

U.S. Department of Homeland Security  
500 12<sup>th</sup> St., SW  
Washington, D.C. 20536



U.S. Immigration  
and Customs  
Enforcement

March 4, 2020

Nathan Freed Wessler  
American Civil Liberties Union Foundation  
125 Broad Street, 18<sup>th</sup> Floor  
New York, NY 10004

**RE: ACLU v DHS (1:19-cv-11311-JSR)  
ICE FOIA Case Number 2020-ICLI-00013  
Final Response**

Dear Mr. Wessler:

This is the final response to your Freedom of Information Act (FOIA) request to U.S. Immigration and Customs Enforcement (ICE). You requested the following:

- 1) Any policy directives, guidance documents, memoranda, training materials, or similar records created on or after October 19, 2015, governing or concerning use of cell site simulators by Immigrations and Customs Enforcement and Customs and Border Protection agents, employees, or partners, including any policy or guidance document that cites Department of Homeland Security Policy Directive 047-02 ("Department Policy Regarding Use of Cell-Site Simulator Technology"), 7 as well as any communications with Congress concerning implementation of or updates to DHS Policy Directive 047-02 and other policies governing cell site simulator use;
- 2) Any records reflecting whether ICE or CBP does use or is permitted to use cell site simulators in furtherance of civil immigration enforcement operations, as opposed to in furtherance of criminal investigations, and any guidance concerning whether and how DHS Policy Directive 047-02 applies to uses of cell site simulators in furtherance of immigration-related investigations that are not criminal. in nature;
- 3) From October 19, 2015 to the present, annual records reflecting the total number of times a cell-site simulator is deployed in the jurisdiction of each field office, the numbers of deployments at the request of other agencies, and the number of times the technology is deployed in emergency circumstances (collection of this information is required by DHS Policy Directive 047-02);
- 4) Since the date of the last annual record described in item 3, above, records reflecting the number of ICE and CBP investigations or operations in which cell site simulators have been deployed, including information about the field office deploying the cell site simulator and whether those deployments were in support of criminal investigations of

- non-immigration-related offenses, criminal investigations of immigration-related offenses, or civil immigration enforcement operations;
- 5) Records reflecting the number of times ICE and CBP have requested the assistance of other law enforcement agencies (including federal, state, local, and foreign) in deploying cell site simulators;
  - 6) Records regarding implementation of an auditing program to ensure deletion of data collected by cell site simulators, as required by DHS Policy Directive 047-02;
  - 7) All applications submitted to state and federal courts since January 1, 2013, for orders or search warrants authorizing the use of cell site simulators in ICE and CBP investigations or operations (including investigations or operations as part of task forces or partnership with other agencies), as well as any warrants or orders, denials of warrants or orders, and returns of warrants associated with those applications. If any responsive records are sealed, please provide the date, court, and docket number for each sealed document;
  - 8) All requests to persons or offices within the Department of Homeland Security for supervisory or legal authorization to deploy cell site simulators;
  - 9) Records dated or created on or after January 1, 2013 concerning the purchase of cell site simulator equipment and related software and hardware, including purchase orders, invoices, documentation of selection, sole source or limited source justification and approval documentation, communications, and other memoranda and documentation. This should include any purchase of cell site simulator equipment from the Harris Corporation (including, but not limited to, Stingray, Stingray II, Hailstorm, Triggerfish, Kingfish, Amberjack, and Harpoon devices), DRT (also known as Digital Receiver Technology), and other companies. At a minimum, please search the ICE Office of Acquisition Management for these records; and
  - 10) Records concerning the use of evidence derived or resulting from use of a cell site simulator in immigration court proceedings, and the provision of notice to respondents in immigration court proceedings informing them that a cell site simulator was used.

ICE has considered your request under the FOIA, 5 U.S.C. § 552.

A search of the Office of Homeland Security Investigations (HSI), Office of Information Governance and Privacy (IGP), and the Office of the Principal Legal Advisor (OPLA) located records that were potentially responsive to your request. For this production ICE reviewed 2,643 pages of potentially responsive records. Of those 2,643 pages, ICE determined that 1,186 pages were deemed responsive. Of those 1,186 pages, 92 pages require further coordination with other agencies/components. Therefore, this production consists of 1,094 pages. These pages have been Bates numbered 2020-ICLI-00013 1 through 2020-ICLI-00013 1094. ICE has applied FOIA Exemptions (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E) to portions of these pages as described below.

ICE has applied FOIA Exemption (b)(5) to withhold draft documents under the deliberative process privilege, the general purpose of which is to prevent injury to the quality of agency decisions, as well as the attorney-client privilege and the attorney work product privilege.

**FOIA Exemption 5** protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. After carefully reviewing the responsive documents, I have determined that portions of the responsive documents qualify for protection under the deliberative process privilege. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.

ICE has applied FOIA Exemptions 6 and 7(C) to protect from disclosure the names, e-mail addresses, and phone numbers of DHS employees contained within the documents.

**FOIA Exemption 6** exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

**FOIA Exemption 7(C)** protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, I have determined that the privacy interest in the identities of individuals in the records you have requested clearly outweigh any minimal public interest in disclosure of the information. Please note that any private interest you may have in that information does not factor into this determination.

ICE has applied FOIA Exemption 7(E) to protect from disclosure internal agency investigations and operations within the document.

**FOIA Exemption 7(E)** protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. I have determined that disclosure of certain law enforcement sensitive information contained within the responsive records could reasonably be expected to risk circumvention of the law. Additionally, the techniques and procedures at issue are not well known to the public.

Sincerely,

*Dexter E. Johnson/for*

Fernando Pineiro Jr  
(A) FOIA Officer

Enclosure(s): 1,094 page(s)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jun 2013 20:05:39 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: HSCEMD-13-J-00015 Spectrum Support Services  
**Attachments:** Contract Document Legal Review Corrections.pdf

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

Thanks, looks good.

V/r

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905.(b)(6);  
(bb) 214.924.(b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, June 13, 2013 2:56 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: HSCEMD-13-J-00015 Spectrum Support Services

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

Attached are the corrected pages (29 and 30) of the award document and comments in response to your legal review.

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

**OAQ Mission Support Dallas | Contract Specialist**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Desk:** 214-905.(b)(6); (b)(7)(C) Fax: 214-905-5568  
**Email:** (b)(6); (b)(7)(C)

**Your First Partner in Acquisition!**

Help us Support You Better: [How's My Service?](#)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, June 13, 2013 10:50 AM

**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** HSCEMD-13-J-00015 Spectrum Support Services

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

Please find attached my comments concerning the award document.

V/r

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor

(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

### REQUEST FOR LEGAL REVIEW

<b>REQUEST DATE</b> June 11, 2013	<b>CONTRACT SPECIALIST</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214-905-(b)(6); (b)(7)(C)
<b>DIVISION/OFFICE</b> OAQ / MSD	<b>CONTRACTING OFFICER</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214-905-(b)(6); (b)(7)(C)
<b>ACQUISITION DOCUMENT NO.</b> HSCEMD-13-J-00015 - <i>Order Review</i>	<b>CONTRACTOR</b> Zantech IT Services, Inc.	
<b>CONTRACTING OFFICER'S COMMENTS</b> Request Pre-Award legal review  1) Added 52.217-8  2) Key personnel names added to HSAR 3052.215-70  3) added 52.212-4 AHI. Also, this clause is included in the contractor's TABBs Contract.	<b>ATTORNEY'S COMMENTS</b> <input type="checkbox"/> Legally Sufficient <input checked="" type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below)  ATTORNEY: (b)(6); (b)(7)(C) DATE: <u>6/13/2013</u>  1) Add: 52.217-8 OPRN to extended services.  2) Reference HSAR 3052.215-70 key personnel, pursuant to (b) identify the "Special individuals" by Name, not just position.  3) Indicate that 52.212-4 AHI applies to this Task Order.	

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

## **16.0 OTHER DELIVERY ORDER TERMS**

### **16.1. INCORPORATED CLAUSES:**

FAR and HSAR provisions and clauses can be accessed at <http://farsite.hill.af.mil/>

#### **52.212-4 Contract Terms and Conditions—Commercial Items (JUNE 2010) with Alternate I (OCT 2008)**

#### **52.213-3 -- Notice to Supplier (Apr 1984)**

#### **52.217-8 -- Option to Extend Services (Nov 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to task order expiration.

**FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000):** (a) The Government may extend the term of this contract by written notice to the Contractor prior to expiration; provided, that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days prior to the contract expiration date. The preliminary notice does not commit the Government to an extension. (b) If the Government exercises this option, the extended contract shall be considered to include this option clause. (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 36 months.  
(End of Clause)

#### **HSAR 3052.205-70 Advertisements, Publicizing Awards, and Releases (SEP 2012).**

The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.  
(End of clause)

### **ALTERNATE I (SEP 2012)**

If a contract involves sensitive or classified information, designate the paragraph in the base clause as (a) and add the following paragraph (b) to the clause:

(b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the



Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.  
(End of clause)

**HSAR 3052.215-70 Key Personnel (DEC 2003)**

(a) The personnel specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel, as appropriate.

(b) Before removing or replacing any of the specified individuals, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel until the Contracting Officer approves the change.

Key Personnel under this task order:

The Project Manager (b)(6); (b)(7)(C)

The Senior Computer Systems Specialist / Network Engineer: (b)(6); (b)(7)(C)

The Senior Engineer Subject Matter Expert (SME) (b)(6); (b)(7)(C)

(End of clause)

**3052.242-72 Contracting officer's technical representative. (DEC 2003)**

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

(b) The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

(End of clause)

**PER ALL TABBS CONTRACTS:**

**H-8 Advertisements, Publicizing Awards, and News Releases**

All press releases or announcements about any contract/task order award hereunder shall be approved by the contract/task order contracting officer prior to release. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the contract/task order contracting officer. The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 18 Sep 2012 14:31:24 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: MFR for not publicizing requirement and J&A  
**Attachments:** MFR - No Posting to Fedbizopps for Crossbow.doc  
**Importance:** High

FYI – Thanks.

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.924 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, September 18, 2012 9:31 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** FW: MFR for not publicizing requirement  
**Importance:** High

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

I have no legal objections.

V/r

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

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.924 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, September 17, 2012 5:25 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** MFR for not publicizing requirement  
**Importance:** High

Team:

By and large, the attached was taken from the last Stingray purchase as well. Please advise if there any objections to or changes that need to be made to the text.

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

**Mission Support - Dallas (MSD), OI East Team – Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6); (b)(7)(C)  
**Email:** (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

Help us Support You Better: [How's My Service?](#)

**MEMO FOR RECORD**

**DATE: September 17, 2012**

**RE: Requisition 192112VSA00000079**

**SUBJECT: Restrictions on Publicizing Requirements for the Purchase of  
Crossbow OTA Tracking Equipment**

**I. BACKGROUND**

(b)(7)(E)

**II. REQUIREMENTS**

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

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

Contract Specialist

Date

**From:** (b)(6); (b)(7)(C)  
**Sent:** 18 Sep 2012 14:30:50 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: MFR for not publicizing requirement  
**Attachments:** MFR - No Posting to Fedbizopps for Crossbow.doc  
**Importance:** High

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

I have no legal objections.

V/r

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6); (b)(7)(C)  
(bb) 214.92 (b)(6); (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§~~

~~552(b)(5), (b)(7)~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, September 17, 2012 5:25 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** MFR for not publicizing requirement  
**Importance:** High

Team:

By and large, the attached was taken from the last Stingray purchase as well. Please advise if there any objections to or changes that need to be made to the text.

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

**Mission Support - Dallas (MSD), OI East Team – Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905- (b)(6); (b)(7)(C)  
Email: s (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

Help us Support You Better: [How's My Service?](#)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 16 May 2018 16:23:38 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** 192118VHQ6TSPC008 OTA Sole Source  
**Attachments:** 192118VHQ6TSPC008 OTA Sole Source.doc

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

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

**1. Agency and Contracting Activity**

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

**2. Nature and/or Description of the Action Being Approved**

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

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Source Selection Sensitive in accordance with FAR 3.104-4



Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

**6. Efforts to Obtain Competition**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

**8. Description of Market Research**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)  
Technical Operations (Tech Ops)  
Phone number: 703 (b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

\_\_\_\_\_  
Date

Contracting Officer

# Document Routing Form



U.S. Immigration  
and Customs  
Enforcement

<b>1</b>	Date: 8/11/14	Purpose: <input type="checkbox"/> Congressional <input type="checkbox"/> DHS <input type="checkbox"/> Routine <input type="checkbox"/> FYI	SharePoint Tracking No:
From:	(b)(6); (b)(7)(C)	Office: IOSD	Telephone No: (b)(6); (b)(7)(C) Room No:
Subject Title:	Review Solicitation HSCEMD-14-Q-00028 for (b)(5); (b)(7)(E)		
Comments:			

2 Required Concurrences Before Routing to the Office of the Director						
Name	Extension	Office	Action Requested	Initial	Date	Comments
(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C)	IOSD	<input type="checkbox"/> Concur <input checked="" type="checkbox"/> Sign	(b)(6); (b)(7)(C)	8/11/14	
		IOSD	<input type="checkbox"/> Concur <input type="checkbox"/> Sign		8/11/14	
		IOSD	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign		8/12/14	Followup on SB Review Form
OPLA		OPLA	<input type="checkbox"/> Concur <input type="checkbox"/> Sign		8/14/14	
			<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
			<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
			<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
			<input type="checkbox"/> Concur <input type="checkbox"/> Sign			

3 Office of the Director Concurrences						
Name	Action Requested	Initial	Date	Comments		
<b>ICE Management and Administration</b>						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign					

## REQUEST FOR LEGAL REVIEW

REQUEST DATE August 11, 2014	CONTRACT SPECIALIST (b)(6); (b)(7)(C)	TELEPHONE NO. 214-90 (b)(6); (b)(7)(C)
DIVISION/OFFICE IOSD	CONTRACTING OFFICER (b)(6); (b)(7)(C)	TELEPHONE NO. 214-905 (b)(6); (b)(7)(C)
ACQUISITION DOCUMENT NO. Review of Solicitation HSCEMD-14-Q-00028 for Harris Crossbow Equipment	CONTRACTOR Harris Corporation	
CONTRACTING OFFICER'S COMMENTS Request legal review of subject RFQ	ATTORNEY'S COMMENTS <input checked="" type="checkbox"/> Legally Sufficient <input type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below) (b)(6); (b)(7)(C) ATTORNEY: _____ DATE: <u>8/14/2014</u>	

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS</b> <i>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, &amp; 30</i>		1 REQUISITION NUMBER 192114VHQ54T00079		PAGE OF 1 18	
2 CONTRACT NO		3 AWARD/EFFECTIVE DATE		4 ORDER NUMBER	
5 SOLICITATION NUMBER HSCEMD-14-Q-00028		6 SOLICITATION ISSUE DATE		7 FOR SOLICITATION INFORMATION CALL: (b)(6); (b)(7)(C)	
8 OFFER DUE DATE/LOCAL TIME 1700 CT		9 ISSUED BY ICE/Mission Support-Dallas Immigration and Customs Enforcement Office of Acquisition Management 7701 N. Stemmons Freeway, Suite (b)(6); (b)(7)(C) Dallas TX 75247		10 THIS ACQUISITION IS X UNRESTRICTED OR SET ASIDE % FOR: SMALL BUSINESS WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAICS: 334511 HUBZONE SMALL BUSINESS EDWOSB SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS 8(A) SIZE STANDARD: 750	
11 DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED SEE SCHEDULE		12 DISCOUNT TERMS		13a THIS CONTRACT IS A RATED ORDER UNDER GPAS (15 CFR 700)	
13b RATING		14 METHOD OF SOLICITATION X RFP IFB RFP		15 DELIVER TO CODE TECHOPS Immigration and Customs Enforcement HSI/Technical Operations 10450 Furnace Rd Stop (b)(6); (b)(7)(C) Attr: (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) Lorton VA 20598 (b)(6); (b)(7)(C)	
16 ADMINISTERED BY ICE/Mission Support-Dallas Immigration and Customs Enforcement Office of Acquisition Management 7701 N. Stemmons Freeway, Suite (b)(6); (b)(7)(C) Attr: (b)(6); (b)(7)(C) (214) 905 (b)(6); (b)(7)(C) Dallas TX 75247		17a CONTRACTOR/OFFEROR CODE FACILITY CODE		18a PAYMENT WILL BE MADE BY CODE	
17b CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER		18b SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED SEE ADDENDUM		19 ITEM NO	
20 SERVICES (b)(6); (b)(7)(C) Technical (b)(6); (b)(7)(C) E:mail: (b)(6); (b)(7)(C) COR: (b)(6); (b)(7)(C) Ph: 703 551 (b)(6); (b)(7)(C) E:mail: (b)(6); (b)(7)(C) ACOR: (b)(6); (b)(7)(C) Ph: 703 551 (b)(6); (b)(7)(C) E:mail: (b)(6); (b)(7)(C)		21 QUANTITY		22 UNIT	
23 UNIT PRICE		24 AMOUNT		25 ACCOUNTING AND APPROPRIATION DATA	
26 TOTAL AWARD AMOUNT (For Govt. Use Only)		27a SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA X ARE ARE NOT ATTACHED.		27b CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4 FAR 52.212-5 IS ATTACHED. ADDENDA ARE ARE NOT ATTACHED.	
28 CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED		29 AWARD OF CONTRACT: REF. OFFER DATED YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS.		30a SIGNATURE OF OFFEROR/CONTRACTOR	
30b NAME AND TITLE OF SIGNER (Type or print)		30c DATE SIGNED		31a UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)	
31b NAME OF CONTRACTING OFFICER (Type or print) (b)(6); (b)(7)(C)		31c DATE SIGNED		32a CONTRACTING OFFICER'S OFFICE ADDRESS (Type or print)	

18 ITEM NO	20 SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
(b)(4); (b)(7)(E)				\$ _____	\$ _____
				\$ _____	\$ _____
				\$ _____	\$ _____
				\$ _____	\$ _____
				\$ _____	\$ _____

Continued ...

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

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

41a I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT 41b SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42a. RECEIVED BY (Print)	
		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)		
(b)(4); (b)(7)(E)						\$ _____	\$ _____
						\$ _____	\$ _____
						\$ _____	\$ _____
						\$ _____	\$ _____
						\$ _____	\$ _____

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)
(b)(4); (b)(7)(E)					

See attached Addenda pages for applicable clauses and provisions.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jun 2013 15:31:32 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Award summary review (cald1).doc - HSCEMD-13-J-00015  
**Attachments:** Award summary review (cald1).doc

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

Please see my comments concerning the award summary attached.

Please coordinate your revisions with me.

Thanks,

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

## REQUEST FOR LEGAL REVIEW

HSCEMD-13-J-00015 (HSI/Technical Operations Spectrum Support Services)

REQUEST DATE	DIVISION/OFFICE	CONTRACT SPECIALIST	TELEPHONE NO.
AQ DOC NO.	CONTRACTOR	CONTRACTING OFFICER	TELEPHONE NO.
CONTRACTING OFFICER'S COMMENTS		ATTORNEY'S COMMENTS	(b)(6); (b)(7)(C) 214-905 (b)(6); (b)(7)(C)
		<input type="checkbox"/> Legally Sufficient <input checked="" type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below)  DATE: June 13, 2013	
		(b)(5); (b)(7)(E)	

**\*\*\*Warning\*\*\* Attorney/Client Privilege\*\*\* Attorney Work Product\*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(5), (b)(7).~~

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

**~~\*\*\*Warning\*\*\* Attorney/Client Privilege\*\*\* Attorney Work Product\*\*\*~~**

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 30 May 2013 12:05:01 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Award Summary  
**Attachments:** Award Summary.docx

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

Here's the award summary

Thank you

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone: 214-90**(b)(6); **FAX: 214-905-5568**

**Email:**(b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

**Help us Support You Better: How's My Service?**

**AWARD SUMMARY AND DOCUMENTATION OF SELECTION  
MEMORANDUM**

**PROJECT TITLE:** Spectrum Professional Mission Support Services

**PROGRAM OFFICE:** Homeland Security Investigations (HSI)  
Technical Operations (TechOps)

**PROCUREMENT  
PARTICIPANTS**

(b)(6); (b)(7)(C)	Contracting Specialist (CS) Contract Officer (CO) Program Manager (PM) COTR National Program manager
(b)(6); (b)(7)(C)	Management Program Analyst
(b)(6); (b)(7)(C)	Technical Enforcement Officer

**GOVERNMENT ESTIMATE:** (b)(4)

	Base	1 <sup>st</sup> Option Year	2 <sup>nd</sup> Option Year	6 month Extension (52.217-8)	TOTAL
<b>IGCE</b>	(b)(4)				\$7,554,618.93

**PERIOD OF PERFORMANCE:** Base Period of 6 months plus two one year options. FAR Clause 52.217-8 Option to Extend Services was also evaluated.

**CONTRACT TYPE:** Time and Materials – Labor Hour

**SOLICITATION NUMBER:** 192113VHQ54SPC001

**CONTRACTOR:** ZANTECH IT Services, Inc.

**CONTRACT NUMBER:** TABSS Contract – HSCG23-12-D-ATB004

**ORDER NUMBER:** Order HSCEMD-13-J-00015

**AWARD AMOUNT:** (b)(4)

- Base Period
- 1<sup>st</sup> Option Year
- 2<sup>nd</sup> Option Year
- 6 Month Option

**TOTAL WITH OPTIONS:** \$ 5,979,448.80

This total does not include the travel CLIN. The RFQ stated “A Travel CLIN will be added to the task order and will not be used as part of the Total Price Evaluation”. In addition, the offerors were advised that all travel must be approved by the COR in advance and comply with the Federal Travel Regulation. The locations and durations of this travel will be determined as needed by the Government with an estimated 64 days total travel. \$ 50,000.00 was funded for the base period and additional funding, if needed, will be provided by the program office.

The following are the award amounts with the estimated travel CLIN:

<b>AWARD AMOUNT:</b>	(b)(4)	Base Period
		1 <sup>st</sup> Option year
		2 <sup>nd</sup> Option Year
	(b)(4)	- 6 Month Option - No Travel
<b>TOTAL WITH OPTIONS &amp; Travel:</b>	(b)(4)	<u>\$6,129,448.80</u>

**A. PURPOSE**

The purpose of this memorandum is: (1) to obtain approval to issue a task order against a Technical, Acquisition and Business Support Services (TABSS) multiple-award indefinite delivery/indefinite quantity (IDIQ) contract (2) to document the best value determination as stated in the RFQ.

**B. COMPLIANCE**

1. FAR 10 and 11.101 - Market Research was conducted for the requirement. A request for information (RFI) along with a draft statement of work (SOW) was sent to the TABSS contractors and 4 small businesses responded. Tab 1-1 - market research & 2-24 - RFI.
2. HSAM 3007.172 - The acquisition has an Advance Acquisition Plan (AAP) in the Acquisition Planning Forecast System (APFS) database, number 201301142. Streamlined AP is not required per HSAM 3007.103(3)(viii). AAP under Tab 1-3.
3. HSAM 3019.202-271 - The Small Business Review is under tab 1-4.
4. FAR 7.503 - The determination that the services are not Inherently Governmental and approval from the Balance Workforce Strategy (BWS) Program Management Office is under Tab 2-12.
5. FAR 16 – The contract type determination is under Tab 2-14.
6. FAR 17.202 - Contract Options. The Contracting Officer has determined that the inclusion of the options is in the best interest of the Government. It is highly likely that the options will be exercised. The Government has a need for continuity of operations without the costs of disrupted support. Offers are evaluated inclusive of options and extension. The determination is under Tab 2-15.



7. TABSS Contracting Officer already made a responsibility determination at the contract level. In addition, the ordering Contracting Officer has verified that the awardee, Zantech IT Services, Inc., is active in the System for Award Management (SAM) and made a further responsibility determination. Tab 3-31

### **C. PROCUREMENT HISTORY**

1. The Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Technical Operations (TechOps), Investigative Intercept Section (IIS), and Covert Video Program (CVP) has a new requirement for non-personal services for temporary professional mission support services in project management, network engineering, help desk/remedy assistance, technical Subject Matter Expertise (SME), procurement and budget assistance, logistics management and facility (warehouse) support. These temporary services are needed in order to support the Congressional funded mandate (Commercial Spectrum Enhancement Act (CSEA)) to relocate radio communication systems from certain spectrum bands, which were authorized to be auction for commercial purposes.

2. Considering the priorities for use of government services of the Federal Acquisition Regulations (FAR) 8.002 (2), and the DHS Directive 060-01, market research indicated that mission support services are commercially available through the General Services Administration (GSA) Multiple Award Schedule (MAS) Program, and through the Program Management, Administrative, Clerical, and Technical Services (PACTS) and Technical, Acquisition and Business Support Services (TABSS), both mandatory vehicles for use in accordance with DHS Directive 060-01. Because the PACTS contracts do not have Engineering and Logistician labor categories, the TABSS contract was found to be the best solution to satisfy this requirement. See contract binder Tab 1-1 for market research.

3. On February 8, 2013, a Request for Information (RFI) along with a draft statement of work was sent to the TABSS contractors in Domain One, Track 2 and 3. Track 2 is the Small Business Track (6 contractors) and Track 3 is 8(a) Track (4 contractors). 4 contractors (3 small and 1 small disadvantaged) responded to the RFI and demonstrated the capabilities to perform all task under this requirement. Tab 2-24

4. On March 27, 2013, an RFQ was emailed to the TABSS contract holders in Domain One, Track 2 and Track 3; 6 - Small Business and 4 - 8(a) business, Ten (10) contractors in total. The cut-off date for questions was 1 April 2013 and the RFQ responses were due on 16 April, 2013 by 2:00 PM CST. Tabs 2-19

5. On 3 and 4 April 2013, emails were sent to the ten (10) contractors providing them a copy of the questions asked and the answers provided by the Government. The email dated 3 April 2013 also contained the 1<sup>st</sup> and only amendment to the RFQ. Tab 2-20 & 2-22.

6. On 16 April 2013, 5 quotes were received in response to the RFQ (Tab 3-28, 3-30 & abstract in 3-25). All Quotes were received on time from the following contractors:

- Zantech IT Services, Inc.
- Immersion Consulting
- BayFirst Solutions LLC
- Dynamis, Inc.
- Sev1Tech, Inc.

(The contractors list above is in the order the quotes were received)

7. On 17 April 2013, the Contracting Officer assembled the Technical Evaluation Committee (TEC) and briefed them on their responsibilities and duties via teleconference. Confidentiality of the source selection proceedings was discussed. The final conflict of interest and confidentiality certification was received from the last member of the team. The other certificates from each TEC member had been received 4-16 April 2013. (Tab 3-34). The evaluation procedures in accordance with the Evaluation Plan (Tab 1-8) were discussed. The Technical Evaluation Committee was requested to provide their evaluation results by Monday, 22 April 2013 but the TEC Chairperson requested the due date to be changed to Friday, 26 April 2013; request was granted.

8. On 26 April 2013, the Technical Evaluation Committee finalized their evaluation of the responses to the RFQ and submitted their evaluation report to the Contracting Office (Tab 3-27).

9. From 29 April 2013 to 3 May 2013 the Contracting Specialist and the Contracting Officers conducted an individual evaluation of all the quotes. CO and CS concluded that the TEC had rushed through the evaluation and did not apply the evaluation factors consistently to all the quotes.

10. On 3 May 2013 a phone conference was schedule by the Contracting Officer/Source Selection Authority and the teleconference took place on 6 May 2013 @ 2:00 EST. All members of the TEC, CS and CO were present for the telecom.

11. During the teleconference on 6 May 2013 the CO explained to the TEC his concerns with the evaluation and asked the TEC to please look closely at two of the vendors

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

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

12. (b)(5); (b)(7)(E)

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

13. On 14 May 2013 the TEC Chairperson submitted a detailed evaluation on (b)(7)(E) in question. The report was detailed but contained inaccurate statements and comments.

14. On 15 & 16 Mar 2013 the CS and CO corrected the evaluation noting all the discrepancies and on 16 March the CO/SSA notified the TEC of his decision; TEC Chairperson thanked the CO for the decision information (TAB – 3-27 #4)

**D. BASIS FOR AWARD AND BEST VALUE ANALYSIS**

The RFQ stated that the Government will award a Time and Material Task Order contract with fixed price hourly labor rates to the responsible offeror whose offer conforms to the RFQ will be the most advantageous and offers the best value to the Government. As stated in the RFQ, The evaluation criteria consist of the following factors in descending order of importance: (1) Performance Capability, (2) Past Performance, and (3) Price. The non-price factors of Performance Capability and Past Performance when combined are significantly more important than price. Offerors were informed that the Government reserved the right to award to other than the lowest price Offeror or other than the highest technically rated Offeror and as offers become more equal in non-price factors, price becomes more important.

As stated in the RFQ the Technical Evaluation Factor of Performance Capability is comprised of the following sub-factors: (a) Technical Approach, (b) Organization, (c) Personnel Qualifications, (d) Specialized Experience and (e) Quality Control. Offerors were informed that the Government after reviewing the sub-factors would assign an overall adjectival rating and that the sub-factors would not be separately rated.

As stated in the evaluation plan, offers could be rated Excellent, Good, Satisfactory, Marginal, or Unsatisfactory on the Performance Capability non-priced factor. For the Technical Evaluation Factor of Past Performance the Offerors would be assigned a risk rating of Low Risk, Moderate Risk, High Risk or Neutral/Unknown Risk.

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

**PERFORMANCE CAPABILITY:**

As stated in the RFQ, the evaluation of the Offeror’s technical approach looked at the Offeror’s existing capability to meet the Statement of Work (SOW) and how the Offeror would implement and manage effectively the various tasks required to accomplish the SOW to include the Offeror’s described method of providing supervision and the coordination of work. Offerors were evaluated on their submitted organizational structure, their resources, how their resources would be utilized and the roles and responsibilities of the team members. In addition, the Offerors were evaluated on their submitted staffing plan and their timeline for providing the required personnel in accordance with the SOW. The evaluation of the Offeror’s proposed personnel looked at the proposed employee’s education and relevant work experience qualifications to accomplish the SOW. The evaluation of Specialized Experience looked at the Offeror’s relevant/similar experience within the last three years that would enhance their performance capability on this requirement. Relevant/similar contracts were defined as contracts that were similar in complexity, scope of work and dollar magnitude. Each Offeror was given one overall adjective rating for Performance Capability, based upon the evaluation of all sub-factors. The evaluation of the Offeror’s Quality Control Plan (QCP) looked at how the Offeror was going to ensure the SOW performance standards and acceptable quality level requirements would be met. The technical evaluation worksheets and the Evaluation Team summary evaluation report is located in tab 3-27.

