the course of carrying out criminal investigations. Before this technology is used, HSI obtains court orders or search warrants (depending on the judicial district) through the appropriate United States Attorneys’ Offices which authorize the use of this technology. CSS does not have the capability to intercept the content of communications to or from mobile phones.	

—LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE—



~~— LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE —~~

(b)(5); (b)(7)(E)

The DHS Privacy Office finds (b)(5); (b)(7)(E) requiring PIA coverage. Coverage will be provided by the forthcoming ICE Surveillance Technologies PIA. This PIA should discuss (b)(5);

(b)(5); (b)(7)(E)

SORN coverage is also required, and is provided by the DHS/ICE-009 External Investigations SORN.

~~— LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE —~~