The TEC convened and conducted their evaluation and provided their technical evaluation report to the Contracting Officer (CO), who in this source selection is the Source Selection Authority (SSA). The CS and CO reviewed and considered the technical evaluation team’s technical evaluation summary report, as well as reviewed the Offerors’ proposals. The CS and CO identified several inconsistencies in the technical evaluation summary report related to specific findings concerning evaluated proposal features and in the correlation between specific findings and the technical ratings assigned. As a result, the CS and CO conducted an independent assessment of the offerors’ proposals in conjunction with a review of the entire evaluation record. Based on this assessment of the entire evaluation record, review of the technical proposals, and consultation with the TEC, the SSA assigned the following technical ratings:

**OFFEROR’S PERFORMANCE CAPABILITY RATINGS:**

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

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

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

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

**OFFEROR'S PAST PERFORMANCE RISK RATINGS:**

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



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

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

**TECHNICAL NON-PRICE FACTORS RATING SUMMARY:**

Below are the ratings for each non-price evaluation factor in the order the quotes were received:

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

**PRICE:**

TABBS ID/IQ Contracting Officer (b)(6); (b)(7)(C) has already determined the rates for services offered at hourly rates under the TABSS contracts to be fair and reasonable. In addition, the ordering CO has also made a price fair and reasonable determination based on the TABSS contracts and the competition for this task order.

The RFQ instructed that Offerors shall quote a Time and Materials (T&M) (Labor Hour) type of pricing structure. The not to exceed hours (NTE) have been provided by the Government. The offer must be priced by the unit hourly rate(s) and extended amount for each labor classification. Price the base period line item(s), both 12 month options and 6 month extension option. Offerors were instructed that the price evaluated will be the total pricing for the base, the 2 - twelve month option periods and option to extend period in accordance with FAR part 52.217-3. Offerors were provided a blank Line Item Pricing Schedule were they were instructed to provide their TABSS labor hour rates for each labor category, the quoted price and the extended price. From this schedule, the Government was able to ascertain any discounts provided from the TABSS contracts.

Each Offeror quoted unit and extended labor prices was entered on an Excel Worksheet in order to perform a price comparison and is attachment # 1 to the Award Summary Document. Below is a summary of the overall pricing quoted by each Offeror arranged in the order the quotes were received:

**Pricing Summary Table:**

Offeror	Base	Option 1	Option 2	6-Month Extension	TOTAL
Zantech IT Services	(b)(4)				
Dynamis, Inc					
Sev1Tech, Inc					

Immersion Consulting	(b)(4)
BayFirst Solutions, LLC	

**TECHNICAL FACTORS RATING & PRICE SUMMARY:**

Below is a summary of the evaluation of the technical non-price factors arranged in the order the quotes were received:

Offeror	Performance Capability	Past Performance	Price
(b)(4); (b)(5); (b)(7)(E)			

**PRICE EVALUATION, LEVEL OF EFFORT AND LABOR MIX ANALYSIS:**

The RFQ stated that offerors may use Attachment A “Line Item Pricing Schedule” to provide their pricing and are permitted to upgrade, down grade and/or change labor categories suitable to accomplish the requirement in the SOW. However, Government will consider the level of effort and the mix of labor proposed to perform the work in evaluating total price. The price evaluated will be the total pricing for the base, the 2-twelve month option periods and option to extend period in accordance with FAR part 52.217-3. Because the Government stated on the RFQ that the non-price factors of Performance Capability and Past Performance when combined are significantly more important than price, the price evaluation was limited to the two highest performance capability and past performance of low risk offers; It was unlikely that the award would be made to a lower performance capability rating. (b)(5); (b)(7)(E)

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

The Government’s requirement included nine labor classifications, which were: Project Manager, Senior Computer Systems Specialist, Junior Acquisition Specialist, Logistician, Software Engineer, Senior Engineer, Junior Engineer, Engineer and Senior Program Management Specialist. The level of effort required by the SOW, in regards to number of personnel needed and hours required by labor category for each labor category was established by the Government. The offerors were permitted to upgrade, down grade and/or change labor

categories suitable to accomplish the requirement in the SOW, but only Zantech changed one labor category.

The SOW stated the required education and experience needed for each labor category, which provided the prospective Offerors the information needed to help them determine the labor mix. The minimum education and experience requirement stated in the SOW for each labor classification are as follows:

Project Manager - B.A. or B.S. degree & eight (8) years' experience in managing large, complex technical efforts involving multiple facets of an engineering discipline.

Senior Computer Systems Specialist - B.A. or B.S. degree & minimum of five (5) years' experience in assisting with large, complex technical efforts involving multiple facets of large projects and programs.

Junior Acquisition Specialist - Bachelor's Degree in Acquisitions, Accounting or Business & minimum of two (2) years Relevant Experience.

Logistician - High School Diploma & five (5) years' warehousing experience.

Software Engineer - B.A. or B.S. degree in relevant field & six (6) years minimum experience of specialized experience including knowledge of covert video, as well as networking and email standards and work on a help desk.

Senior Engineer - Master of Science in any Engineering discipline & Twelve (12) years total; Six (6) years minimum in specialty, or equivalent work experience

Junior Engineer - BA/BS in any Engineering discipline & minimum experience of four (4) years total; Two (2) years minimum in specialty, or equivalent work experience.

Engineer - BA/BS in a relevant field & Six (6) years total; Two (2) years minimum in specialty, or equivalent work experience.

Senior Program Management Specialist - B.A. or B.S. degree & minimum experience of five (5) years' experience in assisting with large, complex technical efforts involving multiple facets of large projects and programs.

### **Zantech IT Services, Inc.**

Level of Effort & Labor Mix. Zantech proposed using their TABSS Pricelist labor classifications of Senior Business Subject Matter Expert for the Government's Project Manager. All the other labor classifications were the same as the Government.

The RFQ required the Offerors to list the education and experience levels of all their proposed personnel. The labor mix, except for one senior engineer, proposed by Zantech met or exceeded the Government's education and experience requirement. The labor mix proposed by Zantech is the appropriate labor category from their TABSS pricelist. The level of effort and labor mix is commensurate with the work required.

Price Analysis. (b)(5); (b)(7)(E) The quoted price (b)(4) included services for the base (six months), the two option years and the 6-month extension. The hourly rates for the labor category on TABSS pricelist and proposed discounted hourly rates are:

Direct Labor by Category	Base Period			Option 1			Option 2			Extension		
	TABBS Rate	Proposed Rate	% Diff	TABBS Rate	Proposed Rate	% Diff	TABBS Rate	Proposed Rate	% Diff	TABBS Rate	Proposed Rate	% Diff
Senior Business Subject Matter Expert*	(b)(4)											
Senior Computer Systems Specialist	(b)(4)											
Junior Acquisition Analyst	(b)(4)											
Logistician (3)	(b)(4)											
Software Engineer/Analyst (2)	(b)(4)											
Senior Engineer (2)	(b)(4)											
Junior Engineer (2)	(b)(4)											
Engineer	(b)(4)											
Senior Program Management Specialist (2)	(b)(4)											

**BayFirst Solutions, LLC.**

Level of Effort & Labor Mix. BayFirst proposed using their TABSS Pricelist labor classifications same as identified by the Government.

The RFQ required the Offerors to list the education and experience levels of all their proposed personnel. Most of the labor mix proposed by BayFirst met or exceeded the Government’s education and experience requirement. 2 of the 3 logisticians and the 2 software engineers did not show to have the level of experience outlined in the SOW

The labor mix proposed by BayFirst is the appropriate labor category from their TABSS pricelist. The level of effort and labor mix is commensurate with the work required.

Price Analysis. (b)(5); (b)(7)(E) BayFirst quoted price of (b)(4) included services for the base (six months), the two option years and the 6-month extension. The hourly rates for the labor category on TABSS pricelist and proposed discounted hourly rates are:

Direct Labor by Category	Base Period			Option 1			Option 2			Extension		
	TABBS Rate	Proposed Rate	% Diff	TABBS Rate	Proposed Rate	% Diff	TABBS Rate	Proposed Rate	% Diff	TABBS Rate	Proposed Rate	% Diff
Project Manager	(b)(4)											
Senior Computer Systems Specialist	(b)(4)											
Junior Acquisition Analyst	(b)(4)											
Logistician (3)	(b)(4)											
Software Engineer/Analyst (2)	(b)(4)											
Senior Engineer (2)	(b)(4)											
Junior Engineer (2)	(b)(4)											
Engineer	(b)(4)											
Senior Program Management Specialist (2)	(b)(4)											

**BEST VALUE TRADE-OFF:**

The RFQ stated that the non-price factors of Performance Capability and Past Performance when combined were significantly more important than Price. Also, the RFQ stated that the Government reserved the right to award to other than the lowest price Offeror or other than the highest technically rated Offeror.

The evaluation ratings and price for the two highest performance capability and past performance of low risk offers following table:

<b>Offeror</b>	<b>Performance Capability</b>	<b>Past Performance</b>	<b>Price</b>
(b)(4); (b)(5); (b)(7)(E)			

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

**E. CONCLUSION**

(b)(5)

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

Contract Administrator

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

Contracting Officer



**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jun 2013 20:03:51 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Award summary review (cald1).doc - HSCEMD-13-J-00015  
**Attachments:** Award summary review (response).doc, Award Summary after Amendment 2.docx, Award Summary after Amendment 2(cald2).docx

(b)(6);

Thanks. Please see attached award summary (cald2), for proposed revision. No legal objections.

Thanks,

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor

(p) 214.90 (b)(6);  
(bb) 214.9 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)

**Sent:** Thursday, June 13, 2013 2:12 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: Award summary review (cald1).doc - HSCEMD-13-J-00015

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

Here's the revised award summary and legal review form.

Thank you sir

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone:** 214-905-(b)(6) **FAX:** 214-905-5568  
**Email:** [mario.curriel@ice.dhs.gov](mailto:mario.curriel@ice.dhs.gov)

***Your First Partner in Acquisition!***  
**Help us Support You Better: [How's My Service?](#)**

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, June 13, 2013 10:32 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** Award summary review (cald1).doc - HSCEMD-13-J-00015

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

Please see my comments concerning the award summary attached.

Please coordinate your revisions with me.

Thanks

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

## REQUEST FOR LEGAL REVIEW

HSCEMD-13-J-00015 (HSI/Technical Operations Spectrum Support Services)

REQUEST DATE	DIVISION/OFFICE	CONTRACT SPECIALIST	TELEPHONE NO.
AQ DOC NO.	CONTRACTOR	CONTRACTING OFFICER	TELEPHONE NO.
CONTRACTING OFFICER'S COMMENTS		ATTORNEY'S COMMENTS	(b)(6); (b)(7)(C) 214-905 (b)(6); (b)(7)(C)
(b)(5); (b)(7)(E)		<input type="checkbox"/> Legally Sufficient <input checked="" type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below)  DATE: June 13, 2013	
		(b)(5); (b)(7)(E)	

**\*\*\*Warning\*\*\* Attorney/Client Privilege\*\*\* Attorney Work Product\*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(5), (b)(7).~~

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

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

**\*\*\*Warning\*\*\* Attorney/Client Privilege\*\*\* Attorney Work Product\*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(5), (b)(7).~~

**AWARD SUMMARY AND DOCUMENTATION OF SELECTION  
MEMORANDUM**

**PROJECT TITLE:** Spectrum Professional Mission Support Services

**PROGRAM OFFICE:** Homeland Security Investigations (HSI)  
Technical Operations (TechOps)

**PROCUREMENT  
PARTICIPANTS**

(b)(5); (b)(7)(E)	Contracting Specialist (CS)
(b)(5); (b)(7)(E)	Contract Officer (CO)
(b)(5); (b)(7)(E)	Program Manager (PM)
(b)(5); (b)(7)(E)	COTR
(b)(5); (b)(7)(E)	National Program manager
(b)(5); (b)(7)(E)	Management Program Analyst
(b)(5); (b)(7)(E)	Technical Enforcement Officer

**GOVERNMENT ESTIMATE:** (b)(4)

	Base	1 <sup>st</sup> Option Year	2 <sup>nd</sup> Option Year	6 month Extension (52.217-8)	TOTAL
<b>IGCE</b>	(b)(4)				

**PERIOD OF PERFORMANCE:** Base Period of 6 months plus two one year options. FAR Clause 52.217-8 Option to Extend Services was also evaluated.

**CONTRACT TYPE:** Time and Materials – Labor Hour

**SOLICITATION NUMBER:** 192113VHQ54SPC001

**CONTRACTOR:** ZANTECH IT Services, Inc.

**CONTRACT NUMBER:** TABSS Contract – HSCG23-12-D-ATB004

**ORDER NUMBER:** Order HSCEMD-13-J-00015

**AWARD AMOUNT:** (b)(4) Base Period  
1<sup>st</sup> Option Year  
2<sup>nd</sup> Option Year  
6 Month Option

**TOTAL WITH OPTIONS:** \$ 5,727,924.80

This total does not include the travel CLIN. The RFQ stated “A Travel CLIN will be added to the task order and will not be used as part of the Total Price Evaluation”. In addition, the Offerors were advised that all travel must be approved by the COR in advance and comply with the Federal Travel Regulation. The locations and durations of this travel will be determined as needed by the Government with an estimated 64 days total travel. \$ 50,000.00 was funded for the base period and additional funding, if needed, will be provided by the program office.

The following are the award amounts with the estimated travel CLIN:

<b>AWARD AMOUNT:</b>	(b)(4)	Base Period
		1 <sup>st</sup> Option Year
		2 <sup>nd</sup> Option Year
	(b)(4)	- 6 Month Option - No Travel
<b>TOTAL WITH OPTIONS &amp; Travel:</b>	(b)(4)	= \$5,877,924.80

**A. PURPOSE**

The purpose of this memorandum is: (1) to obtain approval to issue a task order against a Technical, Acquisition and Business Support Services (TABSS) multiple-award indefinite delivery/indefinite quantity (IDIQ) contract (2) to document the best value determination as stated in the RFQ.

**B. COMPLIANCE**

1. FAR 10 and 11.101 - Market Research was conducted for the requirement. A request for information (RFI) along with a draft statement of work (SOW) was sent to the TABSS contractors and 4 small businesses responded. Tab 1-1 - market research & 2-24 - RFI.
2. HSAM 3007.172 - The acquisition has an Advance Acquisition Plan (AAP) in the Acquisition Planning Forecast System (APFS) database, number 201301142. Streamlined AP is not required per HSAM 3007.103(3)(viii). AAP under Tab 1-3.
3. HSAM 3019.202-271 - The Small Business Review is under tab 1-4.
4. FAR 7.503 - The determination that the services are not Inherently Governmental and approval from the Balance Workforce Strategy (BWS) Program Management Office is under Tab 2-12.
5. FAR 16 – The contract type determination is under Tab 2-14.
6. FAR 17.202 - Contract Options. The Contracting Officer has determined that the inclusion of the options is in the best interest of the Government. It is highly likely that the options will be exercised. The Government has a need for continuity of operations without the costs of disrupted support. Offers are evaluated inclusive of options and extension. The determination is under Tab 2-15.

7. TABSS Contracting Officer already made a responsibility determination at the contract level. In addition, the ordering Contracting Officer has verified that the awardee, Zantech IT Services, Inc., is active in the System for Award Management (SAM) and made a further responsibility determination. Tab 3-31

### **C. PROCUREMENT HISTORY**

1. The Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Technical Operations (TechOps), Investigative Intercept Section (IIS), and Covert Video Program (CVP) has a new requirement for non-personal services for temporary professional mission support services in project management, network engineering, help desk/remedy assistance, technical Subject Matter Expertise (SME), procurement and budget assistance, logistics management and facility (warehouse) support. These temporary services are needed in order to support the Congressional funded mandate (Commercial Spectrum Enhancement Act (CSEA)) to relocate radio communication systems from certain spectrum bands, which were authorized to be auction for commercial purposes.

2. Considering the priorities for use of government services of the Federal Acquisition Regulations (FAR) 8.002 (2), and the DHS Directive 060-01, market research indicated that mission support services are commercially available through the General Services Administration (GSA) Multiple Award Schedule (MAS) Program, and through the Program Management, Administrative, Clerical, and Technical Services (PACTS) and Technical, Acquisition and Business Support Services (TABSS), both mandatory vehicles for use in accordance with DHS Directive 060-01. Because the PACTS contracts do not have Engineering and Logistician labor categories, the TABSS contract was found to be the best solution to satisfy this requirement. See contract binder Tab 1-1 for market research.

3. On February 8, 2013, a Request for Information (RFI) along with a draft statement of work was sent to the TABSS contractors in Domain One, Track 2 and 3. Track 2 is the Small Business Track (6 contractors) and Track 3 is 8(a) Track (4 contractors). 4 contractors (3 small and 1 small disadvantaged) responded to the RFI and demonstrated the capabilities to perform all task under this requirement. Tab 2-24

4. On March 27, 2013, an RFQ was emailed to the TABSS contract holders in Domain One, Track 2 and Track 3; 6 - Small Business and 4 - 8(a) business, Ten (10) contractors in total. The cut-off date for questions was 1 April 2013 and the RFQ responses were due on 16 April, 2013 by 2:00 PM CST. Tabs 2-19

5. On 3 and 4 April 2013, emails were sent to the ten (10) contractors providing them a copy of the questions asked and the answers provided by the Government. The email dated 3 April 2013 also contained the 1<sup>st</sup> and only amendment to the RFQ. Tab 2-20 & 2-22.

6. On 16 April 2013, 5 quotes were received in response to the RFQ (Tab 3-28, 3-30 & abstract in 3-25). All Quotes were received on time from the following contractors:

- Zantech IT Services, Inc.

- Immersion Consulting
- BayFirst Solutions LLC
- Dynamis, Inc.
- Sev1Tech, Inc.

(The contractors list above is in the order the original quotes were received)

7. On 17 April 2013, the Contracting Officer assembled the Technical Evaluation Committee (TEC) and briefed them on their responsibilities and duties via teleconference. Confidentiality of the source selection proceedings was discussed. The final conflict of interest and confidentiality certification was received from the last member of the team. The other certificates from each TEC member had been received 4-16 April 2013. (Tab 3-34). The evaluation procedures in accordance with the Evaluation Plan (Tab 1-8) were discussed. The Technical Evaluation Committee was requested to provide their evaluation results by Monday, 22 April 2013 but the TEC Chairperson requested the due date to be changed to Friday, 26 April 2013; request was granted.

8. On 26 April 2013, the Technical Evaluation Committee finalized their evaluation of the responses to the RFQ and submitted their evaluation report to the Contracting Office (Tab 3-27).

9. From 29 April 2013 to 3 May 2013 the Contracting Specialist and the Contracting Officers conducted an individual evaluation of all the quotes. CO and CS concluded that the TEC had rushed through the evaluation and did not apply the evaluation factors consistently to all the quotes.

10. On 3 May 2013 a phone conference was schedule by the Contracting Officer/Source Selection Authority and the teleconference took place on 6 May 2013 @ 2:00 EST. All members of the TEC, CS and CO were present for the telecom.

11. During the teleconference on 6 May 2013 the CO explained to the TEC his concerns with the evaluation and asked the TEC to please look closely at two of the Offerors. (b)(5); (b)(7)(E)

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

12. (b)(5); (b)(7)(E)

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

13. On 14 May 2013 the TEC Chairperson submitted a detailed evaluation on the two offeror's in question. The report was detailed but contained inaccurate statements and comments.



14. On 15 & 16 May 2013 the CS and CO corrected the evaluation noting all the discrepancies and on 16 May the CO/SSA notified the TEC of his decision; TEC Chairperson thanked the CO for the decision information (TAB – 3-27 #4)

15. On 22 & 23 May 2013 the OAQ Deputy Assistant Director for the HSI, West Team and the Assistant Director for OAQ Dallas reviewed and concurred with the award summary.

16. On 29 May 2013, OPLA gave OAQ a “verbal” notification that the award was not legally sufficient. OPLA’s opinion was based on the Key Personnel minimum qualifications. None of the proposals had offered key personnel that met all the minimum qualifications (experience). In support of making the award, the CO cited case no. 00-579 in the United States Court of Federal Claims where the Court of Federal Claims differentiates between “minimum requirements” and “mandatory minimum requirements” the Court stated *“Rather this court is obliged to look to the Solicitation in determining whether the minimum personnel requirements, combined with the clause requiring that complying resumes be submitted for each of the key positions, comprised a mandatory minimum requirement.”*. OPLA did not agree and cited GAO case B-406708; in this case, one of the Offerors quote was rated “Unacceptable” because the key personnel did not meet the minimum requirements and GAO agreed.

17. Between 29 May and 3 June 2013, OAQ met with the Program office to determine the actual qualification level required for personnel experience. OAQ in conjunction with OPLA and with the Program offices’ approval changed some of the minimum experiences to desirable experiences in the SOW/RFQ.

18. On 3 June 2013 the amendment to the RFQ reflecting the changes to the desirable experiences was sent to the 5 Offerors whom originally had responded to the RFQ and allowed for submission of revised proposals if the Offerors needed to submit one. Due date for revised proposal (if needed) was 6 June 2013 @ 4:00 PM CST.

19. Questions concerning the amendment were submitted to the CO on 3 June 2013 and answers were provided to all 5 Offerors the same day.

20. On 6 June 2013, all 5 Offerors provided revised proposals.

21. On 7 June 2013 the CS and CO evaluated the changes to the previously evaluated proposals and prepared this award summary.

#### **D. BASIS FOR AWARD AND BEST VALUE ANALYSIS**

The RFQ stated that the Government will award a Time and Material Task Order contract with fixed price hourly labor rates to the responsible offeror whose offer conforms to the RFQ will be the most advantageous and offers the best value to the Government. As stated in the RFQ, The evaluation criteria consist of the following factors in descending order of importance: (1) Performance Capability, (2) Past Performance, and (3) Price. The non-price factors of Performance Capability and Past Performance when combined are significantly more important than price. Offerors were informed that the Government reserved the right to award to other than

the lowest price Offeror or other than the highest technically rated Offeror and as offers become more equal in non-price factors, price becomes more important.

As stated in the RFQ the Technical Evaluation Factor of Performance Capability is comprised of the following sub-factors: (a) Technical Approach, (b) Organization, (c) Personnel Qualifications, (d) Specialized Experience and (e) Quality Control. Offerors were informed that the Government after reviewing the sub-factors would assign an overall adjectival rating and that the sub-factors would not be separately rated.

As stated in the evaluation plan, offers could be rated Excellent, Good, Satisfactory, Marginal, or Unsatisfactory on the Performance Capability non-priced factor. For the Technical Evaluation Factor of Past Performance the Offerors would be assigned a risk rating of Low Risk, Moderate Risk, High Risk or Neutral/Unknown Risk.

Offeror	Performance Capability	Past Performance	Price
(b)(4); (b)(5); (b)(7)(E)			

**PERFORMANCE CAPABILITY:**

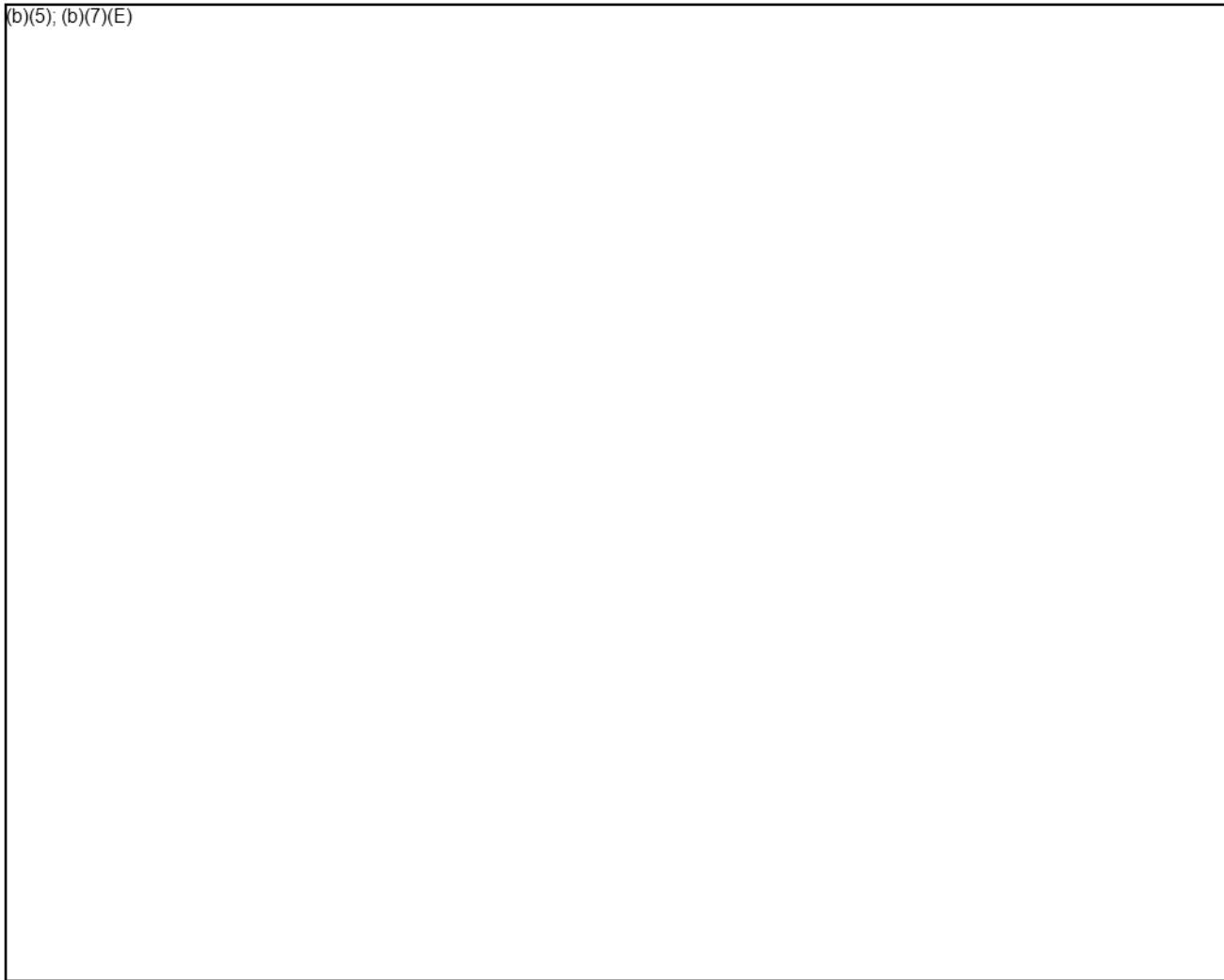
As stated in the RFQ, the evaluation of the Offeror’s technical approach looked at the Offeror’s existing capability to meet the Statement of Work (SOW) and how the Offeror would implement and manage effectively the various tasks required to accomplish the SOW to include the Offeror’s described method of providing supervision and the coordination of work. Offerors were evaluated on their submitted organizational structure, their resources, how their resources would be utilized and the roles and responsibilities of the team members. In addition, the Offerors were evaluated on their submitted staffing plan and their timeline for providing the required personnel in accordance with the SOW. The evaluation of the Offeror’s proposed personnel looked at the proposed employee’s education and relevant work experience qualifications to accomplish the SOW. The evaluation of Specialized Experience looked at the Offeror’s relevant/similar experience within the last three years that would enhance their performance capability on this requirement. Relevant/similar contracts were defined as contracts that were similar in complexity, scope of work and dollar magnitude. The evaluation of the Offeror’s Quality Control Plan (QCP) looked at how the Offeror was going to ensure the SOW performance standards and acceptable quality level requirements would be met. Each Offeror was given one overall adjective rating for Performance Capability, based upon the evaluation of all sub-factors. The technical evaluation worksheets and the Evaluation Team summary evaluation report is located in tab 3-27.

The TEC convened and conducted their evaluation and provided their technical evaluation report to the Contracting Officer (CO), who in this source selection is the Source Selection Authority (SSA). The CS and CO reviewed and considered the technical evaluation team’s technical

evaluation summary report, as well as reviewed the Offerors' proposals. The CS and CO identified several inconsistencies in the technical evaluation summary report related to specific findings concerning evaluated proposal features and in the correlation between specific findings and the technical ratings assigned. As a result, the CS and CO conducted an independent assessment of the Offerors' proposals in conjunction with a review of the entire evaluation record. The CS and CO also independently evaluated the revised proposals that were a result of amendment 2. Three of the revised proposals had minor changes in the Performance Capability, one offeror changed two of the key personnel and one offeror changed one of the key personnel. Two of the proposals included price changes. Based on the assessment of the entire evaluation record, review of the technical proposals and revised technical proposals, and consultation with the TEC, the SSA assigned the following technical ratings:

**OFFEROR'S PERFORMANCE CAPABILITY RATINGS:**

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



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

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

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

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

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



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

**TECHNICAL NON-PRICE FACTORS RATING SUMMARY:**

Below are the ratings for each non-price evaluation factor in the order the quotes were received:

<b>Offeror</b>	<b>Performance Capability</b>	<b>Past Performance</b>
(b)(7)(E); (b)(5)		

**PRICE:**

TABBS ID/IQ Contracting Officer, (b)(6); (b)(7)(C) has already determined the rates for services offered at hourly rates under the TABSS contracts to be fair and reasonable. In addition, the ordering CO has also made a price fair and reasonable determination based on the TABSS contracts and the competition for this task order.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Jul 2014 16:44:00 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Commercial or Non-commercial Item, that is the question

FYI. Quick turnaround.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-<sup>(b)(6);</sup><sub>(b)(7)(C)</sub>  
**Email:** (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, July 22, 2014 3:40 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: Commercial or Non-commercial Item, that is the question

(b)(6); (b)(7)(C); (b)(5); (b)(7)(E)

(b)(6); (b)(7)(C); (b)(5); (b)(7)(E)

V/R

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

Contracts Manager

Harris Corporation

Phone: 321-30

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

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Tuesday, July 22, 2014 4:28 PM

**To:** (b)(6); (b)(7)(C)

**Subject:** Commercial or Non-commercial Item, that is the question

**Importance:** High

Team:

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

Please advise ASAP. Many thanks.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-5

**Email:**

**From:** (b)(6); (b)(7)(C)  
**Sent:** 10 Nov 2015 16:49:35 -0500  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Stingrays/FYI

Thanks (b)(6); (b)(7)(C) I forwarded your email to (b)(6); (b)(7)(C) Chief HSILD, for his awareness.

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

Chief  
Commercial and Administrative Law Division

p: 202.732 (b)(6); (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, November 10, 2015 10:40 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Stingrays/FYI

FYSA

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, November 10, 2015 8:21 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Stingrays/FYI

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

FYI- We have bought Stingrays down here for the past several years.

V/r,

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor

(o) 214.9 (b)(6); (b)(7)(C)  
(c) 214.92 (b)(6); (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal~~

Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, November 10, 2015 7:17 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Stingrays/FYI

(b)(7)(E)

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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6);  
Blackberry: 202-380-(b)(6);  
Email: (b)(6); (b)(7)(C)

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.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jun 2016 12:13:35 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Harris

Harris's Crossbows were the upgrade to Harris's Stingrays. This equipment is for

(b)(7)(E)

FYI: ICE could be procuring equipment to (b)(7)(E) I would reach out to (b)(6); (b)(7)(C) from Techops. He could provide more definitive information.

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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6);  
Blackberry: 202-380-(b)(6);  
Email: (b)(6); (b)(7)(C)

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.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 21 Jan 2020 14:24:36 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Harris Crossbow Bailment Agreement

Harris Crossbow Bailment Agreement

(b)(7)(E)



**From:** (b)(6); (b)(7)(C)  
**Sent:** 18 Sep 2012 12:37:44 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Proposed LSJ for purchase of a Crossbow System from Harris Corporation  
**Attachments:** Sole Source Harris Crossbow System.doc, Sole Source Harris Crossbow System(cald1).doc  
**Importance:** High

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

Please take a look at my proposed edits. If you have questions, let's please discuss. Otherwise, I have no legal objection.

V/r

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§~~

~~552(b)(5), (b)(7)~~

~~**From:** (b)(6); (b)(7)(C)~~

~~**Sent:** Monday, September 17, 2012 4:37 PM~~

~~**To:** (b)(6); (b)(7)(C)~~

~~**Subject:** Porposed LSJ for purchase of a Crossbow System from Harris Corporation~~

~~**Importance:** High~~

Gentlemen:

I you would please review the attached draft document and provide your comments, I would appreciate it. (b)(7)(E)

(b)(7)(E)

I am trying to make award by this coming Friday, so I need your input quickly please. Many thanks.

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

**Mission Support - Dallas (MSD), OI East Team – Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-900-(b)(6);

Email: (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

Help us Support You Better: [How's My Service?](#)

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

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

**2. Nature and/or Description of the Action Being Approved**

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

**3. Description of Supplies/Services**

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

~~—FOR OFFICIAL USE ONLY—LAW ENFORCEMENT SENSITIVE—~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

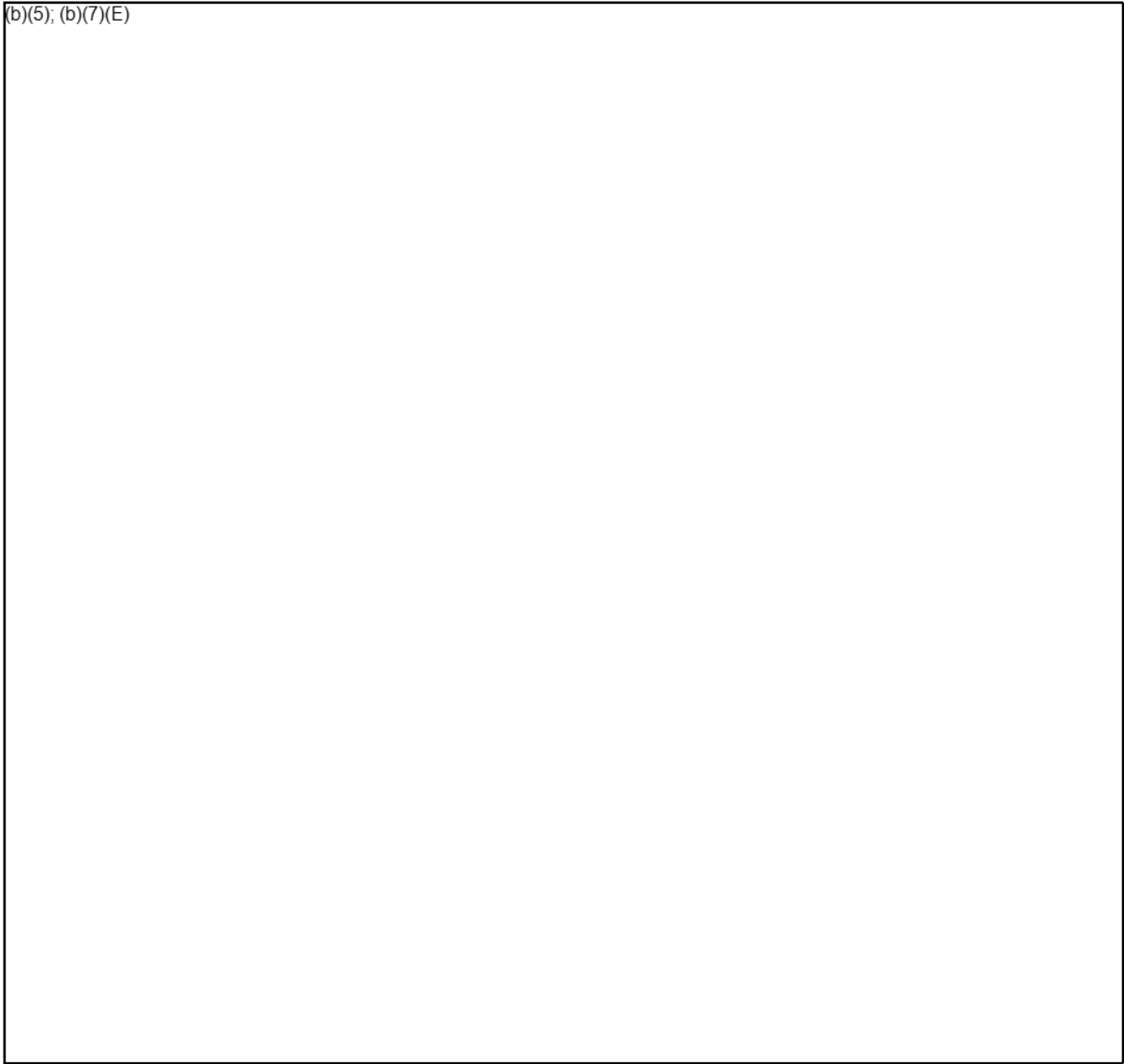
(b)(5); (b)(7)(E)

~~—FOR OFFICIAL USE ONLY—LAW ENFORCEMENT SENSITIVE—~~

Source Selection Sensitive in accordance with FAR 3.104-4

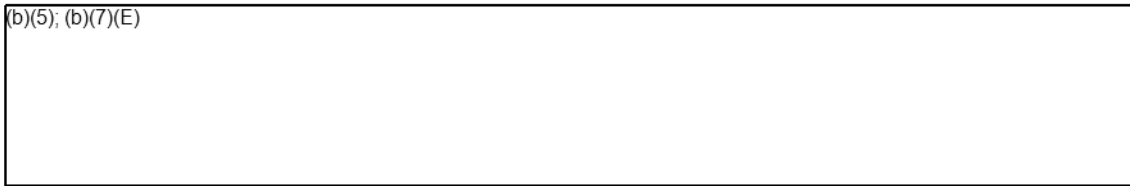
**6. Efforts to Obtain Competition**

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



**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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



**8. Description of Market Research**

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

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

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

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

\_\_\_\_\_  
(b)(6); (b)(7)(C)

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)  
Technical Operations (Tech Ops)  
Phone number: 703- (b)(6);

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

\_\_\_\_\_  
(b)(6); (b)(7)(C)

\_\_\_\_\_  
Date

Contracting Officer  
ICE/OAQ - MSD

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
OAQ-MD-AD

\_\_\_\_\_  
Date

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
OPLA

\_\_\_\_\_  
Date



Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

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

**2. Nature and/or Description of the Action Being Approved**

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

**3. Description of Supplies/Services**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

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

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**8. Description of Market Research**

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

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

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

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

\_\_\_\_\_ Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703 (b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER'S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

\_\_\_\_\_ Date

Contracting Officer  
ICE/OAQ - MSD

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
OAQ-MD-AD

\_\_\_\_\_  
Date

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
OPLA

\_\_\_\_\_  
Date

**From:** (b)(6); (b)(7)(C)  
**Sent:** 1 Apr 2016 11:26:58 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Request for legal of Supply of Harris equipment.  
**Attachments:** Sole Source OTA Sole Source Harris 2016 - 31 March 2016.doc, Sole Source OTA Sole Source Harris 2016 - 31 March 2016(cald).doc

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

I made a few revisions and comments in track-changes format. Please review and revise LSJ accordingly. I will return to Dallas next week and can sign-off on the final version.

V/r,

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(c) 214.924 (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, March 31, 2016 1:46 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Request for legal of Supply of Harris equipment.

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

Request legal review of the attached sole source word document for the supply of Harris Over-the-Air equipment. Hard copy of legal review request will be hand delivery.

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

Investigations & Operations Support Dallas | Deputy Assistant Director

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6);

Blackberry: 202-381-(b)(6);

Email: (b)(6); (b)(7)(C)

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.~~



Department of Homeland Security (DHS)  
Immigration & Customs Enforcement (ICE)  
Office of Acquisition Management (OAQ)  
Investigations and Operations Support Dallas

**Justification and Approval for other than Full and Open Competition**

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

**1. Agency and Contracting Activity**

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

**2. Nature and/or Description of the Action Being Approved**

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

**3. Description of Supplies/Services**

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

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

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

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

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

**6. Efforts to Obtain Competition**

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

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

**8. Description of Market Research**

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

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

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

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703 (b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

\_\_\_\_\_  
Date

Contracting Officer

ICE/OAQ - MSD

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

**Reviewed by:**

(b)(6); (b)(7)(C)  
OAQ-IOSD-DAD

\_\_\_\_\_  
Date

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
OAQ-IOSD-AD

\_\_\_\_\_  
Date

**Approved by:**

This justification is hereby approved:

(b)(6); (b)(7)(C)  
\_\_\_\_\_  
Competition Advocate  
Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

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

**Justification and Approval for other than Full and Open Competition**

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

**1. Agency and Contracting Activity**

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

**2. Nature and/or Description of the Action Being Approved**

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

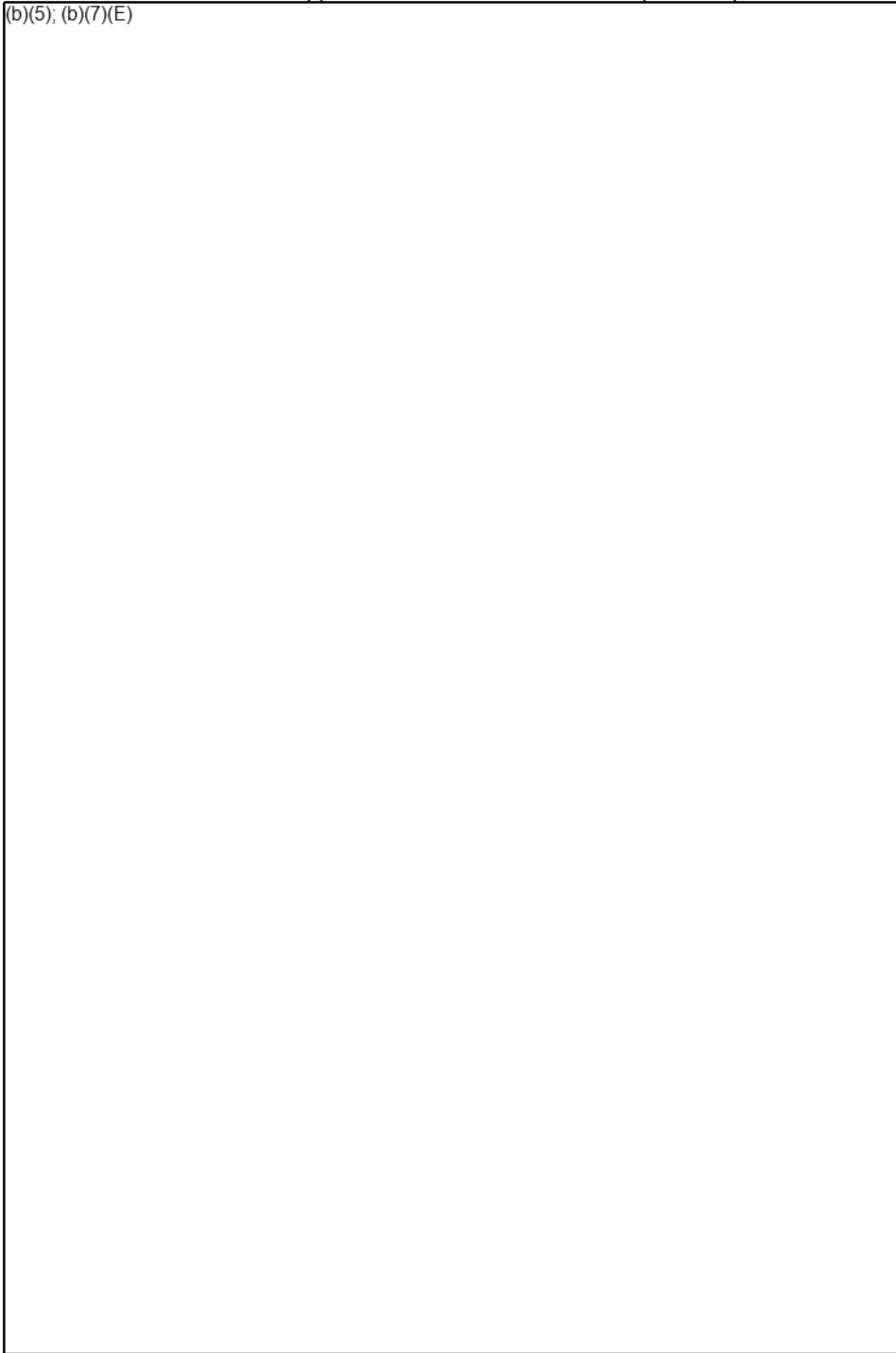
**3. Description of Supplies/Services**

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

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Justification and Approval for Other than Full and Open Competition

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



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



~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

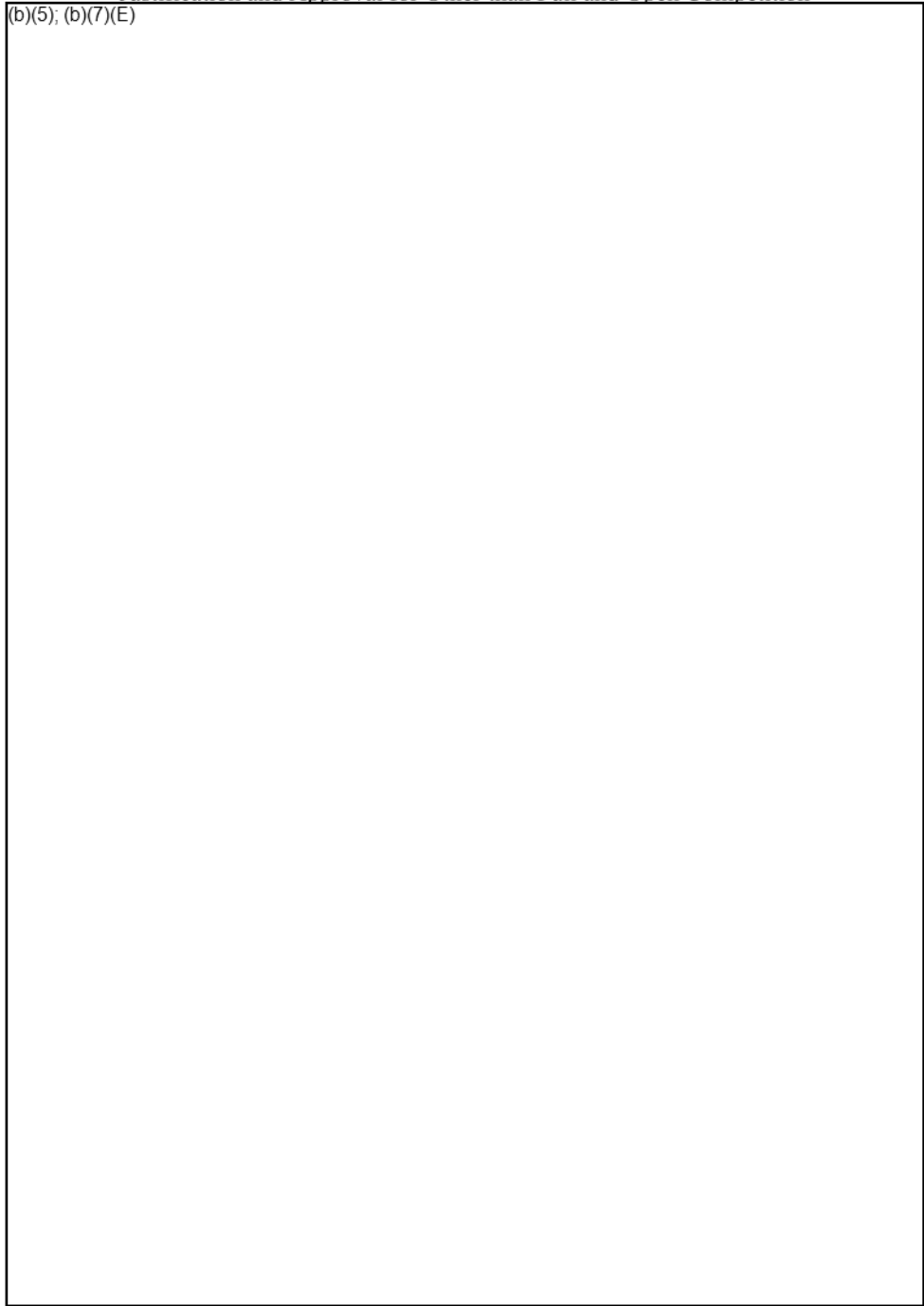
Source Selection Sensitive in accordance with FAR 3.104-4



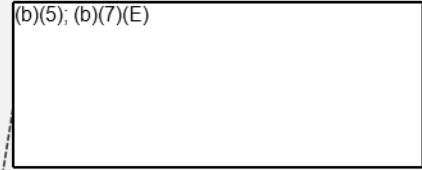
~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Justification and Approval for Other than Full and Open Competition

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



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



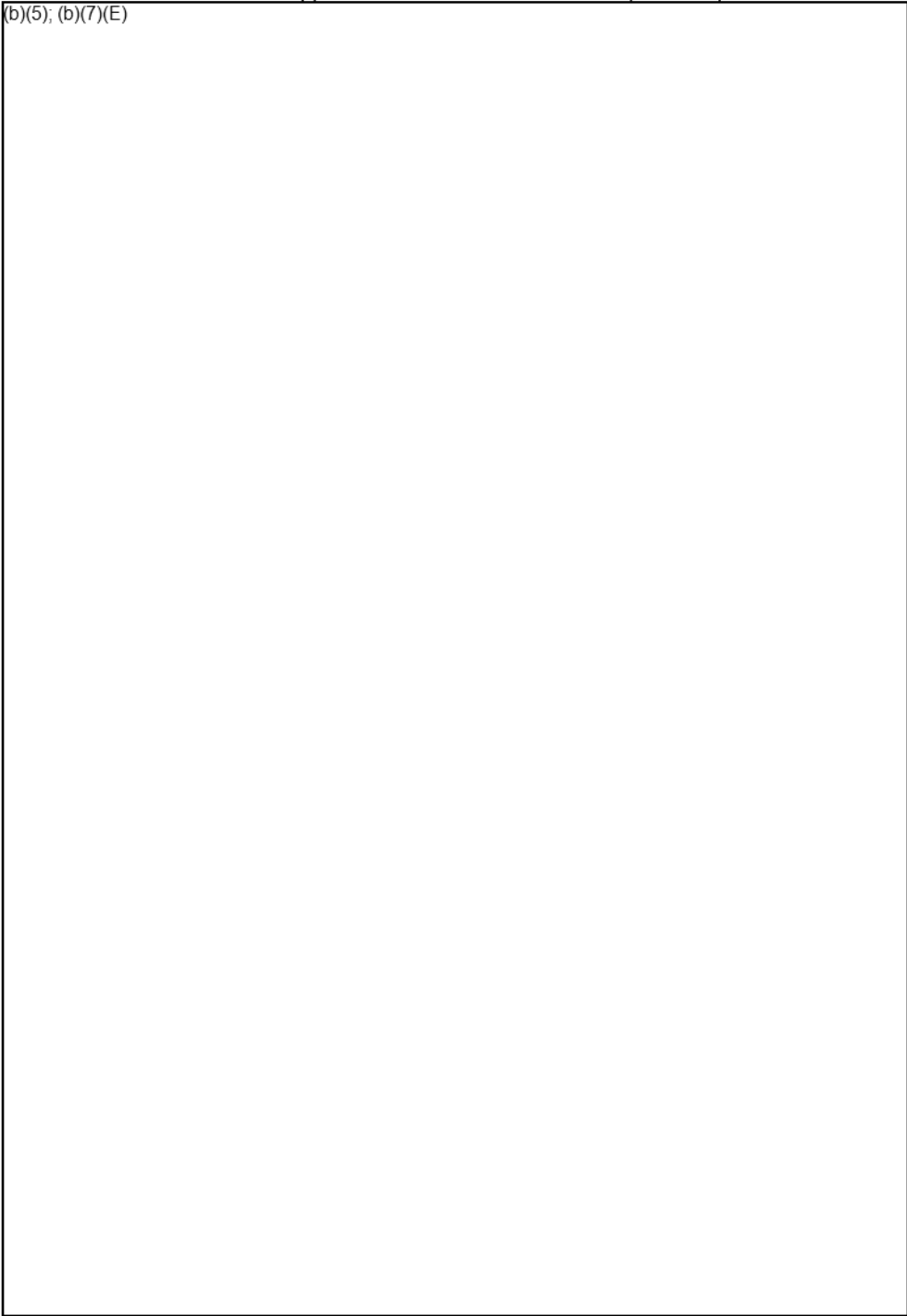
~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Source Selection Sensitive in accordance with FAR 3.104-4

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Justification and Approval for Other than Full and Open Competition

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



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

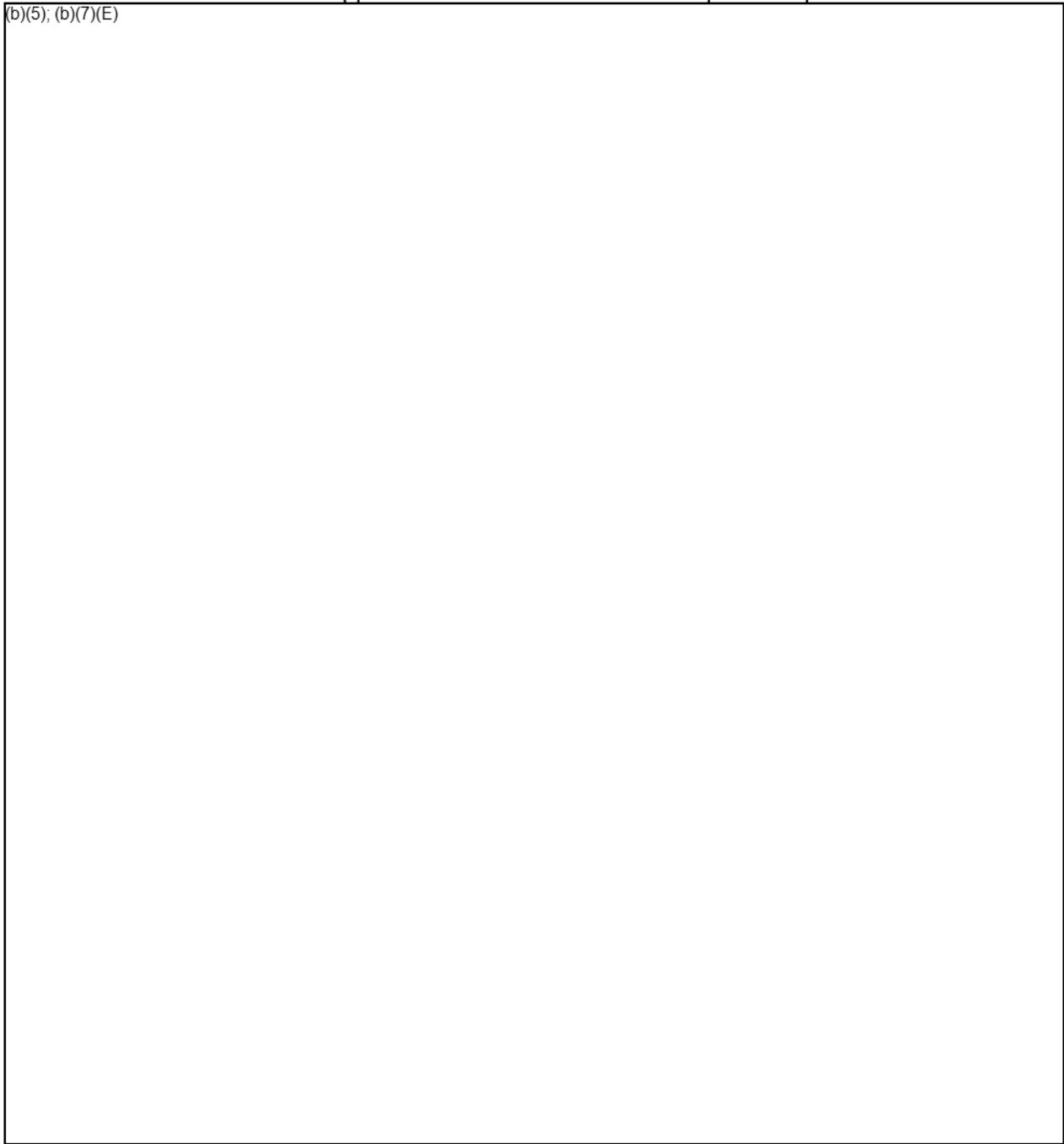


~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition

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



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

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)  
Technical Operations (Tech Ops)  
Phone number: 703 (b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

\_\_\_\_\_  
Date

Contracting Officer  
ICE/OAQ - MSD

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

**Reviewed by:**

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

OAQ-IOSD-DAD

\_\_\_\_\_  
Date

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

OAQ-IOSD-AD

\_\_\_\_\_  
Date

**Approved by:**

This justification is hereby approved:

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

**From:** (b)(6); (b)(7)(C)  
**Sent:** 21 Jul 2014 16:34:55 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Request for Legal review  
**Attachments:** Sole Source Harris Crossbow System 2014.doc, Sole Source Harris Procurement 21 July 2014.pdf, Sole Source Harris Crossbow System 2014(cald).doc

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

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, July 21, 2014 8:27 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Request for Legal review

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

Request legal review of the attached Sole Source for the supply of Crossbows from Harris Corporation.

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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905- (b)(6);  
Blackberry: 202-380- (b)(6);  
Email: (b)(6); (b)(7)(C)

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.~~

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

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

**2. Nature and/or Description of the Action Being Approved**

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

**3. Description of Supplies/Services**

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



Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

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

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

**8. Description of Market Research**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

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

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703-551-<sup>(b)(6);</sup><sub>(b)(7)(C)</sub>

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

\_\_\_\_\_  
Date

Contracting Officer

ICE/OAQ - MSD

~~FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

(b)(6); (b)(7)(C) \_\_\_\_\_  
OAQ-IOSD-DAD

\_\_\_\_\_  
Date

(b)(6); (b)(7)(C) \_\_\_\_\_  
OAQ-IOSD-AD

\_\_\_\_\_  
Date

**Approved by:**

This justification is hereby approved:

(b)(6); (b)(7)(C) \_\_\_\_\_  
Competition Advocate  
Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

# Document Routing Form



U.S. Immigration  
and Customs  
Enforcement

<b>1</b>	Date: July 18, 2014	Purpose: <input type="checkbox"/> Congressional <input type="checkbox"/> DHS <input type="checkbox"/> Routine <input type="checkbox"/> FYI	SharePoint Tracking No:
From:	(b)(7)(C); (b)(6)	Office: OAQ-IOSD	Telephone No: 214-910-2000 (b)(7)(C); Room No:
Subject Title: Request for Review of Justification Other than Full and Open Competition in support of Crossbow procurement for HSI Tech.Ops.			
Comments: Request review and signature for subject sole source documentation. Return to (b)(6); (b)(7)(C)			

2 Required Concurrences Before Routing to the Office of the Director						
Name	Extension	Office	Action Requested	Initial	Date	Comments
(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C)	IOSD	<input type="checkbox"/> Concur <input checked="" type="checkbox"/> Sign	(b)(6); (b)(7)(C)	18 July 14	
		IOSD	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign		18 July 14	
		IOSD	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign		7/21/14	
OPLA		OPLA	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
OAQ-AP		AP	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
(b)(6); (b)(7)(C)		RM	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
		DD	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
		HCA	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
		RM	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			

3 Office of the Director Concurrences: N/A Return to CO (b)(6); (b)(7)(C)							
Name	Action Requested	Initial	Date	Comments			
<b>ICE Management and Administration</b>							
(b)(6); (b)(7)(C)	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<b>ICE Director's Office</b>						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
Deputy Director Daniel Ragsdale	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
PDAS Thomas S. Winkowski	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						

## REQUEST FOR LEGAL REVIEW

<b>REQUEST DATE</b> July 18, 2014	<b>CONTRACT SPECIALIST</b> <div style="border: 1px solid black; padding: 2px; width: 100%;">(b)(6); (b)(7)(C)</div>	<b>TELEPHONE NO.</b> 214-905- <div style="border: 1px solid black; padding: 2px; width: 40px;">(b)(6); (b)(7)(C)</div>
<b>DIVISION/OFFICE</b>  OAQ-IOSD	<b>CONTRACTING OFFICER</b> <div style="border: 1px solid black; padding: 2px; width: 100%;">(b)(6); (b)(7)(C)</div>	<b>TELEPHONE NO.</b> 214-905- <div style="border: 1px solid black; padding: 2px; width: 40px;">(b)(6); (b)(7)(C)</div>
<b>ACQUISITION DOCUMENT NO.</b>  192114VHQ54T00079	<b>CONTRACTOR</b>  Will be Harris Corporation	
<b>CONTRACTING OFFICER'S COMMENTS</b>  Request legal review of JOFOC in support of purchase of <div style="border: 1px solid black; padding: 2px; width: 150px;">(b)(7)(E)</div> systems to refresh existing outdated equipment inventory	<b>ATTORNEY'S COMMENTS</b>  <input type="checkbox"/> Legally Sufficient <input type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below)  ATTORNEY: _____  DATE: _____	

Office of Acquisition Management (OAM)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

The Department of Homeland Security (DHS), United States (U.S.) Immigration and Customs Enforcement (ICE), proposes to enter into a contract on a basis other than full and open competition. The contracting activity is the Office of Acquisition Management, Investigation and Operations Support Dallas, TX.

**2. Nature and/or Description of the Action Being Approved**

(b)(7)(E)

**3. Description of Supplies/Services**

(b)(7)(E)



~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

(b)(7)(E)

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

(b)(7)(E)

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

(b)(7)(E)

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

(b)(7)(E)

**8. Description of Market Research**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

(b)(7)(E)

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

(b)(7)(E)

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

7-18-14  
Date

Immigration and Customs Enforcement (ICE)  
Technical Operations (Tech Ops)  
Phone number: 703-(b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER'S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

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

\_\_\_\_\_  
Date

Contracting Officer  
ICE/OAQ - MSD

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

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

OAQ-IOSD-DAD

18 July 14

Date

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

OAQ-IOSD-AD

7/21/14

Date

**Approved by:**

This justification is hereby approved:

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

\_\_\_\_\_  
Competition Advocate  
Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

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

**2. Nature and/or Description of the Action Being Approved**

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

**3. Description of Supplies/Services**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

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

[Redacted content for section 6]

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

[Redacted content for section 6]

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

[Redacted content for section 7]

**8. Description of Market Research**

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

[Redacted content for section 8]

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Source Selection Sensitive in accordance with FAR 3.104-4



~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

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

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703-  
(b)(7)(C); (b)(6)

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

\_\_\_\_\_  
Date

Contracting Officer  
ICE/OAQ - MSD

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

(b)(7)(C); (b)(6)  
\_\_\_\_\_  
OAQ-IOSD-DAD

\_\_\_\_\_  
Date

(b)(7)(C); (b)(6)  
\_\_\_\_\_  
OAQ-IOSD-AD

\_\_\_\_\_  
Date

**Approved by:**

This justification is hereby approved:

(b)(7)(C); (b)(6)  
\_\_\_\_\_  
Competition Advocate  
Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

**From:** (b)(6); (b)(7)(C)  
**Sent:** 3 Jun 2013 13:07:28 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Spectrum Amendment (2) to RFQ(CALD).doc  
**Attachments:** Spectrum Amendment (2) to RFQ(CALD).doc, Spectrum Amendment (2) to RFQ(CALD2).doc

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

Please see attached amendment (CALD2) wherein I proposed some minor edits for clarification. Please advise if you accept all proposed changes. If so, I have no objection to proceeding with the amendment.

Thanks,

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:**  
**Sent:** Thursday, May 30, 2013 2:25 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Spectrum Amendment (2) to RFQ(CALD).doc

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

(b)(6); (b)(7)(C) d I scrubbed it – for your review.

Thanks

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone:** 214-905 (b)(6); (b)(7)(C) **FAX:** 214-905-5568  
**Email:** (b)(6); (b)(7)(C)

**Your First Partner in Acquisition!**  
**Help us Support You Better: [How's My Service?](#)**

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, May 30, 2013 1:33 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Spectrum Amendment (2) to RFQ(CALD).doc

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

I made some initial comments on the PWS. Please take a look, and standardized the format of the positions and ensure that the desired experience is clearly communicated.

V/r

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 17 Sep 2012 18:24:35 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** MFR for not publicizing requirement  
**Attachments:** MFR - No Posting to Fedbizopps for Crossbow.doc  
**Importance:** High

Team:

By and large, the attached was taken from the last Stingray purchase as well. Please advise if there any objections to or changes that need to be made to the text.

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

**Mission Support - Dallas (MSD), OI East Team – Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6); (b)(7)(C)

Email: (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

Help us Support You Better: [How's My Service?](#)

**MEMO FOR RECORD**

**DATE: September 17, 2012**

**RE: Requisition 192112VSA00000079**

**SUBJECT: Restrictions on Publicizing Requirements for the Purchase of  
Crossbow OTA Tracking Equipment**

**I. BACKGROUND**

(b)(7)(E)

**II. REQUIREMENTS**

(b)(7)(E)

(b)(7)(E)

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

Contract Specialist

Date



**From:** (b)(6); (b)(7)(C)  
**Sent:** 11 Apr 2016 14:23:16 -0400  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** Over the Air (OTA) Sole Source Documentation  
**Attachments:** 2016\_04\_11\_14\_15\_00.pdf

Good Afternoon.

Please find final (signed) document attached.

Thank you,

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

**Executive Assistant | Management & Program Analyst**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 202-73 (b)(6); (b)(7)(C)  
Cell: (202) 430 (b)(6); (b)(7)(C)  
Email: (b)(6); (b)(7)(C)

# Document Routing Form



U.S. Immigration  
and Customs  
Enforcement

Date: March 29, 2016		Purpose: <input type="checkbox"/> Congressional <input type="checkbox"/> DHS <input checked="" type="checkbox"/> Routine <input type="checkbox"/> FYI		SharePoint Tracking No.	
From: (b)(7)(C); (b)(6)		Office: IOSD		Telephone No. 214 905 (b)(7)(C); (b)(6)	
Subject Title: (b)(5)		Room No.			
Comments:			Additional Requirements		

Required Concurrences Before Routing to the Office of the Director							
Name	Extension	Office	Action Requested	Initial	Date	Comments	
(b)(7)(C); (b)(6)		OAQ/IOSD	<input type="checkbox"/> Concur <input checked="" type="checkbox"/> Sign	(b)(7)(C); (b)(6)			
		OAQ/IOSD	<input type="checkbox"/> Concur <input checked="" type="checkbox"/> Sign		April 2016		
		OAQ/IOSD	<input type="checkbox"/> Concur <input checked="" type="checkbox"/> Sign			4/4/16	
		OPLA/IOSD	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign			4/4/2016	See email
		OPQ/APO	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign			4/6/2016	
		OAQ-CoS	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign			4/7/16	
		OAQ-(A)DD	<input type="checkbox"/> Concur <input checked="" type="checkbox"/> Sign			4/8/16	

Office of the Director Concurrences						
ICE Director's Office						
(b)(6); (b)(7)(C)		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
Deputy Director Daniel Ragsdale		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				
Director Sarah R. Saldaña		<input type="checkbox"/> Concur <input type="checkbox"/> Sign				

**Department of Homeland Security (DHS)  
Immigration & Customs Enforcement (ICE)  
Office of Acquisition Management (OAM)  
Investigations and Operations Support Dallas**

**Justification and Approval for other than Full and Open Competition**

(b)(7)(E)

**1. Agency and Contracting Activity**

The Department of Homeland Security (DHS), United States (U.S.) Immigration and Customs Enforcement (ICE), Office of Acquisition Management (OAM), Investigations and Operations Support Dallas (IOSD) propose to enter into a contract on a basis other than full and open competition.

**2. Nature and/or Description of the Action Being Approved**

(b)(4); (b)(7)(E)

**3. Description of Supplies/Services**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

(b)(7)(E)

Equipment to be purchased:

Part Number	Description	Qty	Unit Price	Total
(b)(4); (b)(7)(E)				
			Total	\$2,220,200.00

Requisition: 192116VHQ54T00046  
Delivery: 120 days ARO

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

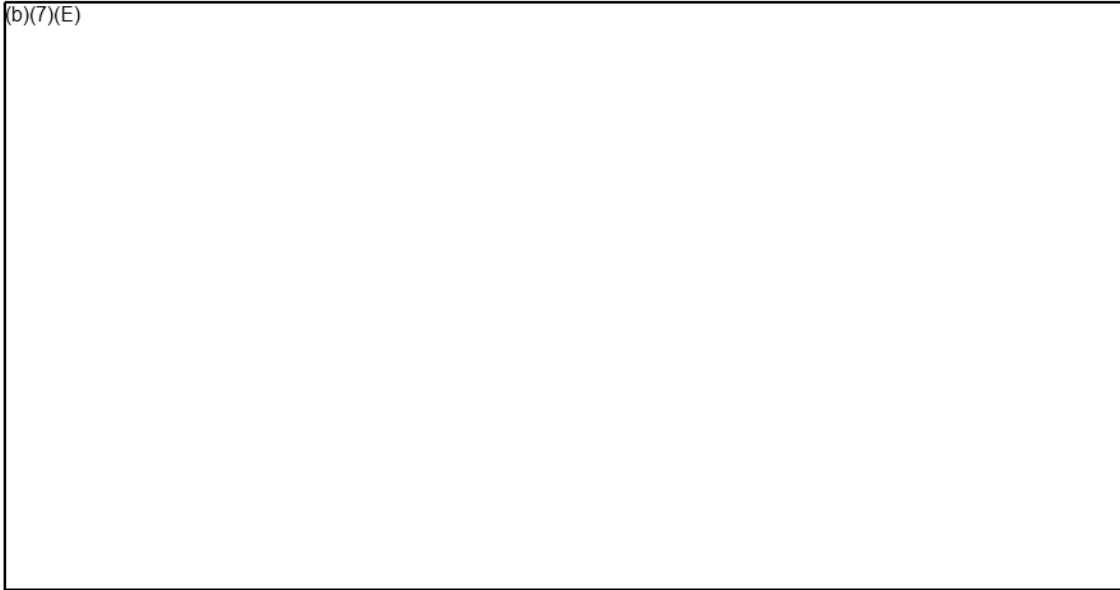
(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

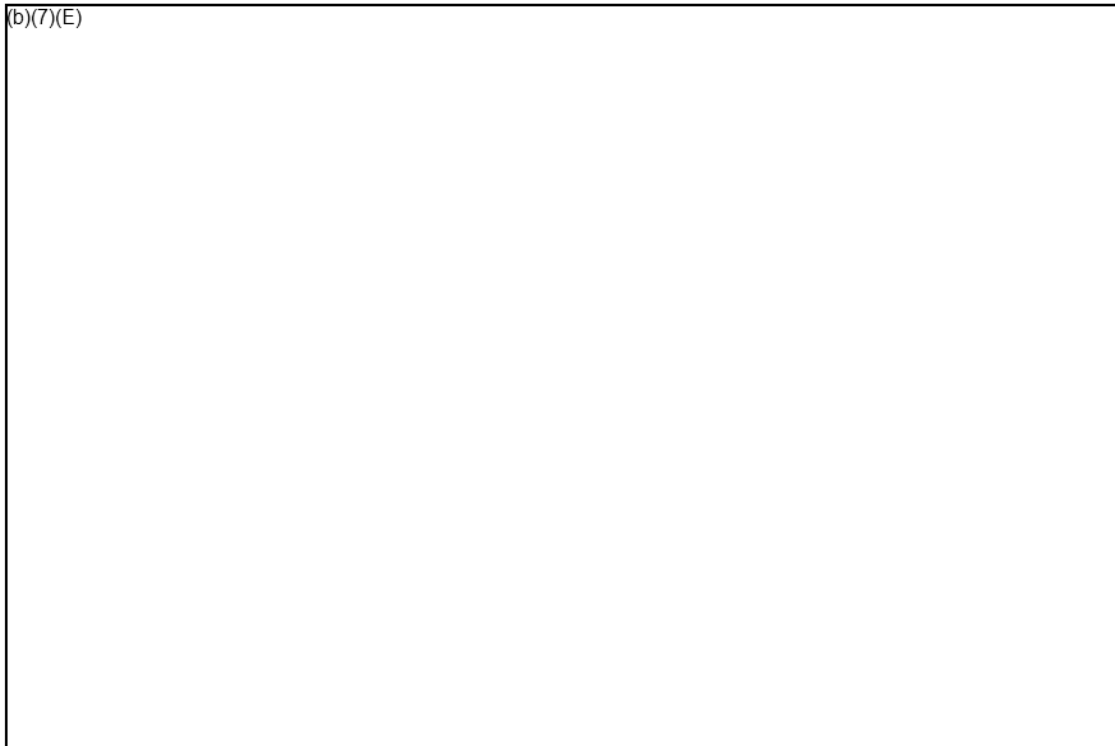
**5. Demonstration that the Nature of the Acquisition Require Use of the Authority Cited**

(b)(7)(E)



**6. Description of Efforts to Ensure that Offers are Solicited from as Many Potential Sources as is Practicable**

(b)(7)(E)



Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

(b)(7)(E)

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

(b)(7)(E)

**8. Description of Market Research**

(b)(7)(E)

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

(b)(7)(E)

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

(b)(7)(E)

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

(b)(7)(E)

Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

4-4-16  
Date

Immigration and Customs Enforcement (ICE)  
Technical Operations (Tech Ops)  
Phone number: 703-55 (b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER'S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

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

Date

Contracting Officer  
ICE/OAQ - MSD



Justification and Approval for Other than Full and Open Competition  
OTA Equipment Upgrade for Tech Ops

Reviewed by:

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

[Redacted signature box]

OAQ-IOSD-DAD

4 April 2016

Date

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

[Redacted signature box]

OAQ-IOSD-AD

4/4/16

Date

Approved by:

This justification is hereby approved:

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

[Redacted signature box]

Competition Advocate  
Office of Acquisition Management (OAQ)

8 APRIL 2016

Date

**From:** (b)(6); (b)(7)(C)  
**Sent:** 6 Jan 2015 09:28:52 -0500  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Harris Stingray Article

(b)(7)(E)

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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6); (b)(7)(C)  
Blackberry: 202-380-(b)(6); (b)(7)(C)  
Email: (b)(6); (b)(7)(C)

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.~~

**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

(b)(7)(E)

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

Investigations & Operations Support Dallas | Section Chief

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-

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

Blackberry: 202-380-

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

Email

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

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.~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Jul 2014 16:31:57 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Harris update

I just spoke to (b)(6); (b)(7)(C) at Harris. They just went through this with (b)(5); (b)(7)(E) (b)(5); (b)(7)(E). Yes this is a developmental item based on their GSA publicized pricing for some components, and they will follow up in writing with a response to my e:mail tomorrow. They were ready for it.

I will change my J&A and send it back to you (b)(6); (b)(7)(C) momentarily.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6); (b)(7)(C)

Email: (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jun 2013 15:50:08 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** HSCEMD-13-J-00015 Spectrum Support Services  
**Attachments:** 2013\_06\_13\_10\_48\_38.pdf

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

Please find attached my comments concerning the award document.

V/r  
(b)(6); (b)(7)(C)

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

## REQUEST FOR LEGAL REVIEW

<b>REQUEST DATE</b> June 11, 2013	<b>CONTRACT SPECIALIST</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214-90 (b)(6); (b)(7)(C)
<b>DIVISION/OFFICE</b> OAA / MSD	<b>CONTRACTING OFFICER</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214 (b)(6); (b)(7)(C)
<b>ACQUISITION DOCUMENT NO.</b> HSCEMD-13-J-00015 - <i>Order Review</i>	<b>CONTRACTOR</b> Zantech IT Services, Inc.	
<b>CONTRACTING OFFICER'S COMMENTS</b> Request Pre-Award legal review	<b>ATTORNEY'S COMMENTS</b> <input type="checkbox"/> Legally Sufficient <input checked="" type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below) (b)(6); (b)(7)(C) ATTORNEY: _____ DATE: <u>          9/13/2013          </u>  1) <i>Add: 5202178 Option to extended services.</i>  2) <i>Reference HSA 3052.215-70 key Personnel, pursuant to (b) identify the "Special individuals" by Name, not just position.</i>  3) <i>Indicate that 52.212-4 AFI applies to this Task Order.</i>	

**From:** (b)(6); (b)(7)(C)  
**Sent:** 21 Jan 2020 14:23:20 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** HSCEMD14Q00028 Harris Crossbow

HSCEMD14Q00028 Harris Crossbow

(b)(7)(E)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 15 May 2018 19:45:31 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** J&A Legal Review 192118VHQ6TSPC008.1

Doug,

Can you please provide a legal review on this one?

FILE NAME	ACTION	LINK
<b>File Link</b>	No Action – For Reference Only -ALL documents are in draft form	(b)(6); (b)(7)(C)
<b>Routing Sheet</b>	Sign	
<b>Legal Review</b>	Sign / Comments	
<b>J&amp;A</b>	Review	

Thank you

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone: 214-905-**(b)(6); (b)(7)(C) **FAX: 214-905-5568**

**Email:** (b)(6); (b)(7)(C)

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



**From:** (b)(6); (b)(7)(C)  
**Sent:** 20 Aug 2014 10:51:42 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Just heard from Harris Corporation

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

I just had a telephone call from Harris Corp. They are trying to identify alternate language that would potentially be agreeable. My POC, (b)(6); (b)(7)(C) let slip that what they are worried about is a DCAA audit if they certify something under the commercial item provisions. They said that they cannot get on a phone call with you until they get their corporate legal position lined up.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6); (b)(7)(C)

**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 31 May 2018 12:00:07 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Lie

Good morning (b)(6); (b)(7)(C)

Unintentionally, I lie to you yesterday! Sorry - I do have a pre-award review for 4.8M coming to you for review later today.  
You already reviewed the J&A for this one.

(I didn't think it need it because it's not over 5M, but awards over \$700K do need OPLA review)

Thanks

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone: 214-905-(b)(6); (b)(7)(C) FAX: 214-905-5568**  
**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Aug 2014 20:03:46 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Question on the Harris Procurement

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

I don't understand their issue, nor do I believe that there is any flexibility to avoid certification through SAM and 52.212.3. Those certifications work in conjunction with one other.

V/r  
(b)(6); (b)(7)(C)

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 19, 2014 2:59 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Question on the Harris Procurement  
**Importance:** High

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

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

BTW, I will have the NUIX revised, revised, revised, (sigh) JOFOC for you shortly.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6); (b)(7)(C)

Email: (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Aug 2014 16:32:59 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Question on the Harris Procurement

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

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6);  
**Email:** (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 19, 2014 3:04 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Question on the Harris Procurement

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

I don't understand their issue, nor do I believe that there is any flexibility to avoid certification through SAM and 52.212.3. Those certifications work in conjunction with one other.

V/r,

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.904-(b)(6);  
(bb) 214.92-(b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 19, 2014 2:59 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Question on the Harris Procurement  
**Importance:** High

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

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

BTW, I will have the NUIX revised, revised, revised, (sigh) JOFOC for you shortly.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6)

**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Jul 2014 15:09:47 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Request for Legal review

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

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

Thanks,

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

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

~~**From:** (b)(6); (b)(7)(C)~~

~~**Sent:** Tuesday, July 22, 2014 9:58 AM~~

~~**To:** (b)(6); (b)(7)(C)~~

~~**Cc:**~~

~~**Subject:** RE: Request for Legal review~~

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

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

Meanwhile, I will visit with the program relative to your comments. Thank you for the quick turnaround.

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

Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6);

Email: (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, July 21, 2014 11:35 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** FW: Request for Legal review

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

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

Thanks,

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

Associate Legal Advisor

ICE Office of the Principal Legal Advisor

(p) 214.905-(b)(6);

(bb) 214.92-(b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, July 21, 2014 8:27 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** Request for Legal review

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

Request legal review of the attached Sole Source for the supply of Crossbows from Harris Corporation.



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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-<sup>(b)(6);</sup>

Blackberry: 202-380-<sup>(b)(6);</sup>

Email: <sup>(b)(6); (b)(7)(C)</sup>

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.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 17 Sep 2012 17:36:39 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Porposed LSJ for purchase of a Crossbow System from Harris Corporation  
**Attachments:** Sole Source Harris Crossbow System.doc  
**Importance:** High

Gentlemen:

I you would please review the attached draft document and provide your comments, I would appreciate it. If this looks very similar to the final LSJ from the Stingray II system purchase from last year, there is a good reason for that. The Crossbow System is the latest, most technologically up-to-date version of a Stingray system.

I am trying to make award by this coming Friday, so I need your input quickly please. Many thanks.

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

**Mission Support - Dallas (MSD), OI East Team – Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6);

Email: (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

Help us Support You Better: [How's My Service?](#)

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

(b)(5); WIF Draft

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

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

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**8. Description of Market Research**

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

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

(b)(5)

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703-55

(b)(5)

**13. CONTRACTING OFFICER'S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

(b)(5)

\_\_\_\_\_  
Date

Contracting Officer  
ICE/OAQ - MSD

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

(b)(5) \_\_\_\_\_

OAQ-MD-AD

\_\_\_\_\_  
Date

(b)(5) \_\_\_\_\_

OPLA

\_\_\_\_\_  
Date



**From:** (b)(6); (b)(7)(C)  
**Sent:** 21 Sep 2012 14:42:20 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Question on FOIA release of info

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

I just got a call from (b)(6); (b)(7)(C) over at C3. It seems that someone came in with a FOIA request for info about Stingray purchases, and the ICE FOIA office released copies of contracts with Harris Corporation, sole source justifications and I don't know how much other info. (b)(6); (b)(7)(C) was furious because there was very sensitive information in there about which offices were receiving the technology, what it would be used for, and even the names of some of the individual agents that would be using it. From what (b)(6); (b)(7)(C) told me, the request was not sent to the HSI FOIA office (b)(6); (b)(7)(C) crew) until after the documents were already released by the main ICE FOIA office (b)(6); (b)(7)(C) did not know for sure, but he did not think any of my documents were released (since I have headers and footers all over them that identify the info as law enforcement sensitive), but I am not the only person who buys this equipment.

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

(b)(6); (b)(7)(C) is talking about doing a telecon sometime next month to discuss this topic. Will keep you posted.

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

**Mission Support - Dallas (MSD), OI East Team – Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905 (b)(6); (b)(7)(C)  
Email: (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

Help us Support You Better: [How's My Service?](#)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Aug 2014 15:58:54 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Question on the Harris Procurement  
**Importance:** High

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

(b)(5)

(b)(5) Do you have any objection? Let me know by e:mail, and I can do a quick amendment. Thx.

BTW, I will have the NUIX revised, revised, revised, (sigh) JOFOC for you shortly.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6);  
**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 21 Jul 2014 09:26:31 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Request for Legal review  
**Attachments:** Sole Source Harris Crossbow System 2014.doc, Sole Source Harris Procurement 21 July 2014.pdf

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

Request legal review of the attached Sole Source for the supply of Crossbows from Harris Corporation.

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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6);  
Blackberry: 202-380-(b)(6);  
Email: (b)(6); (b)(7)(C)

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.~~

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

The Department of Homeland Security (DHS), United States (U.S.) Immigration and Customs Enforcement (ICE), proposes to enter into a contract on a basis other than full and open competition. The contracting activity is the Office of Acquisition Management, Investigation and Operations Support Dallas, TX.

**2. Nature and/or Description of the Action Being Approved**

(b)(7)(E)

**3. Description of Supplies/Services**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

(b)(7)(E)

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

(b)(7)(E)

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

(b)(7)(E)

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

(b)(7)(E)

**8. Description of Market Research**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

(b)(7)(E)

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

(b)(7)(E)

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

(b)(7)(E)

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703-(b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER'S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

\_\_\_\_\_  
Date

Contracting Officer  
ICE/OAQ - MSD



~~FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
OAQ-IOSD-DAD

\_\_\_\_\_  
Date

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
OAQ-IOSD-AD

\_\_\_\_\_  
Date

**Approved by:**

This justification is hereby approved:

\_\_\_\_\_  
(b)(6); (b)(7)(C)  
Competition Advocate  
Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

# Document Routing Form



U.S. Immigration  
and Customs  
Enforcement

<b>1</b>	Date: July 18, 2014	Purpose: <input type="checkbox"/> Congressional <input type="checkbox"/> DHS <input type="checkbox"/> Routine <input type="checkbox"/> FYI	SharePoint Tracking No:
From: (b)(6); (b)(7)(C)	Office: OAQ-IOSD	Telephone No: 214 (b)(6);	Room No:
Subject Title: Request for Review of Justification Other than Full and Open Competition in support of Crossbow procurement for HSI Tech.Ops.			
Comments: Request review and signature for subject sole source documentation. Return to (b)(6); (b)(7)(C)			

2 Required Concurrences Before Routing to the Office of the Director						
Name	Extension	Office	Action Requested	Initial	Date	Comments
(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C)	IOSD	<input type="checkbox"/> Concur <input checked="" type="checkbox"/> Sign	(b)(6); (b)(7)(C)	18 July 14	
		IOSD	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign		18 July 14	
		IOSD	<input checked="" type="checkbox"/> Concur <input type="checkbox"/> Sign		7/21/14	
OPLA		OPLA	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
OAQ-AP		AP	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
(b)(6); (b)(7)(C)		RM	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
		DD	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
		HCA	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			
		RM	<input type="checkbox"/> Concur <input type="checkbox"/> Sign			

3 Office of the Director Concurrences: N/A Return to CO (b)(6); (b)(7)(C)							
Name	Action Requested	Initial	Date	Comments			
<b>ICE Management and Administration</b>							
(b)(6); (b)(7)(C)	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<b>ICE Director's Office</b>						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
Deputy Director Daniel Ragsdale	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						
PDAS Thomas S. Winkowski	<input type="checkbox"/> Concur <input type="checkbox"/> Sign						

## REQUEST FOR LEGAL REVIEW

<b>REQUEST DATE</b> July 18, 2014	<b>CONTRACT SPECIALIST</b> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">(b)(6); (b)(7)(C)</div>	<b>TELEPHONE NO.</b> 214- <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">(b)(6); (b)(7)(C)</div>
<b>DIVISION/OFFICE</b>  OAQ-IOSD	<b>CONTRACTING OFFICER</b> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">(b)(6); (b)(7)(C)</div>	<b>TELEPHONE NO.</b> 214- <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">(b)(6); (b)(7)(C)</div>
<b>ACQUISITION DOCUMENT NO.</b>  192114VHQ54T00079	<b>CONTRACTOR</b>  Will be Harris Corporation	
<b>CONTRACTING OFFICER'S COMMENTS</b>  Request legal review of JOFOC in support of purchase of <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">(b)(7)(E)</div> Harris Crossbow systems to refresh existing outdated equipment inventory	<b>ATTORNEY'S COMMENTS</b>  <input type="checkbox"/> Legally Sufficient <input type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below)  ATTORNEY: _____  DATE: _____	

Office of Acquisition Management (OAM)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

The Department of Homeland Security (DHS), United States (U.S.) Immigration and Customs Enforcement (ICE), proposes to enter into a contract on a basis other than full and open competition. The contracting activity is the Office of Acquisition Management, Investigation and Operations Support Dallas, TX.

**2. Nature and/or Description of the Action Being Approved**

(b)(7)(E)

**3. Description of Supplies/Services**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

(b)(7)(E)

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

(b)(7)(E)

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

(b)(7)(E)

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

(b)(7)(E)

**8. Description of Market Research**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

(b)(7)(E)

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

(b)(7)(E)

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

(b)(7)(E)

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~  
Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

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

7-18-14  
Date

Immigration and Customs Enforcement (ICE)  
Technical Operations (Tech Ops)  
Phone number: 703-(b)(6); (b)(7)(C)

**13. CONTRACTING OFFICER'S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

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

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

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

Date

Contracting Officer  
ICE/OAQ - MSD



Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

(b)(6); (b)(7)(C)  
[Redacted Signature Box]

18 July 14  
Date

OAQ-IOSD-DAD

(b)(6); (b)(7)(C)  
[Redacted Signature Box]

7/21/14  
Date

OAQ-IOSD-AD

**Approved by:**

This justification is hereby approved:

(b)(6); (b)(7)(C) \_\_\_\_\_  
Competition Advocate  
Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

**From:** (b)(6); (b)(7)(C)  
**Sent:** 31 May 2018 15:28:29 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Review 70CMSD18P00000076

Sir,

For Award Review:

FILE NAME	ACTION	LINK
<b>File Link</b>	No Action – For Reference Only	(b)(7)(E)
<b>Award</b>	Review	
<b>Legal Review</b>	Sign	
<b>Award Summary</b>	Review	
<b>Routing Sheet</b>	Sign	

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**  
 DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone:** 214-905-(b)(6); **FAX:** 214-905-5568  
**Email:** (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Thursday, May 31, 2018 7:00 AM

**To:** (b)(6); (b)(7)(C)  
**Subject:** Lie

Good morning (b)(6); (b)(7)(C)

Unintentionally, I lie to you yesterday! Sorry - I do have a pre-award review for 4.8M coming to you for review later today.  
You already reviewed the J&A for this one.

(I didn't think it need it because it's not over 5M, but awards over \$700K do need OPLA review)

Thanks

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone: 214-905-(b)(6); FAX: 214-905-5568**  
**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jun 2013 15:12:17 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Award summary review (cald1).doc - HSCEMD-13-J-00015  
**Attachments:** Award summary review (response).doc, Award Summary after Amendment 2.docx

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

Here's the revised award summary and legal review form.

Thank you sir

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone: 214-905-(b)(6); FAX: 214-905-5568**

**Email:** (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***

**Help us Support You Better: [How's My Service?](#)**

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, June 13, 2013 10:32 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Award summary review (cald1).doc - HSCEMD-13-J-00015

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

Please see my comments concerning the award summary attached.

Please coordinate your revisions with me.

Thanks,

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

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

Associate Legal Advisor

ICE Office of the Principal Legal Advisor

(p) 214.905.(b)(6);

(bb) 214.924.(b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any~~

~~disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

## REQUEST FOR LEGAL REVIEW

HSCEMD-13-J-00015 (HSI/Technical Operations Spectrum Support Services)

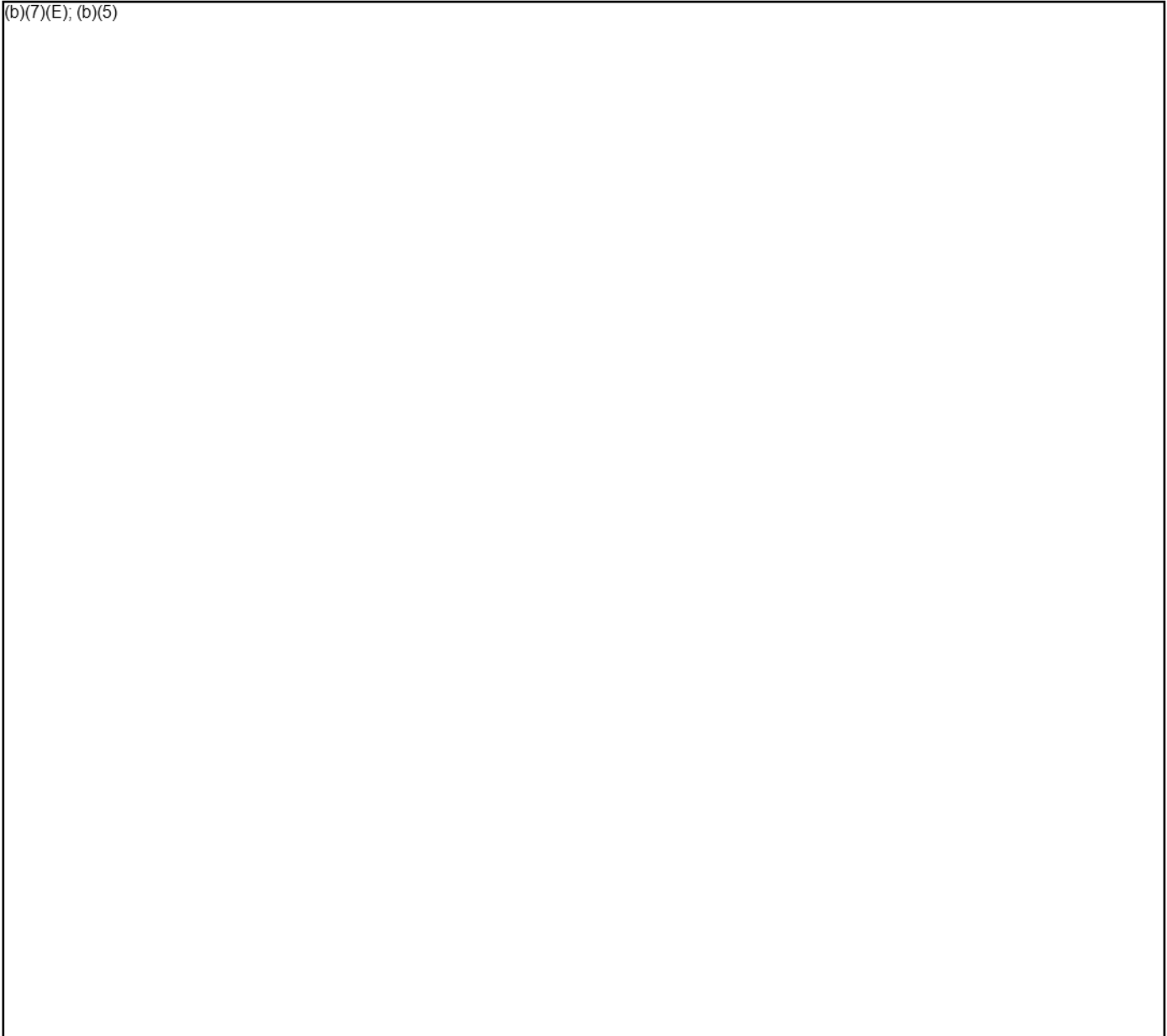
REQUEST DATE	DIVISION/OFFICE	CONTRACT SPECIALIST	TELEPHONE NO.
AQ DOC NO.	CONTRACTOR	CONTRACTING OFFICER	TELEPHONE NO.
CONTRACTING OFFICER'S COMMENTS		ATTORNEY'S COMMENTS	<div style="border: 1px solid black; display: inline-block; padding: 2px;">(b)(6); (b)(7)(C)</div> <div style="border: 1px solid black; display: inline-block; padding: 2px;">214-90</div> <div style="border: 1px solid black; display: inline-block; padding: 2px;">(b)(6); (b)(7)(C)</div>

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

**\*\*\*Warning\*\*\* Attorney/Client Privilege\*\*\* Attorney Work Product\*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(5), (b)(7).~~

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




**\*\*\*Warning\*\*\* Attorney/Client Privilege\*\*\* Attorney Work Product\*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 4 Apr 2016 14:50:46 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Final JOFOC for Harris Equipment Upgrade

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

I have no legal objection to the proposed LSJ. I will sign the routing sheet for you when I return from DC later this week.

V/r,

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

V/r,

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(O) 214-904 (b)(6);  
(C) 214-924 (b)(7)(C)

~~\*\*\*Warning\*\*\*Attorney Client Privilege\*\*\*Attorney Work Product~~

~~This communication and any attachments may contain confidential or sensitive attorney/client privileged information or attorney work product or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore, do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC 552(b)(5) and (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, April 01, 2016 3:06:21 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Final JOFOC for Harris Equipment Upgrade

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



I have corrected/implemented all comments that you had (see attached), and am in the process of obtaining a new signature page signed by (b)(6); (b)(7)(C). Please provide your signed legal sufficiency documentation, and doc routing signature cover page to me. Thank you for your review.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-904-(b)(6);

**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Jul 2014 16:33:18 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Harris update

That's ok. I can take it. ☺

It makes the solicitation a lot easier and faster to create though!

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-900-(b)(6);

**Email:** (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, July 22, 2014 3:32 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Harris update

Hate to say it...

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

Associate Legal Advisor

ICE Office of the Principal Legal Advisor

(p) 214.905

(bb) 214.92

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5); (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, July 22, 2014 3:32 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Harris update

I just spoke to (b)(6); (b)(7)(C) at Harris. They just went through this with (b)(5); (b)(7)(E)  
(b)(5); (b)(7)(E) Yes this is a developmental item based on their GSA publicized pricing for some components, and they will follow up in writing with a response to my e:mail tomorrow. They were ready for it.

I will change my J&A and send it back to you (b)(6); (b)(7)(C) momentarily.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-(b)(6);

Email: (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jun 2013 15:56:19 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: HSCEMD-13-J-00015 Spectrum Support Services  
**Attachments:** Contract Document Legal Review Corrections.pdf

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

Attached are the corrected pages (29 and 30) of the award document and comments in response to your legal review.

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

**OAQ Mission Support Dallas | Contract Specialist**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Desk:** 214.905.(b)(6); Fax: 214.905.5568  
**Email:** (b)(6); (b)(7)(C)

### Your First Partner in Acquisition!

Help us Support You Better: [How's My Service?](#)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, June 13, 2013 10:50 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** HSCEMD-13-J-00015 Spectrum Support Services

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

Please find attached my comments concerning the award document.

V/r

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905.(b)(6);  
(bb) 214.924.(b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

### REQUEST FOR LEGAL REVIEW

<b>REQUEST DATE</b> June 11, 2013	<b>CONTRACT SPECIALIST</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214 (b)(6); (b)(7)(C)
<b>DIVISION/OFFICE</b> OAQ / MSD	<b>CONTRACTING OFFICER</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214 (b)(6); (b)(7)(C)
<b>ACQUISITION DOCUMENT NO.</b> HSCEMD-13-J-00015 - <i>Order Review</i>	<b>CONTRACTOR</b> Zantech IT Services, Inc.	
<b>CONTRACTING OFFICER'S COMMENTS</b> Request Pre-Award legal review  1) Added 52.217-8  2) Key personnel names added to HSAR 3052.215-70  3) added 52.212-4 AHTI. Also, this clause is included in the contractor's TABBs Contract.	<b>ATTORNEY'S COMMENTS</b> <input type="checkbox"/> Legally Sufficient <input checked="" type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below)  ATTORNEY: (b)(6); (b)(7)(C) DATE: <u>6/13/2013</u>  1) Add: 52.217-8 OPRN to extended services.  2) Reference HSAR 3052.215-70 key personnel, pursuant to (b) identify the "Special individuals" by Name, not just position.  3) Indicate that 52.212-4 AHTI applies to this Task Order.	

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

## **16.0 OTHER DELIVERY ORDER TERMS**

### **16.1. INCORPORATED CLAUSES:**

FAR and HSAR provisions and clauses can be accessed at <http://farsite.hill.af.mil/>

#### **52.212-4 Contract Terms and Conditions—Commercial Items (JUNE 2010) with Alternate I (OCT 2008)**

#### **52.213-3 -- Notice to Supplier (Apr 1984)**

#### **52.217-8 -- Option to Extend Services (Nov 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to task order expiration.

**FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000):** (a) The Government may extend the term of this contract by written notice to the Contractor prior to expiration; provided, that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days prior to the contract expiration date. The preliminary notice does not commit the Government to an extension. (b) If the Government exercises this option, the extended contract shall be considered to include this option clause. (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 36 months.  
(End of Clause)

#### **HSAR 3052.205-70 Advertisements, Publicizing Awards, and Releases (SEP 2012).**

The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.  
(End of clause)

### **ALTERNATE I (SEP 2012)**

If a contract involves sensitive or classified information, designate the paragraph in the base clause as (a) and add the following paragraph (b) to the clause:

(b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the

Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.  
(End of clause)

**HSAR 3052.215-70 Key Personnel (DEC 2003)**

(a) The personnel specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel, as appropriate.

(b) Before removing or replacing any of the specified individuals, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel until the Contracting Officer approves the change.

Key Personnel under this task order:

The Project Manager: Ken Atkinson

The Senior Computer Systems Specialist / Network Engineer: Behrouz Kohan

The Senior Engineer Subject Matter Expert (SME): Dave Kanterman

(End of clause)

**3052.242-72 Contracting officer's technical representative. (DEC 2003)**

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

(b) The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

(End of clause)

**PER ALL TABBS CONTRACTS:**

**H-8 Advertisements, Publicizing Awards, and News Releases**

All press releases or announcements about any contract/task order award hereunder shall be approved by the contract/task order contracting officer prior to release. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the contract/task order contracting officer. The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 16 May 2018 16:26:06 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: J&A Legal Review 192118VHQ6TSPC008.1  
**Attachments:** 192118VHQ6TSPC008 OTA Sole Source.doc

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

I saved the other documents to the file. See comments attached. No objection provided you address my comment.

Thanks.

V/r,

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

Associate Legal Advisor  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
Department of Homeland Security  
Desk: (214) 905 (b)(6);  
Email: (b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, May 15, 2018 2:46 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** J&A Legal Review 192118VHQ6TSPC008.1

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

Can you please provide a legal review on this one?

FILE NAME	ACTION	LINK
-----------	--------	------



<b>File Link</b>	No Action – For Reference Only -ALL documents are in draft form	(b)(7)(E)
<b>Routing Sheet</b>	Sign	
<b>Legal Review</b>	Sign / Comments	
<b>J&amp;A</b>	Review	

Thank you

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone: 214-905-**(b)(6); (b)(7) **FAX: 214-905-5568**

**Email:** (b)(6); (b)(7)(C)

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

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

**1. Agency and Contracting Activity**

The Department of Homeland Security (DHS), United States (U.S.) Immigration and Customs Enforcement (ICE), proposes to enter into a contract on a basis other than full and open competition. The contracting activity is the Office of Acquisition Management, Investigation and Operations Support Dallas, TX.

**2. Nature and/or Description of the Action Being Approved**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

**6. Efforts to Obtain Competition**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

**8. Description of Market Research**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

(b)(5)

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703-551 (b)(5)

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

(b)(5)

\_\_\_\_\_  
Date

Contracting Officer

**From:** (b)(6); (b)(7)(C)  
**Sent:** 16 May 2018 16:34:16 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: J&A Legal Review 192118VHQ6TSPC008.1

Thank you (b)(6); (b)(7)(C)

I will include the part numbers in the document.

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone:** 214-905-(b)(6); (b)(7)(C) **AX:** 214-905-5568  
**Email:** (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, May 16, 2018 11:26 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: J&A Legal Review 192118VHQ6TSPC008.1

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

I saved the other documents to the file. See comments attached. No objection provided you address my comment.

Thanks.

V/r  
(b)(6); (b)(7)(C)

Associate Legal Advisor  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
Department of Homeland Security  
Desk: (214) 905-(b)(6);  
Email (b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal~~

~~Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, May 15, 2018 2:46 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** J&A Legal Review 192118VHQ6TSPC008.1

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

Can you please provide a legal review on this one?

FILE NAME	ACTION	LINK
<b>File Link</b>	No Action – For Reference Only -ALL documents are in draft form	(b)(7)(E)
<b>Routing Sheet</b>	Sign	
<b>Legal Review</b>	Sign / Comments	
<b>J&amp;A</b>	Review	

Thank you

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone:** 214-905-5144 **FAX:** 214-905-5568  
**Email:** (b)(6); (b)(7)(C)



**From:** (b)(6); (b)(7)(C)  
**Sent:** 14 Jun 2013 10:20:35 -0400  
**To:** (b)(6); (b)(7)(C)

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

**Subject:** RE: Pre-Award CRB for SPECTRUM

Good morning everyone,

Here's the link to the SPECTRUM CRB

(b)(7)(E)

Thank you

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone:** 214-905-(b)(6); (b)(7)(C) **FAX:** 214-905-5568

**Email:** (b)(6); (b)(7)(C)

*Your First Partner in Acquisition!*

**Help us Support You Better:** [How's My Service?](#)

-----Original Appointment-----

**From:** (b)(6); (b)(7)(C)

**Sent:** Thursday, June 13, 2013 3:42 PM

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

**Subject:** Pre-Award CRB for SPECTRUM

**When:** Wednesday, June 19, 2013 12:00 PM-1:00 PM (UTC-06:00) Central Time (US & Canada).

**Where:** Conference Call

CRB schedule for Pre-award of the SPECTRUM Support Services.

Teleconference and videoconference numbers will be provided upon confirmation.

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone:** 214-905-(b)(6) **FAX:** 214-905-5568

**Email:** (b)(6); (b)(7)(C)

*Your First Partner in Acquisition!*

**Help us Support You Better:** [How's My Service?](#)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 21 Sep 2012 19:33:10 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Question on FOIA release of info

So were the documents released or not?

Check the DHS and ICE management directives, but I believe you may be able to mark them with a FOUO marking. I'll check into that when I have a chance.

V/r

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor

(p) 214.905 (b)(6);  
(b) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 21, 2012 1:42 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Question on FOIA release of info

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

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

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

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

is talking about doing a telecon sometime next month to discuss this topic. Will keep you posted.

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

**Mission Support - Dallas (MSD), OI East Team – Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-5[redacted]

Email: [redacted]

***Your First Partner in Acquisition!***

Help us Support You Better: [How's My Service?](#)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Jul 2014 16:47:06 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Updated sole source for Harris  
**Attachments:** Sole Source Harris Crossbow System 2014 - rev inc Comm Item info.doc

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

Please see attached, and advise if there are any other changes you would recommend.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905 (b)(6);

**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 23 Jul 2014 12:31:39 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** [procurement-J&A] FW: Updated sole source for Harris Corporation  
**Attachments:** Sole Source Harris Crossbow System 2014 - rev inc Comm Item info.doc, Sole Source Harris Crossbow System 2014 - rev inc Comm Item info(cald).doc

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

I have no objections provided you incorporate my proposed edits (see track-changes) prior to executing the J&A.

V/r,

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, July 22, 2014 3:47 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Updated sole source for Harris

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

Please see attached, and advise if there are any other changes you would recommend.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905 (b)(6);  
**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 31 May 2018 19:01:56 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Review 70CMSD18P00000076  
**Attachments:** Request for Legal Review - Award - OTA(calds).doc, Routing Sheet Award - OTA(calds).doc

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

No objections.

Thanks.

V/r,

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

Associate Legal Advisor  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
Department of Homeland Security  
Desk: (714) 905- (b)(6);  
Email: (b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, May 31, 2018 10:28 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Review 70CMSD18P00000076

Sir,

For Award Review:

FILE NAME	ACTION	LINK
<b>File Link</b>	No Action – For Reference Only	(b)(7)(E)

		(b)(7)(E)
<b>Award</b>	Review	
<b>Legal Review</b>	Sign	
<b>Award Summary</b>	Review	
<b>Routing Sheet</b>	Sign	

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone: 214-905-(b)(6); AX: 214-905-5568**

**Email:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)

**Sent:** Thursday, May 31, 2018 7:00 AM

**To:** (b)(6); (b)(7)(C)

**Subject:** Lie

Good morning (b)(6); (b)(7)(C)

Unintentionally, I lie to you yesterday! Sorry - I do have a pre-award review for 4.8M coming to you for review later today.

You already reviewed the J&A for this one.

(I didn't think it need it because it's not over 5M, but awards over \$700K do need OPLA review)

Thanks

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

**Investigations & Operations Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone: 214-90** (b)(6); (b)(7)(C) **FAX: 214-905-5568**

**Email:** (b)(6); (b)(7)(C)



## REQUEST FOR LEGAL REVIEW

<b>REQUEST DATE</b> 31 May 2018	<b>CONTRACT SPECIALIST</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214-90 (b)(6); (b)(7)(C)
<b>DIVISION/OFFICE</b> OAQ / IOSD	<b>CONTRACTING OFFICER</b> (b)(6); (b)(7)(C)	<b>TELEPHONE NO.</b> 214-90 (b)(6); (b)(7)(C)
<b>ACQUISITION DOCUMENT NO.</b> 70CMSD18P00000076	<b>CONTRACTOR</b> Harris Corporation	
<b>CONTRACTING OFFICER'S COMMENTS</b> Request pre-award legal review of over-the-air (OTA) equipment.	<b>ATTORNEY'S COMMENTS</b> x Legally Sufficient <input type="checkbox"/> Legally Sufficient Subject to Comments <input type="checkbox"/> Legally Insufficient (see comments below) ATTORNEY: (b)(6); (b)(7)(C) DATE: ___5/31/18	

# Document Routing Form



U.S. Immigration  
and Customs  
Enforcement

<b>1</b>	Date: May 31, 2018	Purpose: <input type="checkbox"/> Congressional <input type="checkbox"/> DHS <input checked="" type="checkbox"/> Routine	SharePoint Tracking No:
From:	(b)(6); (b)(7)(C)	Office: OAQ/IOSD	Telephone No: 214- (b)(6); (b)(7)(C)
			Room No: (b)(6); (b)(7)(C)
Subject Request one level above CO & Legal review – Pre-Award.			
Comments: Document will be signed once review is completed		Additional Requirements	

2 Required Concurrences Before Routing to the Office of the Director						
Name	Extension	Office	Action Requested	Initial	Date	Comments
(b)(6); (b)(7)(C)		OAQ	X Concur <input type="checkbox"/> Sign	(b)(6); (b)(7)(C)	5/31/2018	
		OAQ	<input type="checkbox"/> Concur <input type="checkbox"/> Sign		31MAY18	No comment.
		OPLA	<input type="checkbox"/> Concur <input type="checkbox"/> Sign		31 May 31, 2018	No comment

3 Office of the Director Concurrences						
ICE Director's Office						

**From:** (b)(6); (b)(7)(C)  
**Sent:** 30 May 2013 15:25:11 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Spectrum Amendment (2) to RFQ(CALD).doc  
**Attachments:** Spectrum Amendment (2) to RFQ(CALD).doc

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

(b)(6);  
(b)(7)(C) and I scrubbed it – for your review.

Thanks

(b)(6); (b)(7)(C)  
**OAQ Mission Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone: 214-905-(b)(6); (b)(7)(C) FAX: 214-905-5568**  
**Email:** (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***  
**Help us Support You Better: [How's My Service?](#)**

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, May 30, 2013 1:33 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Spectrum Amendment (2) to RFQ(CALD).doc

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

I made some initial comments on the PWS. Please take a look, and standardized the format of the positions and ensure that the desired experience is clearly communicated.

V/r

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905 (b)(6);  
(bb) 214.92 (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal~~

~~Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 3 Jun 2013 10:39:13 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Spectrum Amendment (2) to RFQ(CALD).doc

Thank you (b)(6); (b)(7)(C)

We accepted all the changes and the Program Office will review it to make sure they have what they need in the SOW. If they are ok with it, the amendment will go out today.

Thanks again

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

**Phone:** 214-905-(b)(6); (b)(7)(C) **FAX:** 214-905-5568

**Email:** (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***  
**Help us Support You Better: [How's My Service?](#)**

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, June 03, 2013 8:08 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Spectrum Amendment (2) to RFQ(CALD).doc

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

Please see attached amendment (CALD2) wherein I proposed some minor edits for clarification. Please advise if you accept all proposed changes. If so, I have no objection to proceeding with the amendment.

Thanks,  
(b)(6); (b)(7)(C)

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905.(b)(6); (b)(7)(C)  
(bb) 214.924

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT~~

~~USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:**  
**Sent:** Thursday, May 30, 2013 2:25 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Spectrum Amendment (2) to RFQ(CALD).doc

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

(b)(6);  
(b)(7)(C) and I scrubbed it – for your review.

Thanks

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

**OAQ Mission Support Dallas | HSI-West | Contracting Officer**  
DHS | ICE | Office of Acquisition Management (OAQ)  
**Phone:** 214-905-(b)(6); **FAX:** 214-905-5568  
**Email:** (b)(6); (b)(7)(C)

***Your First Partner in Acquisition!***  
**Help us Support You Better: [How's My Service?](#)**

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, May 30, 2013 1:33 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Spectrum Amendment (2) to RFQ(CALD).doc

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

I made some initial comments on the PWS. Please take a look, and standardized the format of the positions and ensure that the desired experience is clearly communicated.

V/r

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

Associate Legal Advisor  
ICE Office of the Principal Legal Advisor  
(p) 214.905-(b)(6);  
(bb) 214.92-(b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any~~

~~disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Jul 2014 15:16:51 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Sole Source for Harris Procurement  
**Attachments:** Sole source documentation from Harris.pdf, Sole Source Harris Crossbow System 2014(cald)kk updated.doc

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

I will bring you the docs for your signature momentarily, but I have attached the revised J&A for your review electronically.

The program updated the market research in two places, and I updated the segment concerning it being a commercial item, or not a commercial item. It definitely is not a commercial item and will not ever be a commercial item according to the Harris Corp CM. Their sole source documentation is attached to this e:mail, and a cy is in file.

Let me know if you need anything else.

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

**Investigations & Operations Support Dallas (IOSD-East) | Contracting Officer**

DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905-<sup>(b)(6);</sup>

Email: (b)(6); (b)(7)(C)





HARRIS CORPORATION

Government  
Communications Systems  
P.O. Box 37  
Melbourne, FL USA 32902-0037  
phone 1-321-727-9100

harris.com

19 September 2013

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

Mission Support – Dallas (MSD), OI East Team – Contracting Office  
DHS/ICE/Office of Acquisition Management  
7701 Stemmons Freeway, Ste (b)(6); (b)(7)(C)  
Dallas, Texas 75247-4232

**Subject: Sole Source Justification and Price Reasonableness**

To Whom It May Concern:

Harris Corporation, Government Communications Systems acting through its Wireless Products Group in Melbourne, Florida ("Harris") offers a comprehensive line of cellular transceiver equipment, accessories, training and maintenance for exclusive use by Government and Law Enforcement Agencies and is protected under USC Title 18. Harris developed the equipment and maintains exclusive ownership rights to its designs and software code. The designs and software code are considered Harris' proprietary information. Disclosure of Harris' proprietary information, including but not limited to posting said proprietary information on public websites, is strictly prohibited by certain confidentiality agreements.

Harris is the only source and supplier in the world for the RayFish® Products which includes the Crossbow System.

Harris maintains an internal price list for its product line. Any quotes provided by Harris use the standard domestic prices contained on the internal price list. Harris' standard domestic prices are the same prices charged to all Government and Law Enforcement customers. In addition, customers who are authorized to purchase off the General Services Administration ("GSA") Contract can use GSA Contract number GS-35F-0283J for applicable Harris products. In accordance with GSA Contract terms and conditions Harris can only offer its prices off GSA Contract number GS-35F-0283J to authorized agencies.

If you have any questions or require any additional information, please contact at (321) 309-(b)(6); (b)(7)(C) by email a (b)(6); (b)(7)(C)

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

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

Contracts Manager

Office of Acquisition Management (OAQ)  
Immigration & Customs Enforcement (ICE)  
Department of Homeland Security (DHS)

**Justification and Approval for other than Full and Open Competition**

**1. Agency and Contracting Activity**

The Department of Homeland Security (DHS), United States (U.S.) Immigration and Customs Enforcement (ICE), proposes to enter into a contract on a basis other than full and open competition. The contracting activity is the Office of Acquisition Management, Investigation and Operations Support Dallas, TX.

**2. Nature and/or Description of the Action Being Approved**

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

**3. Description of Supplies/Services**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**4. Identification of Statutory Authority Permitting Other Than Full and Open Competition**

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

**5. Demonstration of the Contractor's Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**6. Efforts to Obtain Competition**

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

**7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable**

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

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

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

**8. Description of Market Research**

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

**9. Any Other Facts Supporting the Use of Other than Full and Open Competition**

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

**10. Listing of Sources, if any, that Expressed in Writing and Interest in the Acquisition**

Harris Corporation  
P.O Box 9800  
Melbourne, FL 32902

**11. A Statements of the Actions, if any, the Agency May Take to Remove or Overcome Barriers To Competition Before any Subsequent Acquisition for Supplies or Services Required**

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

**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**12. Certifications**

I certify that the facts and representation under my cognizance, which are included in this justification, meet the Government’s minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

(b)(5)

\_\_\_\_\_  
Date

Immigration and Customs Enforcement (ICE)

Technical Operations (Tech Ops)

Phone number: 703-551-(b)(5)

**13. CONTRACTING OFFICER’S CERTIFICATION**

I certify that the justification is accurate and complete to the best of my knowledge and belief.

(b)(5)

\_\_\_\_\_  
Date

Contracting Officer

ICE/OAQ - MSD

~~FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE~~

Source Selection Sensitive in accordance with FAR 3.104-4

Justification and Approval for Other than Full and Open Competition  
Open Market Equipment/Training for the Harris Crossbow System

**Reviewed by:**

(b)(5) \_\_\_\_\_  
OAQ-IOSD-DAD

\_\_\_\_\_  
Date

(b)(5) \_\_\_\_\_  
OAQ-IOSD-AD

\_\_\_\_\_  
Date

**Approved by:**

This justification is hereby approved:

(b)(5) \_\_\_\_\_  
Competition Advocate  
Office of Acquisition Management (OAQ)

\_\_\_\_\_  
Date

**From:** (b)(6); (b)(7)(C)  
**Sent:** 10 Nov 2015 08:17:17 -0500  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Stingrays/FYI

(b)(7)(E)

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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)  
Phone: 214-905-(b)(6);  
Blackberry: 202-380-(b)(6); (b)(7)(C)  
Email: (b)(6); (b)(7)(C)

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.



**From:**

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

**Sent:**

7 Apr 2015 14:41:07 -0400

**To:**

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

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

**Subject:**

StingRay/harris Corp

(b)(7)(E)

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

Investigations & Operations Support Dallas | Deputy Assistant Director  
DHS | ICE | Office of Acquisition Management (OAQ)

Phone: 214-905 (b)(6);

Blackberry: 202-380 (b)(6);

Email: (b)(6); (b)(7)(C)

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.~~



---

**U.S. Immigration and Customs Enforcement**  
**Response to Request for the Rate of Use of International Mobile Subscriber Identity**  
**Catcher Technology**  
9/21/2017

The statistics listed below reflect only Homeland Security Investigations usage of international subscriber identity catcher technology.

- 1) The number of times your Office has deployed International Mobile Subscriber Identity (IMSI) Catchers, i.e., cell-site simulators. 223
- 2) How many individuals have been apprehended (i.e., arrested) using IMSI Catchers and related technologies i.e., cell-site simulators? 95
- 3) How many times IMSI Catchers and related technologies, i.e., cell-site simulators, have been utilized to gather evidence relevant to a case against any apprehended individuals? 104



---

**U.S. Immigration and Customs Enforcement**  
**Response to Request for the Rate of Use of International Mobile Subscriber Identity**  
**Catcher Technology**  
9/21/2017

(b)(5)

(b)(5)

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

---

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

**From:** OPLA-CLS  
**Sent:** 9 Jun 2017 15:11:43 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: query - CLS SME re Cell Site Simulator  
**Attachments:** 12-2258\_opn[1].pdf

Good Morning,

Please note the email below from (b)(6); (b)(7)(C) the CLS inbox seeking guidance on the use of cell site simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) office)  
202-494-(b)(6); (b)(7)(C) mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 10:41 AM  
**To:** OPLA-CLS  
**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

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

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

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you, (b)(6); (b)(7)(C)

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

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (w)  
202-904-(b)(7)(c)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

UNITED STATES COURT OF APPEALS

FOR THE SECOND CIRCUIT

---

August Term, 2014

(Argued: August 26, 2014    Decided: November 3, 2014)

Docket No. 12-2258-ag

---

SUZHEN MENG,

*Petitioner,*

— v. —

ERIC H. HOLDER, JR., UNITED STATES ATTORNEY GENERAL,

*Respondent.*

Before:

---

WINTER, RAGGI, CARNEY, *Circuit Judges.*

---

Petition for review of a Board of Immigration Appeals decision upholding an order of removal and the denial of (1) asylum and withholding of removal on the ground that the statutory “persecutor bar” precluded such relief given petitioner’s two-decade history of reporting women pregnant in violation of

China's family planning policy to local authorities, knowing that many such women would then be subject to forcible abortions or involuntary sterilizations; and (2) relief pursuant to the Convention Against Torture because petitioner failed to establish that it was more likely than not that she would be tortured if returned to China.

Petition for review DENIED.

---

GARY J. YERMAN, The Yerman Group, LLC, New York, New York, *for Petitioner.*

ALISON MARIE IGOE, Senior Counsel (Stuart F. Delery, Principal Deputy Assistant Attorney General; Lyle Jentzer, Senior Counsel, *on the brief*), Office of Immigration Litigation, United States Department of Justice, Washington, D.C., *for Respondent.*

---

REENA RAGGI, *Circuit Judge:*

Petitioner Suzhen Meng is a native and citizen of the People's Republic of China who seeks asylum, withholding of removal, and relief pursuant to the Convention Against Torture ("CAT") based on past political persecution in China, which she claims to have experienced because, as a local public security officer, she refused to collect security fees and reported police corruption. Meng now petitions this court for review of the May 9, 2012 decision of the Board of

Immigration Appeals (“BIA”) upholding the April 22, 2010 decision of Immigration Judge (“IJ”) Javier E. Balasquide, which denied Meng such relief and ordered her removal from the United States. See In re Suzhen Meng, No. A089 224 906 (B.I.A. May 9, 2012), aff’g No. A089 224 906 (Immig. Ct. N.Y.C. Apr. 22, 2010).

Meng contends that the agency erred in concluding that the statutory “persecutor bar” rendered her ineligible for asylum and withholding of removal. See 8 U.S.C. §§ 1158(b)(2)(A)(i), 1231(b)(3)(B)(i). She maintains that her actions as a public security officer, specifically, her reporting women pregnant in violation of China’s family planning limitations to local authorities, were insufficient as a matter of law to constitute “assistance” in persecution. Meng also challenges the agency’s finding that she failed to carry her burden for CAT relief.

For the reasons explained in this opinion, we identify no error in the agency’s rulings and, accordingly, we deny the petition for review.

## **I. Background**

### **A. Meng’s Application for Relief**

On February 25, 2008, Meng was admitted to the United States as a non-immigrant visitor with authorization to remain for six months. Five months later, on July 24, 2008, Meng filed for asylum, withholding of removal, and CAT



relief, stating that she had suffered past political persecution when, as a public security officer in her local community, she refused to collect a security fee from residents and wrote a letter to the local public security bureau alleging that the police chief was corrupt. Meng asserted that, as a result of these actions, her passport was confiscated and she was arrested and held in custody for 14 days, during which time a guard slapped her in the face several times and fellow prisoners beat her on instruction of the guards. Ten months later, Meng's passport was returned when she promised not to engage in any further anti-government activities, whereupon she left China.

B. Meng's Immigration Hearing

On September 16, 2008, Meng was charged as subject to removal for having overstayed her visa. See 8 U.S.C. § 1182(a)(7)(A)(i)(I). At an October 1, 2009 hearing before the IJ, Meng pursued her claim for relief from removal by testifying to the persecution alleged in her application. She also testified to her job responsibilities as a public security officer, a position she had held for 22 years. Meng stated that, in that capacity, she oversaw approximately 1,100 households, and that her duties included reporting all pregnant women to China's family planning office, including women pregnant in violation of state

limitations. Meng understood that when she reported a policy-violating woman to authorities, that woman would be punished, typically by being forced to undergo an abortion or sterilization. Indeed, she testified to having seen such women dragged away forcibly by the police. Nevertheless, Meng voluntarily continued to serve as a security officer and to make her reports, although she sometimes advised women whom she would report as being pregnant in violation of family planning policy to go into hiding or to flee.

C. Denial of Relief

On April 22, 2010, the IJ denied Meng's application for relief and ordered her removed. Although the IJ found Meng credible, he ruled that her active assistance in the persecution of women pregnant in violation of China's family planning policy barred her from receiving asylum or withholding of removal. The IJ further denied Meng CAT relief, concluding that she had failed to show that it was more likely than not that she would be tortured if returned to China.

The BIA essentially agreed with the IJ and dismissed Meng's appeal, prompting this petition for review.

## II. Discussion

### A. Standard of Review

On a petition for review of a BIA decision, we apply the deferential substantial-evidence standard to the agency’s findings of fact, treating them as “conclusive unless any reasonable adjudicator would be compelled to conclude to the contrary.” 8 U.S.C. § 1252(b)(4)(B); see Shunfu Li v. Mukasey, 529 F.3d 141, 146 (2d Cir. 2008). We apply de novo review, however, to questions of law, including whether an alien’s conduct could render her a “persecutor” as that term is statutorily defined. See 8 U.S.C. §§ 1158(b)(2)(A)(i), 1231(b)(3)(B)(i); Yanqin Weng v. Holder, 562 F.3d 510, 513 (2d Cir. 2009).

Where, as here, the BIA upholds the IJ’s decision and “closely tracks the IJ’s reasoning, this Court may consider both the IJ’s and the BIA’s opinions for the sake of completeness.” Maldonado v. Holder, 763 F.3d 155, 158–59 (2d Cir. 2014).

### B. Asylum and Withholding of Removal: The “Persecutor Bar”

Asylum is a form of discretionary relief that allows an otherwise removable alien to remain and work in the United States if she demonstrates that she is a “refugee,” i.e., an alien who “is unable or unwilling to return to, and is

unable or unwilling to avail . . . herself of the protection of, [her native] country because of [past] persecution or a well founded fear of [future] persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.” See 8 U.S.C. §§ 1101(a), 1158(b)(1)(A), (b)(3), (c)(1); 8 C.F.R. §§ 1208.13(b), 1208.21; Mei Fun Wong v. Holder, 633 F.3d 64, 68 (2d Cir. 2011). Withholding of removal, meanwhile, is a form of mandatory relief that prevents the removal of an alien to a country where “the alien’s life or freedom would be threatened . . . because of the alien’s race, religion, nationality, membership in a particular social group, or political opinion.” 8 U.S.C. § 1231(b)(3).

Both forms of relief are subject to a statutory “persecutor bar,” which renders an alien ineligible for either asylum or withholding if she has “ordered, incited, assisted, or otherwise participated in the persecution of any person on account of race, religion, nationality, membership in a particular social group, or political opinion.” Id. §§ 1158(b)(2)(A)(i), 1231(b)(3)(B)(i); see Xu Sheng Gao v. U.S. Att’y Gen., 500 F.3d 93, 97–98 (2d Cir. 2007). This court has identified four factors relevant to determining when this persecutor bar applies: (1) “the alien must have been involved in acts of persecution”; (2) a “nexus must be shown between the persecution and the victim’s race, religion, nationality, membership

in a particular social group, or political opinion”; (3) if the alien “did not [herself] incite, order, or actively carry out” the persecution, her conduct “must have assisted the persecution”; and (4) the alien must have had “sufficient knowledge that . . . her actions may assist in persecution to make those actions culpable.” Balachova v. Mukasey, 547 F.3d 374, 384–85 (2d Cir. 2008) (internal quotation marks omitted). Where evidence indicates that an alien assisted in persecution, the alien seeking relief from removal bears “the burden of proving by a preponderance of the evidence” that she “did not so act.” 8 C.F.R. § 208.13(c); see Zhang Jian Xie v. INS, 434 F.3d 136, 139 (2d Cir. 2006).

Here, the IJ and BIA concluded that Meng had assisted in the persecution of women who became pregnant in violation of China’s family planning policy because, in her role as a public security officer, she had reported such women to Chinese authorities for more than two decades knowing that, as a result, any number of these women would be subjected to forced abortions or sterilizations. Meng does not—and cannot—dispute that forced abortions and involuntarily sterilizations constitute persecution on a protected ground; they are statutorily defined as such. See 8 U.S.C. § 1101(a)(42); Yan Yan Lin v. Holder, 584 F.3d 75, 80 (2d Cir. 2009) (“It is settled law that forced abortion is persecution on account

of political opinion.”). Nor does she dispute that women in her community who became pregnant in violation of family planning policy were subjected to such persecution. Instead, Meng contends that the record evidence was insufficient as a matter of law to admit a finding that she “assisted” in such persecution. She maintains that her actions in registering and reporting unauthorized pregnancies were merely tangential, passive accommodations of the persecutory conduct of Chinese family planning authorities, which Zhang Jian Xie v. INS, 434 F.3d at 143, holds is not enough to constitute assistance in persecution. See also Xu Sheng Gao v. U.S. Att’y Gen., 500 F.3d at 99–100 (holding mere association with persecutory enterprise insufficient to trigger persecutor bar). Indeed, Meng argues that Xu Sheng Gao requires evidence that one of her reports led to a specific forced abortion or involuntary sterilization to admit a finding of assistance. See id. In fact, the cited precedents do not support Meng’s arguments.

In Zhang Jian Xie, at the same time that this court observed that conduct “passive in nature” and “tangential” to third-party acts of oppression is insufficient to manifest “assistance,” we stated that “active” conduct, having “direct consequences for the victims,” can constitute “assistance in persecution.”

434 F.3d at 143. Here, Meng's conduct was clearly active and not passive. She affirmatively identified pregnant women in her community, including those pregnant in violation of China's family planning policy, and she deliberately reported these women to authorities. Nor was she merely associated with a persecutory enterprise. She was integral to the effectuation of persecution. Meng's reporting of policy-violating women was no "minor" action, but the critical step that set in motion the entire persecutory scheme of enforcement. Cf. id. (upholding agency's imposition of persecutor bar even though petitioner's assistance was "arguably minor"). Indeed, without Meng's reports, authorities would not have known which women had violated family planning policy. Moreover, Meng's actions had direct consequences for the victims insofar as her reports were the basis for women being subjected to forced abortions and sterilizations. Meng not only admitted knowing that her conduct had this effect; she testified that it was the reason she sometimes urged the women whom she reported to hide or flee. Nevertheless, with knowledge that her conduct triggered persecution, Meng voluntarily continued to serve for more than two decades as a public security officer and to report women for unauthorized pregnancies. This record was sufficient to admit the agency finding that Meng

assisted in persecution. See In re Suzhen Meng, No. 089 224 906, at 2 (finding that “as a result of [Meng’s] actions, the Family Planning officials went to women’s homes who had illegal pregnancies, seized them, and subjected them to forced abortions and sterilizations”).

Xu Sheng Gao v. U.S. Attorney General compels no different conclusion. In that case, the alien who reported offending booksellers to Chinese authorities knew only that there was a possibility that the booksellers “could” be arrested and imprisoned, but nothing indicated that any bookseller had, in fact, been subjected to such treatment. 500 F.3d at 100 (emphasis in original). Rather, the most serious sanction that petitioner knew ever to have been imposed on a reported bookseller was revocation of a business license. See id. It was in these circumstances—with no evidence of persecution ever resulting from the alien’s conduct—that we were “unable to conclude” that the alien had “the requisite level of knowledge that his acts assisted in persecution to sustain a finding that he was a ‘persecutor’ under the statute.” Id. at 102. By contrast, here, Meng admitted knowing that forced abortions and sterilizations were the typical punishment meted out to women she reported for unauthorized pregnancies. Where, as in this case, the occurrence of the persecution is undisputed, and there



is such evidence of “culpable knowledge that the consequences of one’s actions would assist in acts of persecution,” Xu Sheng Gao specifically states that “the evidence need not [further] show that the alleged persecutor had specific actual knowledge that his actions assisted in a particular act of persecution.” Id. at 103.<sup>1</sup>

Yanqin Weng v. Holder also affords Meng no support in challenging the application of the persecutor bar to this case. 562 F.3d at 515. In Yanqin Weng, the petitioning alien, a nurse’s assistant, provided post-surgical medical care to women in China who had undergone forced abortions and, on one occasion, sat outside the locked door of a room where women awaiting forced abortions were being held until delayed doctors arrived to perform the procedures. See id. at 512, 515. In concluding that the persecutor bar did not apply to these circumstances, this court observed that the petitioner’s provision of post-surgical care did not contribute to the abortions. See id. at 515. As for petitioner’s guarding women facing forced abortions, that one-time occurrence was deemed to have “deviated markedly from her routine duties” and lasted only ten minutes

---

<sup>1</sup> Xu Sheng Gao also concluded that the reporting petitioner did not assist in persecution that reflected the discretionary decision of others at the end of an attenuated chain of authority. See 500 F.3d at 101–02. But where, as here, Meng’s reports regularly resulted in persecution, she knew that, and she nevertheless continued to report, we conclude that the agency has a substantial basis for finding assistance and applying the persecutor bar.

before petitioner, in fact, helped one of the women escape, which resulted in petitioner losing her job. Id. Here, as already noted, Meng's reporting of women pregnant in violation of China's family planning policy did contribute directly to the forced abortion and sterilization of these women. Further, Meng engaged in such reporting over a period of two decades. In short, her assistance in persecution was not a single, marked departure from her duties, but a regular, and important, aspect of her duties. While Meng may have encouraged some women to hide or flee to avoid the persecution that she knew would follow from her conduct, the record indicates that Meng nevertheless persisted in reporting women with unauthorized pregnancies as long as she served as a public security official.

Accordingly, because the record evidence was sufficient to support a finding that Meng assisted in persecution, we identify no legal error in the agency's determination that the persecutor bar rendered Meng ineligible for asylum or withholding of removal.

D. CAT Relief

A petitioner seeking CAT relief must demonstrate that it is "more likely than not" that she will be tortured if removed to her home country. See 8 C.F.R.

§ 208.16(c)(2); Yan Yan Lin v. Holder, 584 F.3d at 82. Here, we identify no error in the agency's denial of CAT relief for failure to satisfy this requirement.

Meng essentially relies on evidence of her past 14-day detention and beatings to argue likely future persecution. We need not here decide if this experience rose to the level of "torture," but see 8 C.F.R. § 1208.18(a)(2) (defining torture as "extreme form of cruel and inhuman treatment"); Kyaw Zwar Tun v. INS, 445 F.3d 554, 567 (2d Cir. 2006) ("[T]orture requires proof of something more severe than the kind of treatment that would suffice to prove persecution."), because even assuming that the issue were resolved in Meng's favor, she would not have demonstrated agency error.

Past torture does not give rise to a presumption of future torture. Rather, it serves as evidence of the possibility of future torture. See 8 C.F.R. § 1208.16(c)(3). Here, the following facts demonstrate why such a possibility cannot be converted into the requisite likelihood: (1) after Meng's release from detention, she remained in China for more than 10 months without experiencing any further harm; (2) Chinese authorities returned her passport, thereby allowing her to travel outside China; and (3) Meng's husband and children remain in China unharmed. See Melgar de Torres v. Reno, 191 F.3d 307, 313 (2d Cir. 1999)

(holding that where family members remain unharmed in petitioner's native country, objective fear of future harm is undermined); see also Mu Xiang Lin v. U.S. Dep't of Justice, 432 F.3d 156, 160 (2d Cir. 2005) (upholding denial of CAT relief where petitioner offered no "particularized evidence" that she would be tortured in her country of removal). We therefore conclude that substantial evidence supports the agency's determination that Meng has not demonstrated that it is "more likely than not" that she will be tortured if returned to China.

### **III. Conclusion**

To summarize, we conclude:

1. The statutory persecutor bar rendered Meng ineligible for asylum and withholding of removal because, for over 20 years, she reported the identities of women with unauthorized pregnancies, knowing that, as a result, many of these women would be subjected to forced abortions and sterilizations. This showing was legally sufficient to demonstrate her assistance in persecution.

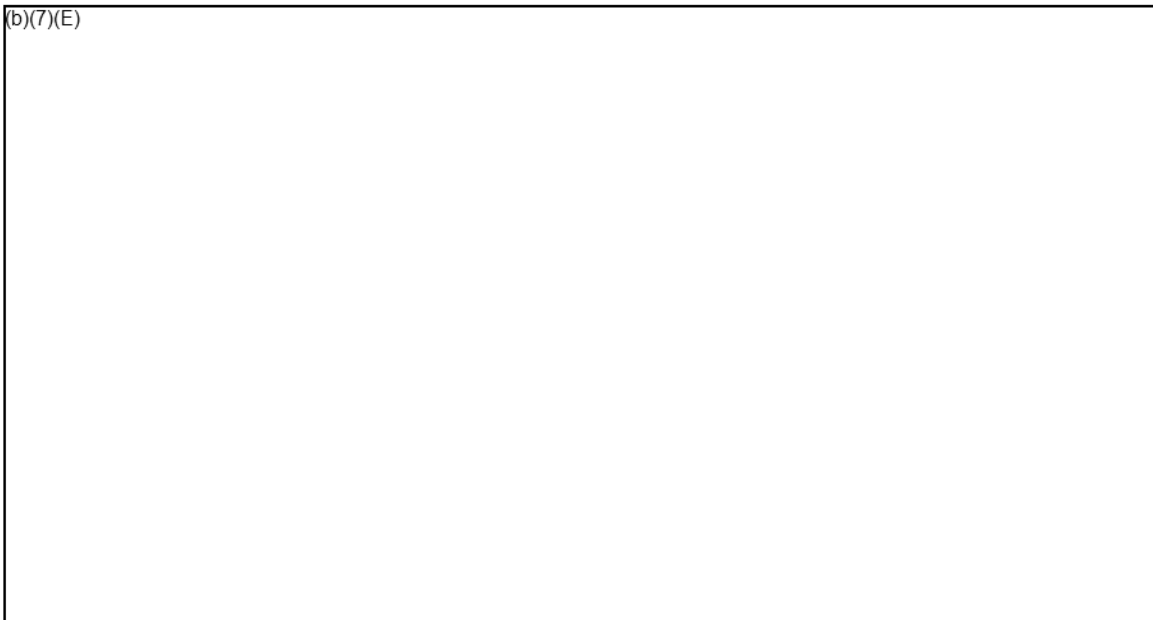
2. Meng is not entitled to CAT relief because she has not established that it is more likely than not that she will be tortured if removed to China.

Accordingly, the petition for review is DENIED.

**The Department of Homeland Security's Response to  
Senator Al Franken's August 24, 2017 Letter**

1. **Policy Directive 047-02 “applies to the use of CSS technology inside the United States in furtherance of criminal investigations.” According to ICE, CSS devices are used “in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act.” ICE has also stated that ICE Enforcement and Removal Operations (ERO) “does not use cell-site simulators for the purpose of civil immigration enforcement.”**
  - a. **In the Department’s use of CSS technology for criminal investigations, does DHS distinguish between the seriousness of criminal offenses in determining whether to deploy CSS technology? If so, how?**

(b)(7)(E)



- b. **The Department’s response to Senator Wyden’s May 23, 2017 letter confirmed that ERO does not use CSS devices for administrative immigration enforcement. Does any other Component within the Department use CSS technology pursuant to non-criminal investigations within the United States.**

(b)(7)(E)



2. **Policy Directive 047-02 states that “[a]ffected DHS Components may issue additional specific guidance consistent with this policy.” Please provide copies of all such**

additional specific guidance, if any, issued by DHS's immigration enforcement Components.

(b)(5)

(b)(5)

3. Policy Directive 047-02 provides that DHS Components shall implement an auditing program to ensure that data collected by CSS technology is deleted following the completion of a mission, upon location of a target, and upon the identification of a target. Are such audits performed by Components that use CSS technology for immigration enforcement? If not, why?

- a. If so, how frequently are such audits performed?
- b. If so, what have such audits revealed about DHS Components' data collection, retention, and disposal practices?

DHS Components do not use CSS for administrative immigration violations.

4. Policy Directive 047-02 provides that "DHS is committed to ensuring that law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals." Furthermore, in response to Senator Wyden's letter, ICE stated that ICE Homeland Security Investigations operates CSS devices "in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information."

- a. Aside from Policy Directive 047-02, what "rules, policies, and laws" apply to information collected through the use of CSS technology? In particular, what "rules, policies, and laws" apply to information about noncitizens obtained through the use of CSS technology?

(b)(7)(E)

(b)(7)(E)

- b. **Section 14 of President Trump’s Executive Order, entitled *Enhancing Public Safety in the Interior of the United States*, seeks to remove Privacy Act protections from immigrants who are not U.S. citizens or permanent residents. What effect does Section 14 of the President’s January 25, 2017 Executive Order have on the Department’s data collection and disposal policies, including but not limited to those laid out in Policy Directive 047-20?**

Section 14 of President Trump’s Executive Order, *Enhancing Public Safety in the Interior of the United States*, will not change how DHS and, specifically, ICE, collects or disposes of data obtained through cell-site simulators.

5. **Policy Directive 047-02 provides that an application or supporting affidavit should inform the court that the target cell phone and other cell phones in the area of the CSS device might experience a temporary disruption of service from the service provider. In response to Senator Wyden’s letter, ICE stated that**

(b)(7)(E)

- a. **Have DHS employees (rather than manufacturers or third parties) tested the CSS technology the Department uses to measure the interference caused to nearby phones? If so, please provide a copy of all testing reports or other documentation related to device and network interference caused by CSS technology.**

---

<sup>1</sup> See DHS/ICE – External Investigations System of Records Notice, (75 FR 404, Jan. 5, 2010), available at: <https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31269.htm>.

<sup>2</sup> [https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf).

(b)(7)(E)

6. Does DHS maintain a record of which components possess CSS technology; how many CSS devices each component has; the makes and models of CSS devices used by each component; and when, where, and for how long the devices are used for immigration enforcement? If so, please provide a copy of such records.

(b)(7)(E)

7. Does DHS maintain a record of how many individuals have been located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology? If so, please provide a copy of such records and state how many of the individuals located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology have been arrested for a crime, convicted of a crime, and convicted of a violent crime.

(b)(5)

8. Does DHS deploy CSS technology for immigration enforcement purposes along the nation's borders? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.

No.



- 9. Does DHS deploy CSS technology during interior immigration enforcement? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.**

No.

The Honorable Al Franken  
United States Senate  
Washington, DC 20510

Dear Senator Franken:

Thank you for your August 24, 2017 letter. Acting Secretary Duke asked that I respond on her behalf.

For specific responses to each of your questions, please refer to the enclosure. To address your specific concern related to U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) utilizing cell-site simulators, I can confirm that ICE/ERO does not use cell-site simulators for the purpose of civil immigration law enforcement. While ICE/ERO's primary mission is to enforce the Nation's civil immigration laws, individual ERO officers may participate in Joint Task Forces with federal, state, and local law enforcement partners, in furtherance of our shared public safety mission. Such a Joint Task Force may employ various technologies, including cell-site simulator technology, to pursue individuals suspected of engaging in criminal activity. However, such use must be conducted in a manner that protects rights afforded by the U.S. Constitution, and in compliance with applicable statutory authorities.

While cell-site simulators are used by several Components of the U.S. Department of Homeland Security (DHS), no Component is using this technology for the purpose of civil immigration enforcement. ICE Homeland Security Investigations (HSI) uses cell-site simulators in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act. ICE/HSI's use of cell-site simulator technology in the context of criminal investigations may result in undocumented immigrants being arrested when they are the targets of said criminal investigations.

U.S. Customs and Border Protection (CBP) currently makes limited use of cell-site simulators. CBP's Office of Professional Responsibility (OPR) has used this technology in support of ongoing criminal investigations related to employee integrity and workforce security.

The United States Secret Service (USSS) also uses cell-site simulators to locate hard to find special interest subjects by locating targeted mobile devices. In appropriate cases, USSS uses this technology to assist Federal and state, local, tribal, and territorial criminal investigations by locating targeted mobile devices associated with suspects wanted for very serious felonies and violent crimes.

The DHS Components that use cell-site simulators do so in a manner that is consistent with DHS Policy Directive 047-02, *Department Policy Regarding the Use of Cell-Site Simulator Technology*, dated October 19, 2015, which closely aligns with the U.S. Department of Justice's policy guidance regarding the use of cell-site simulator technology. Under current policy, operators must obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent).

(b)(7)(E)

(b)(7)(E)

DHS remains committed to ensuring law enforcement practices concerning the collection or retention of data are lawful and respect the important privacy interests of individuals.

Thank you again for your letter and interest in this important matter. The co-signers of your letter will receive separate, identical responses.

Sincerely,

James D. Nealon  
Assistant Secretary for International Affairs  
Office of Strategy, Policy, and Plans

Enclosure



*Office of the Director*

**U.S. Department of Homeland Security**  
500 12th Street, SW  
Washington, D.C. 20536



**U.S. Immigration  
and Customs  
Enforcement**

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

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

[www.ice.gov](http://www.ice.gov)

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

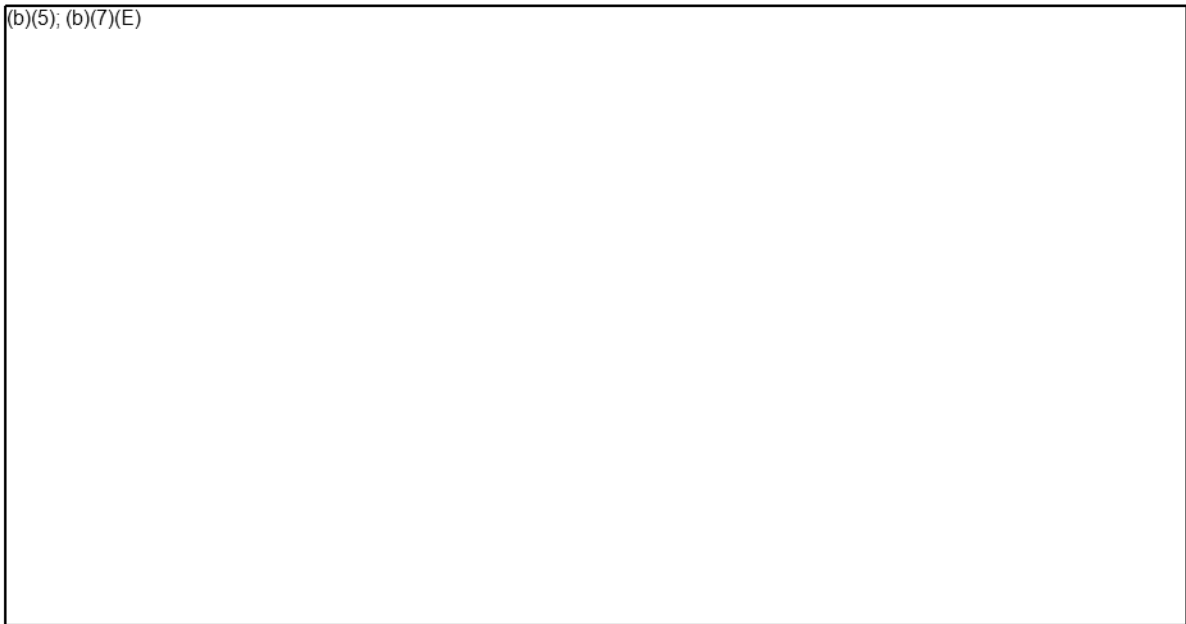
Respectfully,

Thomas D. Homan  
Acting Director

**The Department of Homeland Security's Response to  
Senator Al Franken's August 24, 2017 Letter**

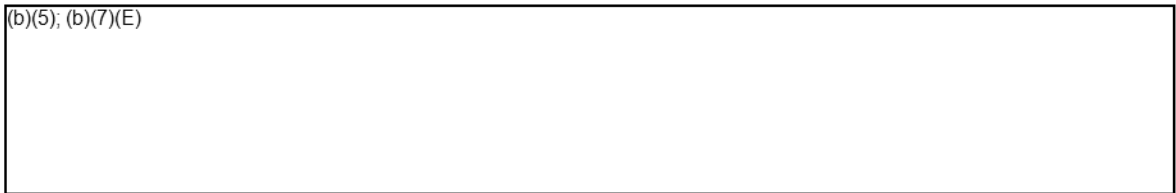
- 1. Policy Directive 047-02 “applies to the use of CSS technology inside the United States in furtherance of criminal investigations.” According to ICE, CSS devices are used “in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act.” ICE has also stated that ICE Enforcement and Removal Operations (ERO) “does not use cell-site simulators for the purpose of civil immigration enforcement.”**
  - a. In the Department’s use of CSS technology for criminal investigations, does DHS distinguish between the seriousness of criminal offenses in determining whether to deploy CSS technology? If so, how?**

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



- b. The Department’s response to Senator Wyden’s May 23, 2017 letter confirmed that ERO does not use CSS devices for administrative immigration enforcement. Does any other Component within the Department use CSS technology pursuant to non-criminal investigations within the United States.**

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



- 2. Policy Directive 047-02 states that “[a]ffected DHS Components may issue additional specific guidance consistent with this policy.” Please provide copies of all such**

(b)(5); (b)(7)(F)

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

3. **Policy Directive 047-02 provides that DHS Components shall implement an auditing program to ensure that data collected by CSS technology is deleted following the completion of a mission, upon location of a target, and upon the identification of a target. Are such audits performed by Components that use CSS technology for immigration enforcement? If not, why?**

- a. **If so, how frequently are such audits performed?**
- b. **If so, what have such audits revealed about DHS Components' data collection, retention, and disposal practices?**

DHS Components do not use CSS for administrative immigration violations.

4. **Policy Directive 047-02 provides that "DHS is committed to ensuring that law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals." Furthermore, in response to Senator Wyden's letter, ICE stated that ICE Homeland Security Investigations operates CSS devices "in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information."**

- a. **Aside from Policy Directive 047-02, what "rules, policies, and laws" apply to information collected through the use of CSS technology? In particular, what "rules, policies, and laws" apply to information about noncitizens obtained through the use of CSS technology?**

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



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

- b. Section 14 of President Trump’s Executive Order, entitled *Enhancing Public Safety in the Interior of the United States*, seeks to remove Privacy Act protections from immigrants who are not U.S. citizens or permanent residents. What effect does Section 14 of the President’s January 25, 2017 Executive Order have on the Department’s data collection and disposal policies, including but not limited to those laid out in Policy Directive 047-20?**

Section 14 of President Trump’s Executive Order, *Enhancing Public Safety in the Interior of the United States*, will not change how DHS and, specifically, ICE, collects or disposes of data obtained through cell-site simulators.

- 5. Policy Directive 047-02 provides that an application or supporting affidavit should inform the court that the target cell phone and other cell phones in the area of the CSS device might experience a temporary disruption of service from the service provider. In response to Senator Wyden’s letter, ICE stated that**

(b)(7)(E)

- a. Have DHS employees (rather than manufacturers or third parties) tested the CSS technology the Department uses to measure the interference caused to nearby phones? If so, please provide a copy of all testing reports or other documentation related to device and network interference caused by CSS technology.**

---

<sup>1</sup> See DHS/ICE – External Investigations System of Records Notice, (75 FR 404, Jan. 5, 2010), available at: <https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31269.htm>.

<sup>2</sup> [https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf).

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

6. Does DHS maintain a record of which components possess CSS technology; how many CSS devices each component has; the makes and models of CSS devices used by each component; and when, where, and for how long the devices are used for immigration enforcement? If so, please provide a copy of such records.

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

7. Does DHS maintain a record of how many individuals have been located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology? If so, please provide a copy of such records and state how many of the individuals located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology have been arrested for a crime, convicted of a crime, and convicted of a violent crime.

DHS does not use CSS for administrative immigration violations.

(b)(5)

- 9. Does DHS deploy CSS technology during interior immigration enforcement? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.**

No.

**From:**

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

**Sent:**

15 Aug 2016 13:12:17 -0400

**To:**

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

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

**Cc:**

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

**Subject:**

Border Search Issues

**Attachments:**

Border search electronic devices checklist (FINAL 1 21 15) (2).docx, Border Searches of Electronic Devices Hypothetical Questions Answers (FINAL 1 21 15).docx, Cybersmuggling Investigations (Updated as of 8.15.16).pptx, Border Search suppression motions, RE: (b)(6); (b)(7)(C) defense motions re search warrants

Border Search Team (copying everyone for awareness though),

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

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

Please let me (b)(5) know if you have any questions.

Thanks.

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

U.S. Immigration and Customs Enforcement  
Office of the Principal Legal Advisor  
2015 Reference Sheet for Border Searches of Electronic Devices

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

U.S. Immigration and Customs Enforcement  
Office of the Principal Legal Advisor  
2015 Reference Sheet for Border Searches of Electronic Devices

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

U.S. Immigration and Customs Enforcement  
Office of the Principal Legal Advisor  
2015 Reference Sheet for Border Searches of Electronic Devices

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

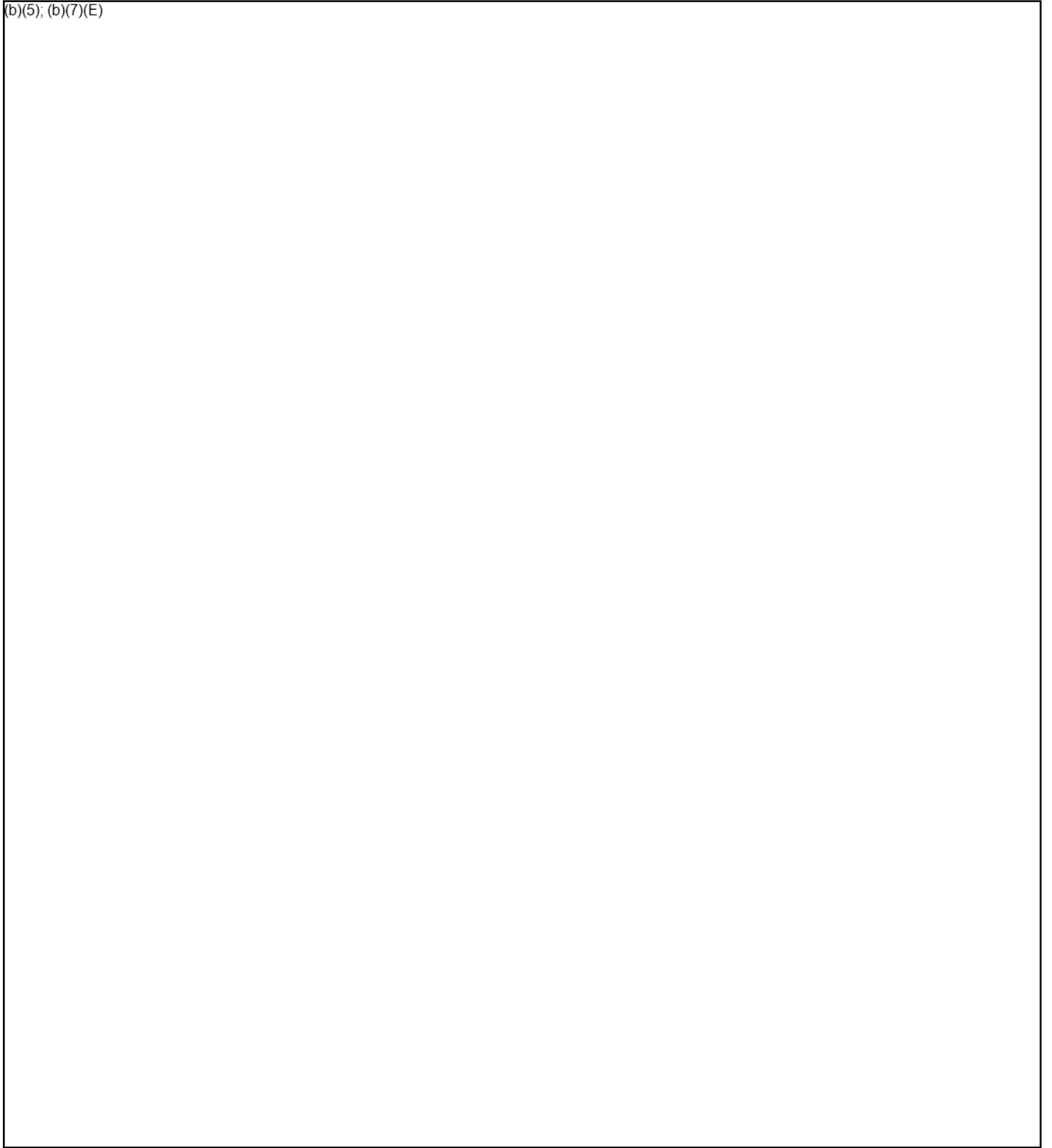


U.S. Immigration and Customs Enforcement  
Office of the Principal Legal Advisor  
2015 Reference Sheet for Border Searches of Electronic Devices

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

**Border Searches of Electronic Devices Hypothetical Questions & Answers**

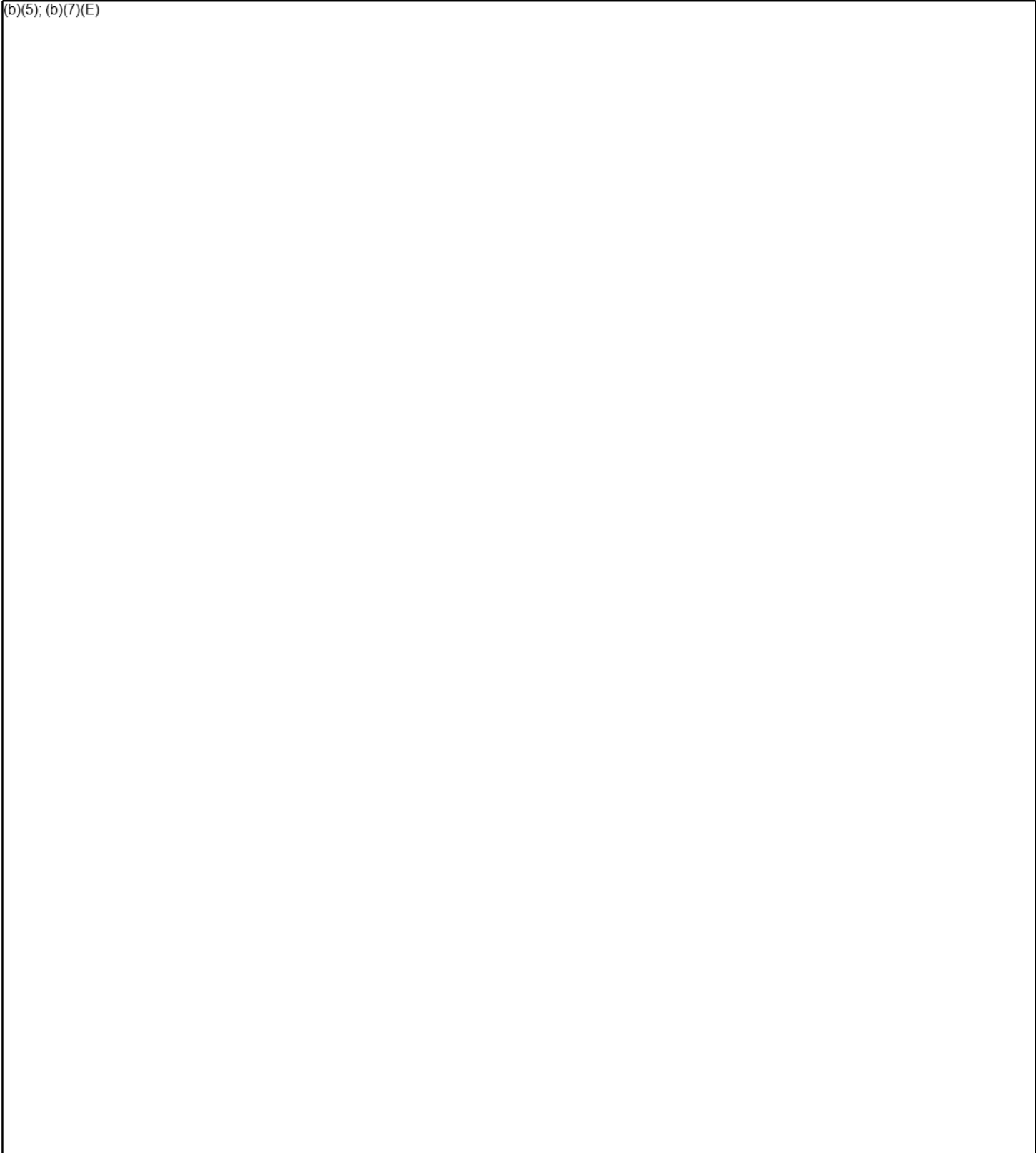
(b)(5); (b)(7)(E)



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

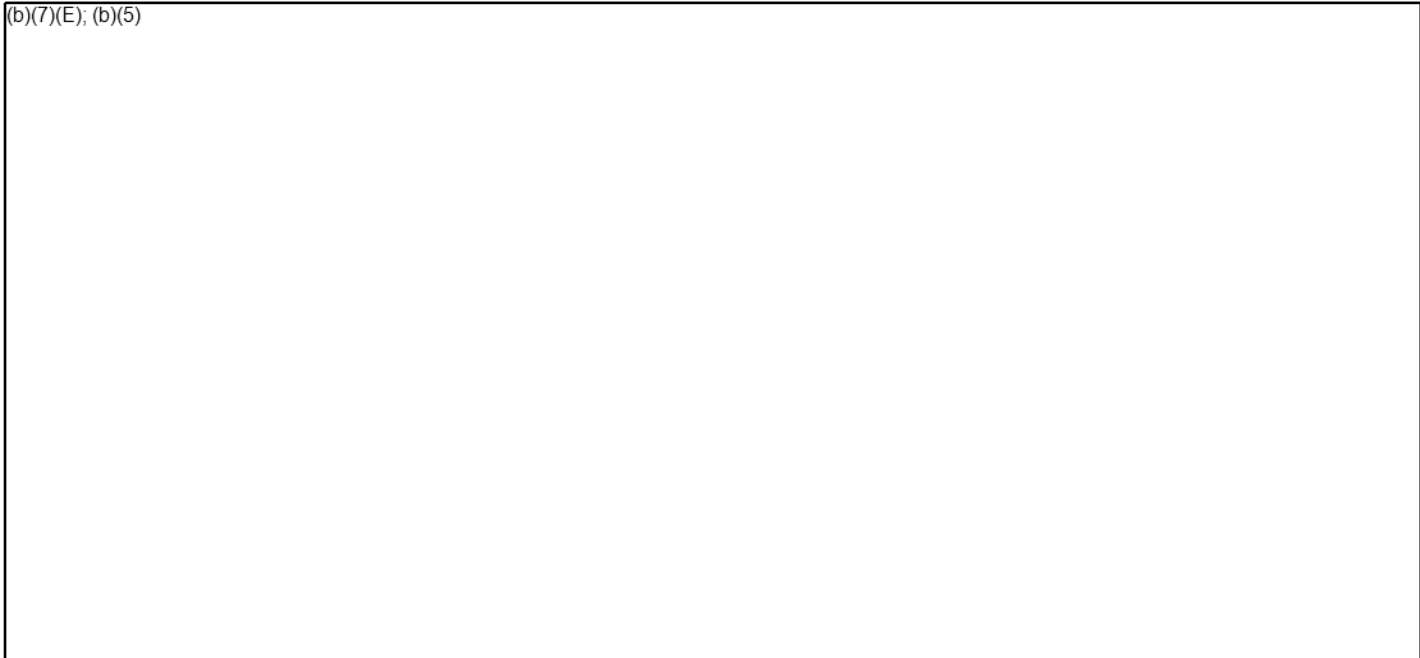
(b)(7)(E); (b)(5)

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



FOR INTERNAL ICE DISCUSSION PURPOSES ONLY  
NOT FOR FURTHER DISSEMINATION

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



~~Law Enforcement Sensitive/For Official Use Only~~  
~~Attorney-Client Work Product/Attorney-Client Privileged~~

# ICE

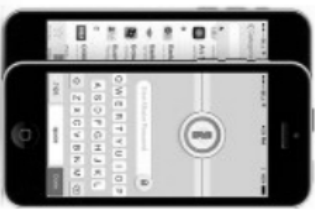


## **Cybersmuggling Investigations**

XXXXXXXXXOffice of the Principal Legal AdvisorApril  
2016



U.S. Immigration  
and Customs  
Enforcement



2020-ICLI-00013 267

## Overview

- OPLACL SHSI Embed Program ICE Cyber Authorities Fourth Amendment Search and Seizure Fifth Amendment and Electronic Devices Statutory Authority and Limitations





## Overview: OPLA

- ICE Office of the Principal Legal Advisor  
Headquarters Overview of Divisions Homeland  
Security Investigations Law Division Criminal  
Law Section  
Offices of the Chief Counsel HSI Embedded  
Attorney



## Overview: HSI

- 19 U.S.C. 1401(i) Definition of Customs Officers  
19 U.S.C. 1589a Enforcement Authority of Customs Officers  
Criminal Investigation Series, 1811



# ICE

## 19 U.S.C. 1589a

An officer of the customs may(1) carry a firearm; (2) execute and serve any order, warrant, subpoena, summons, or other process issued under the authority of the United States;(3) make an arrest without a warrant:for any offense against the U.S. committed in the officer's presencefor a felony, cognizable under the laws of the U.S. committed outside the officer's presence if the officer has reasonable grounds to believe that the person to be arrested has committed or is committing a felony(4) perform any other law enforcement duty that the Secretary of the Treasury may designate.



U.S. Immigration  
and Customs  
Enforcement

## HSI Investigations

- Money Laundering / Bulk Cash Smuggling Narcotics Smuggling / Trafficking Commercial Trade and Fraud Human Smuggling / Trafficking Export Enforcement Intellectual Property Rights (IPR) Trade Secrets Theft Child Sexual Exploitation / Child Sex Tourism Identity Document / Benefit Fraud Worksite Enforcement / Critical Infrastructure Protection



## Authority v. Jurisdiction

- Authorities are granted by statute, Executive Order, etc. Usually to Department and then delegated Federal law enforcement agents with general arrest authority  
Jurisdictional agreements “Beltway” lines to avoid jurisdictional disagreements  
Courts recognize jurisdiction ≠ authority



# ICE

## Cyber Authorities

- General Authority Computer Fraud and Abuse Act/HERO Act of 2015



U.S. Immigration  
and Customs  
Enforcement

## Trade Secrets Theft

- 18 U.S.C. § 1831 “Economic espionage” statute, criminalizes the knowing theft of a trade secret for the benefit of any foreign government, foreign instrumentality, or foreign agent
- 18 U.S.C § 1832 “Trade secrets theft” statute, criminalizes the same conduct; however, the beneficiary of the theft is anyone other than the owner of the trade secret







# ICE

## Fourth Amendment and How it Protects

- 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.



U.S. Immigration  
and Customs  
Enforcement



## Fourth Amendment Exclusionary Rule: Exception

- Good faith reliance on search warrant issued by neutral and detached magistrate, even if lacking in probable cause or otherwise defective, will not be excluded.



## Searches

- Government participation Intrusion (physical, visual, auditory) Reasonable Expectation of Privacy (“REP”) Subjective expectation of privacy Objectively reasonable



# ICJE

# No REFP

- Open fields  
Open view
- Overheard conversations  
Abandoned Property
- Trash  
Odors
- Items previously and lawfully searched  
Movement of vehicles and containers in public



U.S. Immigration  
and Customs  
Enforcement

## *U.S. v. Jones*

- Warrantless Installation of GPS Tracker  
Intent to obtain information + Trespass  
Short duration monitoring permissible  
48-hour rule (DOJ policy)  
Inapplicable situations  
Exceptions to warrant requirement  
Commercial vehicles, aircraft, vessels  
Border searches  
Per se reasonable  
Extended border search  
Extraterritorial application



## General Rule - Warrants

- Warrantless searches & seizures generally are presumed to be unreasonable unless a reasonable exception applies  
Requirements: Probable Cause  
Particularity



# ICE

## Warrants & Electronic Devices

- Scope  
Particularity  
Retention  
Time limits



U.S. Immigration  
and Customs  
Enforcement



# IOE

## Exceptions to Warrants But PC Still Needed

- Arrest in a Public Place Plain View  
Lawful presence/access Probable  
cause to seize is immediately  
apparent Exigent  
Circumstances Mobile  
Conveyances



U.S. Immigration  
and Customs  
Enforcement

# IOE

## Exceptions – Warrant & PC

- Protective Sweep  
Regulatory  
Stop/FriskInventory Administrative  
Search Incident to  
Arrest Consent Border Search



U.S. Immigration  
and Customs  
Enforcement

# ICJE

## Search Incident to Arrest

- Purpose: To prevent arrestee's access to weapons or destruction/concealment of evidence  
Scope: Exterior of arrestee's clothing; Objects carried by arrestee; Area within arrestee's immediate control; Strip Search – Reasonable Suspicion articles are concealed beneath clothing  
No cell phones



U.S. Immigration  
and Customs  
Enforcement

## *Riley v. California*

- *Wirie (First Circuit) Limited search of a flip phone Categorical rule against SIA*  
*Riley (California) Two searches of a smart phone Categorical rule for SIA of device found on person*  
*S.Ct. – Categorical rule against SIA of cell phones Qualitatively and quantitatively different Other exception may be ok, including border search*



# ICJE

## Consent

Voluntary from a Totality of the  
Circumstances Knowledge of rights, Written  
consent, Presence of witnesses Age and  
sophistication, Authority to consent  
Authority to Consent: Actual: Person with  
RFP in thing/place to be searched Apparent:  
Person who appears to have RFP



U.S. Immigration  
and Customs  
Enforcement

# ICJE

## **Consent and Electronic Devices**

**Ambiguity of authority  
Scope  
Revocation  
Answering calls**



U.S. Immigration  
and Customs  
Enforcement

2020-ICLI-00013 290

## Border Search Exception

- *General Rule: Searches & seizures must be conducted with a warrant supported by probable cause*  
*Exception: Border searches*  
*No warrant needed*  
*No probable cause needed*  
*NOT exempt from reasonableness requirement of the Fourth Amendment*



# ICE

## Border Search

- Purpose Protect nation's bordersProtect revenueProhibit importation or exportation of merchandise contrary to lawScope MerchandiseEvidence related to merchandise



U.S. Immigration  
and Customs  
Enforcement



- **Customs Officer**  
Searching for merchandise or evidence relating to merchandise  
At the Border includes Functional Equivalent of the Border (FEB) includes Extended Border (EB)



# ICE

## Customs Officer

- ICE Special Agents  
CBP officers  
Coast Guard officers -commissioned,  
warrant, or petty officer  
Others formally designated by ICE or  
CBP (other Fed, State, local, or  
foreign LEOs who go through formal  
cross-designation training)



U.S. Immigration  
and Customs  
Enforcement

## Merchandise

- Goods, wares & chattels of every description, including: Prohibited items - contraband Monetary instruments Intellectual property – trade secrets, copyrighted material Merchandise or evidence relating to merchandise  
Merchandise is not: General evidence of criminality Intelligence Exclusively correspondence



## At the Border

- What is “the Border”?  
Territorial Limits of the United States  
Land, Air, Marine  
Border  
Functional Equivalent of the  
Border  
Extended Border



# ICE

## Functional Equivalent of the Border (FEB)

- Reasonable certainty of border nexus  
Crossing or contact with something or someone that has crossed/will cross  
Reasonable certainty of no material change – and  
First practicable detention point or... last practicable detention point (for outbound searches)



U.S. Immigration  
and Customs  
Enforcement

## Extended Border (EB)

- Reasonable certainty of border nexus  
Crossing or contact with something or someone that has crossed  
Reasonable certainty of no material change – and  
Reasonable suspicion of criminal activity



# ICE

## Landmark Cases

- General – U.S. v. Ramsey, 1977  
People – U.S. v. Montoya de Hernandez, 1985  
Objects – U.S. v. Flores-Montano, 2004



U.S. Immigration  
and Customs  
Enforcement





# ICE

## *U.S. v. Ickes*

- Searching contents of a laptop at border is categorically a routine border search Specifically applied Flores-Montano to computer searches No level of suspicion needed



U.S. Immigration  
and Customs  
Enforcement

# ICE

## *U.S. v. Arnold*

- D. Ct. - Non-routine border search & requires RS Implicates dignity & privacy interests Likened to inner most recesses of human mind Reversed by 9th Circuit  
panellaptop is merchandise; requires no heightened level of suspicion for border search Followed Flores-Montano En Banc denied, Cert. denied.



U.S. Immigration  
and Customs  
Enforcement

# ICE

## *U.S. v. Cotterman*

- *D. Ariz. - Movement to ICE lab considered 2nd search requiring reasonable suspicion under EB doctrine*  
*Court of Appeals (Round 1) – Not an extended border search, no reasonable suspicion necessary and search itself was reasonable*  
*En Banc 2013 – Forensic searches require reasonable suspicion.*  
*Reasonable suspicion was present here.*



U.S. Immigration  
and Customs  
Enforcement

# ICIE

## *Post-Cotterman Issues*

What is a forensic search? The “in the alternative” reasonable suspicion argument. The “stop and get a warrant” approach. Detention pretextual Eroding authority Probable cause vs. Cotterman reasonable suspicion



U.S. Immigration  
and Customs  
Enforcement

# ICE

## *U.S. v. Saboonchi*

- IIEPPA & ITSR charges  
Not an extended border search just because examined away from the border  
Forensic search requires reasonable suspicion  
Forensic search = creation of a bitstream copy + analysis by special software



U.S. Immigration  
and Customs  
Enforcement

# ICE

## *Post-Riley Issues*

Cell phone ≠ any other container  
What if traveler is arrested?

Expansion of Riley to other warrant exceptions



U.S. Immigration  
and Customs  
Enforcement

## *U.S. v. Kim*

- IIEPPA & AECA & ITSR chargesSearch done entirely in Ninth CircuitSearch limited to allocated space onlyHolding:Reasonable suspicion for past criminal activity is not sufficientDegree to which search intruded on privacy outweighed need for promotion of legitimate governmental interests (outbound v. inbound)Limited to “unique circumstances of this case”



# IOE

## Injunctive Relief & the ACLU

- *Abidor v. Napolitano, E.D.N.Y. House v. Napolitano, D. Mass*



U.S. Immigration  
and Customs  
Enforcement



# ICIE

## DHS Policies

- Congressional Interest Timeframes  
Training Supervisory Review  
Reasonable Suspicion



U.S. Immigration  
and Customs  
Enforcement

# ICE

## DHS Policies (cont.)

- 2009 Policies Privacy Impact Assessment  
Civil Rights and Civil Liberties Impact Assessment  
Coordination between CBP & ICE policies Publicly available



U.S. Immigration  
and Customs  
Enforcement

## Levels of Suspicion

- Search No suspicion necessary  
Assistance Technical Assistance  
Subject Matter Assistance



# ICE

## Timeframes

- Reasonable Period of Time Assistance



U.S. Immigration  
and Customs  
Enforcement

2020-ICLI-00013 312

# ICE

## Sharing

(b)(5)

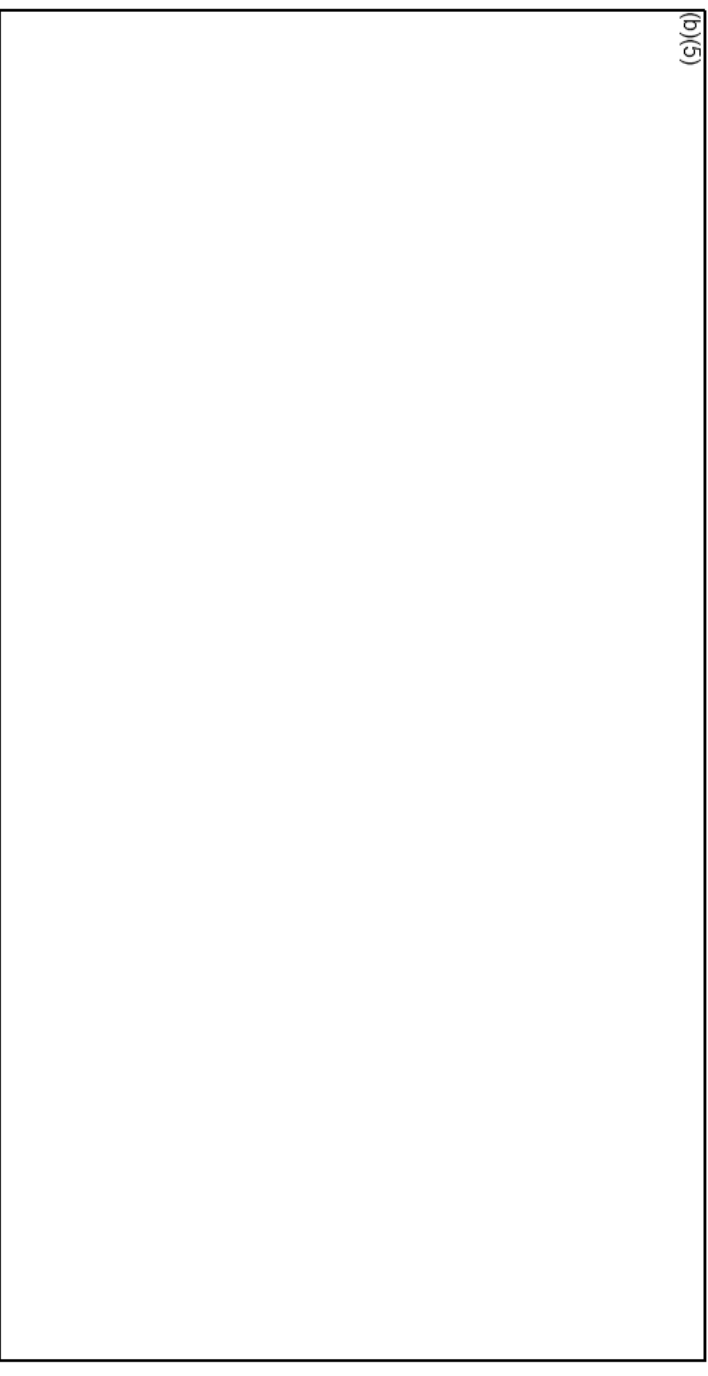


U.S. Immigration  
and Customs  
Enforcement

# ICE

## Remotely Stored Information

(b)(5)

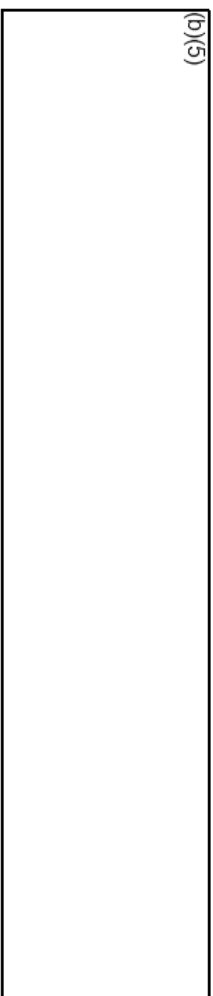


U.S. Immigration  
and Customs  
Enforcement

# ICE

## **Fifth Amendment & Electronic Devices**

(b)(5)



U.S. Immigration  
and Customs  
Enforcement

## **Fifth Amendment & Electronic Devices (cont.)**

- (b)(5)





## Electronic Communications Privacy Act

- Electronic Communications Privacy Act of 1986 (“ECPA”) is comprised of the Stored Communications Act, the Pen Register Statute, and amendments to the Wiretap Act. Controls the collection and disclosure of content and non-content information related to electronic communications, as well as content that has been stored remotely.



# ICE

## Electronic Communications Privacy Act

- Title I of ECPA – Wiretap Act Title II of ECPA – Stored Communications Act Title III of ECPA – Pen register and trap and trace devices



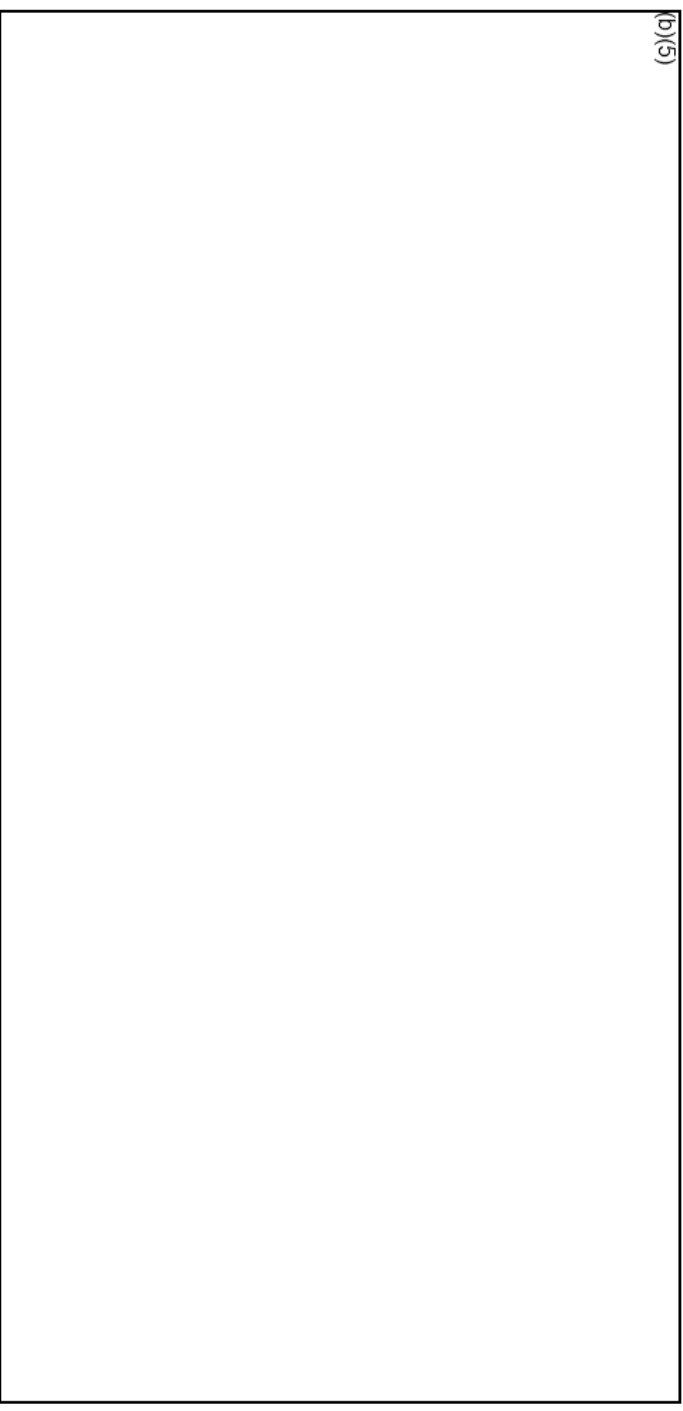
U.S. Immigration  
and Customs  
Enforcement



# ICE

## Title II – Stored Communications Act

(b)(5)

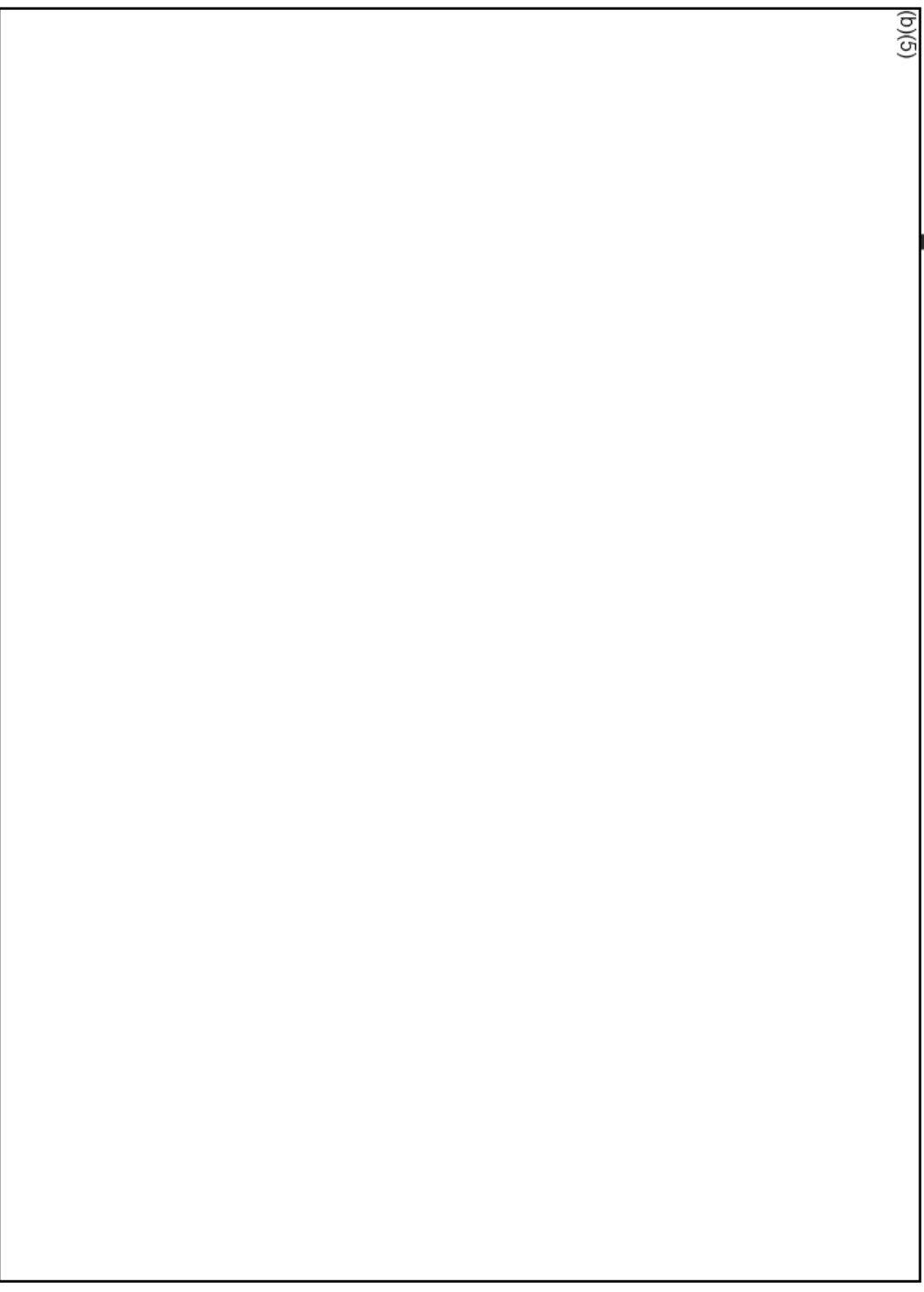


U.S. Immigration  
and Customs  
Enforcement

# ICE

## Title III – Pen Register and Trap and Trace Devices

(b)(5)



U.S. Immigration  
and Customs  
Enforcement

# ICE

## Cell Phone Location Data

(b)(5)



U.S. Immigration  
and Customs  
Enforcement

# ICE

## Title III – Penalties

- Suppression (18 USC § 2515) Criminal – fines & jail (18 USC § 2511(4) & (5)) Civil: Compensatory and punitive damages Attorneys fees Against individual or agency 18 USC § 2520



U.S. Immigration  
and Customs  
Enforcement

**From:**

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

**Sent:**

20 May 2016 18:38:43 +0000

**To:**

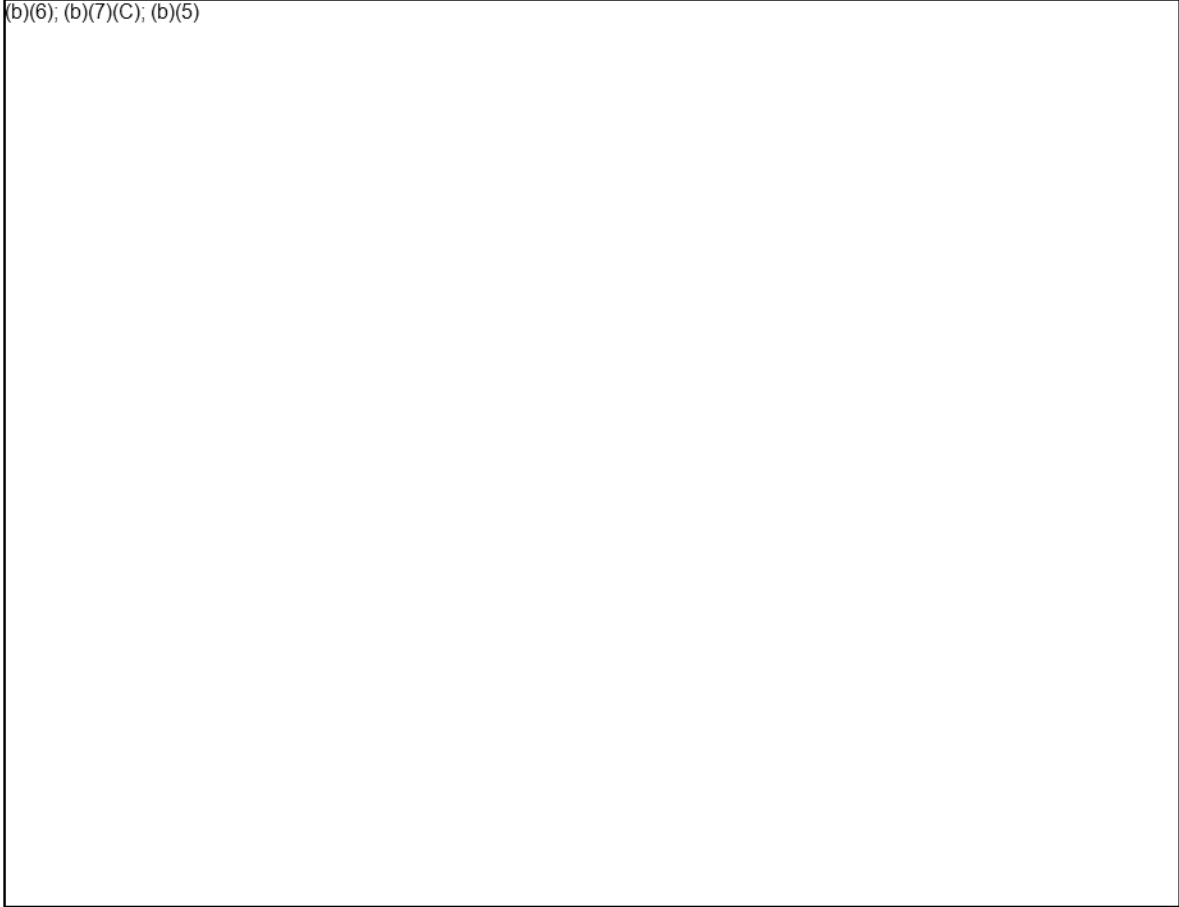
(b)(6); (b)(7)(C)

**Subject:**

Border Search suppression motions

Team,

(b)(6); (b)(7)(C); (b)(5)





**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Aug 2016 10:16:29 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** (b)(6); (b)(7)(C) defense motions re search warrants

Good morning,

Judge Bredar denied the motion to suppress the border search on Thursday August 11, 2016. Not sure if he will issue an opinion.

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

Sent with Good (www.good.com)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, May 18, 2016 4:19:07 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Re: (b)(6); (b)(7)(C) defense motions re search warrants

Oh, got it. With other border search issues, DOJ's National Security Division has gotten involved. I wasn't sure if they were reviewing here as well. I'll get you our comments (with input from CBP OCC) by tomorrow morning. Sorry for the delay.

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) Desk  
202-536-(b)(6); (b)(7)(C) Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, May 18, 2016 4:18 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

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

(b)(5)

Thanks,

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

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, May 18, 2016 4:14 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

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

(b)(5)

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732- (b)(6); (b)(7)(C) (Desk)  
202-536- (b)(6); (b)(7)(C) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 4:01 PM

**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

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

I would appreciate the brief and holding in Kolsuz.

Thanks,

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

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

Assistant United States Attorney  
United States Attorney's Office, District of Maryland/36 S. Charles Street, Fourth Floor/Baltimore, MD 21201  
(desk) 410-209-4600/(cell) 410-908-6000 (fax) 410-962-3091  
[Ayn.Ducao@usdoj.gov](mailto:Ayn.Ducao@usdoj.gov)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 3:57 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(5)

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-6000 (b)(6); (b)(7)(C) Desk)  
202-536-6000 (b)(6); (b)(7)(C) Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE~~

ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 3:23 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(6); (b)(7)(C); (b)(5)

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

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 1:55 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

Thank (b)(6); (b)(7)(C) - please let us know what we can do to help with the reply brief.

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (Desk)  
202-536-(b)(7)(C) (Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 12:10 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(6);  
(b)(7)(C) just reached out to me on this, so I don't know if the AUSA has drafted her  
reply. (b)(6); (b)(7)(C) copied on this email and can fill us in.

Sent with Good ([www.good.com](http://www.good.com))

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 12:02:43 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

Thank (b)(6); (b)(7)(C) Did you already reach out to the AUSA? Can I contact (b)(6); (b)(7)(C) directly (or can you put me in touch with her) so that we can review the draft responses?

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) (Desk)  
202-536-(b)(6); (b)(7)(C) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 11:33 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

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

Sent with Good ([www.good.com](http://www.good.com))

(b)(6); (b)(7)(C)  
**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 11:16:52 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: (b)(6); (b)(7)(C) defense motions re search warrants

Sorry I didn't send this early. I've been so unbelievably busy.

-----Original Message-----

From: (b)(6); (b)(7)(C)  
Sent: Monday, May 09, 2016 12:48 PM  
To: (b)(6); (b)(7)(C)  
Subject: (b)(6); (b)(7)(C) defense motions re search warrants  
(b)(6); (b)(7)(C)

Attached are the defense motions that we discussed this morning.


Thanks,

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

**ICE**  
Title III  
Training

**Electronic  
Surveillance**

(b)(6); (b)(7)(C)  
Criminal Law Section  
October 2018



---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Introduction to  
Electronic Surveillance**

- (b)(5)



---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Introduction to  
Electronic Surveillance**

- (b)(5)
- 



---

---

---

---

---

---


---

---

**ICE**

Title III  
Training

TITLE III BACKGROUND AND  
STATUTORY AUTHORITY




---

---

---

---

---

---

---


---

**ICE**

Title III  
Training

**Statutory History of TIII**

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Wiretap Act”)
- Electronic Communications Privacy Act of 1986 (ECPA)
- Communications Assistance for Law Enforcement Act of 1994 (CALEA)




---

---

---

---

---

---

---


---

**ICE**

Title III  
Training

**Statutory Authority**

- Interception of Communications (Title III) – 18 U.S.C. §§ 2510-2522
- Stored Wire and Electronic Communications and Transactional Records Access – 18 U.S.C. §§ 2701-2711 (Part of the ECPA)
- Pen Registers and Trap and Trace Devices – 18 U.S.C. §§ 3121-3127




---

---

---

---

---

---

---

---



# ICE

Title III  
Training



## Title III – 18 U.S.C. §§ 2510-2522

Live Communications

- 2510 – Definitions
- 2511 – Unlawful to Intercept & Disclose
- 2516 – Authorization for Interception
- 2517 – Authorization for Disclosure
- 2520 – Civil Action

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III – 18 U.S.C. § 2516

- Court authorization required for:
  - Interception, disclosure, or use
  - Of content
  - Of any wire, oral, or electronic communication

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III – 18 U.S.C. § 2510

- Intercept
- Device
- Wire Communication
- Oral Communication
- Electronic Communication

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definitions – Intercept

A communication is 'intercepted' if a device is used by a third party to acquire any information concerning the substance, purport or meaning (i.e., the "content") of that communication.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definitions – Device

- A 'device' is anything that does the job of acquiring the content of any wire, oral, or electronic communication.
- Some devices are specifically excluded
  - Hearing Aids

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definition – Wire Communication

- Any communication
- the human voice travels
- in whole or part
- by means of a wire, cable, or other like connection provided by a communications facility
- interstate or foreign commerce.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definition – Oral Communication

- Any speaking
- other than a wire or electronic communication
- in which the speaker exhibits a reasonable expectation of privacy in that speaking.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definition – Electronic Communication

- Any communication
- other than a wire or oral communication
- in which anything is transmitted
- in whole or in part
- by a wire, radio, electromagnetic, photo-electronic or photo-optical system
- affecting interstate or foreign commerce.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Authorization Rules

### Electronic

- AUSA may approve
- May be made in connection with any federal felony investigation

### Wire/Oral

- Requires AG approval
- May be made only in connection with investigations of certain predicate offenses

---

---

---

---

---

---

---

---

**ICE**

**Title III Training**

U.S. Immigration and Customs Enforcement

**Predicate Offenses**

- 18 USC § 115 (Retaliation Against a Federal Official)
- 18 USC § 659 (Theft from Interstate Shipment)
- 18 USC § 1963 (RICO)
- 18 USC §§ 2251-52 (Sexual Exploitation of Children)
- 18 USC § 201 (Bribery of a Public Official)
- 18 USC §§ 1956-57 (Money Laundering)
- 18 USC § 2332d (Financial Transactions with Certain Governments)
- 22 USC § 2778 (AECA)
- 31 USC 5322 (Monetary Instruments Reporting)
- Any Drug Importation
- Conspiracy to Violate any of these statutes

---

---

---

---

---

---

---

---

---

---

---

**ICE**

**Title III Training**

U.S. Immigration and Customs Enforcement

**Disclosure & Use by ICE**

Lawfully obtained – Disclosure by ICE (sharing)

- Communications & “other offense evidence” to other agents for criminal investigative purposes
- Communications during testimony / oath
- Foreign intelligence info to other LEOs for official purposes

Lawfully obtained – Use by ICE

- Contents for criminal investigative purposes
- “Other offense evidence”

---

---

---

---

---

---

---

---

---

---

---

**ICE**

**Title III Training**

U.S. Immigration and Customs Enforcement

**Title III – Penalties**

- Suppression (18 USC § 2515)
- Criminal – fines & jail (18 USC § 2511(4) & (5))
- Civil:
  - Compensatory and punitive damages
  - Attorneys fees
  - Against individual or agency
  - 18 USC § 2520

---

---

---

---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Stored Communications  
and Records –  
18 U.S.C. §§ 2701-2712**

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



---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Pen Registers / Trap and  
Trace –  
18 U.S.C. §§ 3121-3127**

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



---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Stingray/Trigger Fish  
Devices**

- Determines location of cellular telephone
- Assists in identifying user of cellular telephone
- Obtain search warrant



---

---

---

---

---

---


---

---

**ICE**

Title III  
Training

**TECHNICAL OPERATIONS'  
ROLE  
IN TITLE III PROCESS**




---

---

---

---

---

---

---


---

**ICE**

Title III  
Training

**Technical Operations**

- The mission of ICE Technical Operations is to provide the field agents (ICE-Wide) with the most innovative cutting edge electronic surveillance equipment and support in furtherance of ICE investigations and national security operations.
- Manages all technical surveillance national initiatives
- Research and development of emerging technologies
- Develop ICE technical surveillance policy and procedures
- Oversee the procurement of all ICE technical surveillance equipment




---

---

---

---

---

---

---


---

**ICE**

Title III  
Training

**Title III Program**

- Located within Operational Technology and Cyber, Technical Operations and Systems Development in Lorton, VA
- Technical Operations consists of HSI Special Agents, Technical Enforcement Officers, and Mission Support Specialists
- Annual budget of \$20+ million
  - Title III Monitor Contract
  - Telecommunications Intercept Fees




---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III Program

- Program established in 2002 creating a centralized point of contact
- Provide Support to Field Offices
  - Facilitate ELSUR Record Checks
  - Provide Go-Bys
  - Streamline the Title III Process
  - National Title III Monitor Contract

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III Funding Requests

- Draft affidavit is submitted by HSI Special Agent to AUSA before the funding request is submitted.
- Funding request memo is submitted from SAC to the Executive Associate Director, HSI.
- The funding request is routed through HSI Domestic Operations to Technical Operations.
- The Technical Operations COTR requests a bid from ICE approved contract monitoring companies.
- Funding approval authority has been delegated to the Unit Chief, Technical Operations.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## OPLA TITLE III REVIEW PROCESS

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III Affidavits

- SAC office sends affidavit to Technical Operations and DOJ Criminal Division, Office of Enforcement Operations (OEO) via the AUSA.
- Technical Operations sends affidavit to OPLA for legal sufficiency review as part of overall approval and funding process.
- OPLA reviews the affidavit for legal sufficiency and works directly with the HSI Special Agent to make necessary revisions.
- Once OPLA is satisfied that the affidavit is legally sufficient, the letter of legal sufficiency is sent to Technical Operations for processing.
- The HSI Special Agent ensures the final version of the affidavit is submitted to the court through the AUSA.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Affidavit: Legal Sufficiency Review

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

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III Affidavit Review Probable Cause

- That "an individual is committing, has committed, or is about to commit a particular offense" AND
- That "particular communications concerning that offense will be obtained through such interception."

---

---

---

---

---

---

---

---




**ICE**  
Title III Training

**Title III Affidavit Review  
Probable Cause**

- Factors courts consider:
  - Type of crime
  - Length of criminal activity
  - Nature of object of search
  - Staleness

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




---

---

---

---

---

---


---

---

**ICE**  
Title III Training

**Title III Affidavit Review  
Necessity**

- Full and Complete Statement  
OR
- Minimum "other investigative procedures have been tried and failed; appear unlikely to succeed; or, are too dangerous"




---

---

---

---

---

---

---


---

**ICE**  
Title III Training

**California Wiretaps**

- Not Title III (CA statute)
- Less formal review process
- Less stringent probable cause requirement

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




---

---

---

---

---

---

---

---

**ICE**

Title III  
Training



### TIII – Emergency Interceptions

- Emergency situation
  - Purpose
  - Determination
- Process to obtain emergency TIII
  - Case agent/SAC
  - Coordination with AUSA and DOJ

---

---

---

---

---

---

---

---

**ICE**

Title III  
Training



### Resources

- What reference materials will I need?
- Submitting Affidavits to Tech Ops at HSI HQ
- Who are the CLS POCs?
  - [OPLA-CLS@ICE.DHS.GOV](mailto:OPLA-CLS@ICE.DHS.GOV)

---

---

---

---

---

---

---

---

**From:**

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

**Sent:**

2 Dec 2016 18:24:30 +0000

**To:**

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

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

**Cc:**

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

**Subject:**

7CTA case; U.S. v. Patrick

(b)(5)

[Redacted content]

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732- (b)(6); (b)(7)(C) (office)  
(202) 308- (C) (cell)

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



**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 18:45:41 +0000  
**To:** OPLA-CLS  
**Subject:** Accepted: Cell-Site Simulator Training to TechOps

**From:** (b)(6); (b)(7)(C)  
**Sent:** 26 Sep 2017 13:00:23 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** CSS doc  
**Attachments:** Cell-site simulator response - IMD TechOps IGP 092017.docx

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-73 (b)(6); (b)(7)(C) Desk)  
202-83 (b)(7)(C) Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

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

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

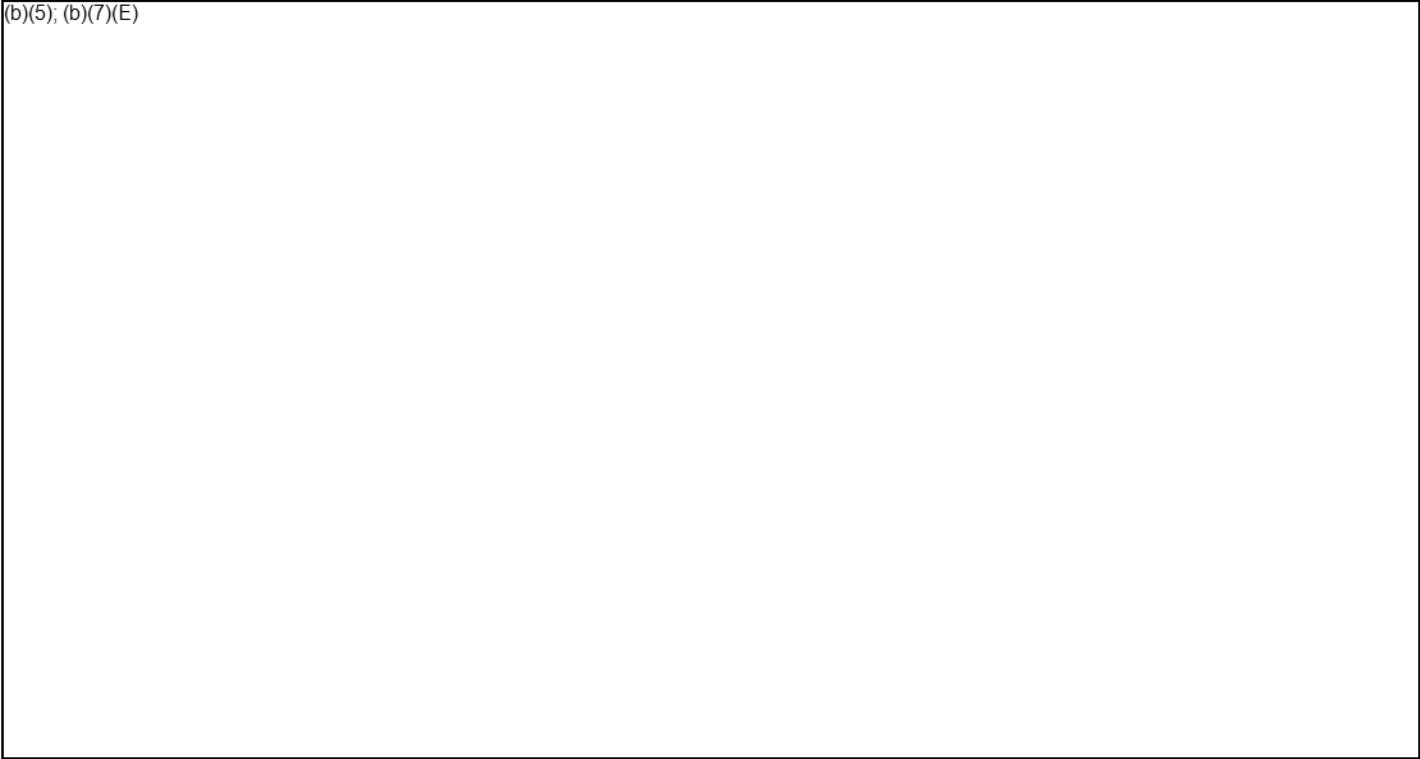
(b)(5); (b)(7)(E)



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

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

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



September 2017



Homeland  
Security

October 19, 2015

POLICY DIRECTIVE 047-02

MEMORANDUM FOR: Sarah Saldaña  
Assistant Secretary  
U.S. Immigration and Customs Enforcement

Joseph Clancy  
Director  
United States Secret Service

R. Gil Kerlikowske  
Commissioner  
U.S. Customs and Border Protection

Admiral Paul F. Zukunft  
Commandant  
United States Coast Guard

Peter Neffenger  
Administrator  
Transportation Security Administration

L. Eric Patterson  
Director  
Federal Protective Service

FROM: Alejandro N. Mayorkas  
Deputy Secretary

A handwritten signature in black ink, appearing to read "AN Mayorkas", written over the printed name of the Deputy Secretary.

SUBJECT: **Department Policy Regarding the Use of Cell-Site  
Simulator Technology**

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 their victims. This policy is being issued in light of the Department of Justice's recent legal analysis of the use of the valuable cell-site simulator technology.

As with any law enforcement capability, the Department of Homeland Security (“DHS” or the “Department”) 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. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data. As technology evolves, DHS must continue to assess its tools to ensure that practice and applicable policies reflect the Department’s law enforcement and national security missions, as well as the Department’s commitments to accord respect for individuals’ privacy and civil liberties.

By this memorandum, I am directing immediate implementation of a DHS-wide policy on the use of cell-site simulator technology. This policy provides guidance and establishes common principles for the use of cell-site simulators across DHS. This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. Affected DHS Components may issue additional specific guidance consistent with this policy.

## **BACKGROUND**

Law enforcement agents can use cell-site simulators to help locate cellular devices the unique identifiers of which 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. This technology is one tool among many traditional law enforcement techniques and is deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

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 device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the 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. This identifying information is, however, limited. 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. Moreover, cell-site simulators used by the Department's law enforcement Components 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 any data contained on the device itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the device. Moreover, cell-site simulators used by the Department's law enforcement Components do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

## **MANAGEMENT CONTROLS & ACCOUNTABILITY**

Department personnel require training and practice to properly operate cell-site simulators. Determinations regarding the appropriate use of this capability always should be informed by technological proficiency and experienced assessments of the suitability of the equipment for any given operation. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. Each Component that uses cell-site simulators shall develop operational policy or procedures to govern the use of this technology consistent with this policy. When developing operational policy or procedures to govern the use of this technology consistent with Department policy, Components will coordinate with the DHS Office of the General Counsel, the Office of Policy, the Privacy Office, and the Office for Civil Rights and Civil Liberties.
2. Department personnel must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their Component to use the technology and whose training has been administered by a qualified Component expert.
3. Within 30 days from the date of this policy, DHS law enforcement Components that use cell-site simulators shall designate an executive-level point of contact at the Component's headquarters office. The point of contact will be responsible for the implementation of this policy and for promoting compliance with its provisions, within his or her area of responsibility.
4. Prior to deployment of the technology, use of a cell-site simulator by the Component must be approved by a first-level supervisor. Any emergency use

of a cell-site simulator must be approved by an appropriate second-level supervisor. Any use of a cell-site simulator on an aircraft must be approved either by a Special Agent in Charge or the executive-level point of contact for the area of responsibility, as described in paragraph 3 of this section.

5. Each Component that uses cell-site simulators shall identify training protocols (including training on privacy and civil liberties) and protocols identifying which officials will have approval authority.

## **LEGAL PROCESS & COURT ORDERS**

The use of cell-site simulators is permitted only as authorized by law and policy. While the Department has, 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, law enforcement Components 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.

As a practical matter, because agents or operators, in consultation with prosecutors, will need to seek authority pursuant to Rule 41 and the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, 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 also must reflect the information noted in the immediately following section of this policy (“Applications for Use of Cell Site Simulators”).

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

### *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 internal approval to use a pen register before using a cell-site simulator. In order to comply with the terms of this policy and with 18 U.S.C. § 3125, the case agent or operator must contact the duty Assistant U.S. Attorney in the local U.S. Attorney's Office, who will coordinate approval within the Department of Justice.<sup>1</sup> Upon approval, the Assistant U.S. Attorney or state or local prosecutor must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125.<sup>2</sup> 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.

#### *Exceptional Circumstances*

There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. For example, potential uses of the technology in furtherance of protective duties pursuant to 18 U.S.C. § 3056 and 18 U.S.C. § 3056A. In these limited circumstances, agents must first obtain approval from executive-level personnel at the Component's headquarters and the relevant U.S. Attorney, who coordinates approval within the Department of 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, if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required (see provisions in *Exigent Circumstances under the Fourth Amendment*, directly above).

---

<sup>1</sup> In 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.

<sup>2</sup> 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, DHS law enforcement personnel must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement personnel must consult with the prosecutors<sup>3</sup> 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.<sup>4</sup>

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 investigators plan to send signals to the cellular phone that will cause it, 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 investigators 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 investigators 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.
3. 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.

---

<sup>3</sup> While this provision typically will implicate notification to Assistant U.S. Attorneys, it also extends to state and local prosecutors when such personnel are engaged in operations involving cell-site simulators.

<sup>4</sup> 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 Department of Justice's Criminal Division. To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS and consult with appropriate agency counsel for compliance with DHS policies.

## DATA COLLECTION & DISPOSAL

DHS is committed to ensuring that law enforcement practices concerning the collection or retention<sup>5</sup> of data are lawful and respect the important privacy interests of individuals. As part of this commitment, DHS's law enforcement Components operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying 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,<sup>6</sup> the Department'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.<sup>7</sup>
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. Components shall implement an auditing program to ensure that the data is deleted in the manner described above. To the extent feasible, this auditing program will include hardware and software controls, for example through an equipment sign-in process that will include operator badge number and an affirmative acknowledgement by the operator that he or she has the proper legal authority to collect and view data.

---

<sup>5</sup> 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.

<sup>6</sup> 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 investigators know or have reason to believe that information is exculpatory or impeaching, they have a duty to memorialize that information.

<sup>7</sup> A typical mission may last anywhere from less than one day and up to several days.

## **STATE AND LOCAL PARTNERS**

The Department 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 Components use cell-site simulators in support of other federal agencies and/or state and local law enforcement agencies.

## **TRAINING AND COORDINATION, AND ONGOING MANAGEMENT**

Each DHS law enforcement Component shall provide this policy, and training as appropriate, to all relevant employees. Periodic review of this policy and training shall be the responsibility of each Component, based upon guidance from DHS oversight offices, with respect to the way the equipment is being used (e.g., significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). Any significant changes in technology or Component information collection, maintenance, use, or retention protocols may also trigger oversight responsibilities, and be reviewed before being implemented accordingly.<sup>8</sup>

Each field office shall report to its Component headquarters annual records 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 in emergency circumstances.<sup>9</sup>

Moreover, it is vital that all appropriate Department attorneys familiarize themselves with the contents of this policy, so that their court filings and disclosures are appropriate and consistent.

## **IMPROPER USE OF CELL-SITE SIMULATORS**

Accountability is an essential element in maintaining the integrity of our Federal law enforcement agencies. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the appropriate Component office that handles such allegations.

---

<sup>8</sup> For example, a significant change in technology could trigger the need for an updated or new privacy impact assessment.

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

## **SCOPE OF THIS POLICY**

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.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 28 Mar 2019 15:33:38 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** can you assist?  
**Attachments:** DTAS Presentation 9.12.18 FLETC.PPTX  
**Importance:** High

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

(b)(5)

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732- (b)(6); (b)(7)(C) office)  
(202) 308- (b)(6); (b)(7)(C) cell)

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



~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL~~

~~GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5  
USC §§ 552(b)(5), (b)(7).~~



**Homeland Security Investigations      Designated  
Technical Agent School (DTAS)      Sept. 12, 2018 -  
FLETC Office of the Principal Legal Advisor  
(OPLA)**

Page 364

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 365

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 366

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 367

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 368

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 369

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 370

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 371

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 372

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 373

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 374

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 375

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 376

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 377

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 378

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 379

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 380

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 381

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 382

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 383

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 384

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 385

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 386

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 387

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 388

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 389

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 390

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 391

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 392

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 393

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 394

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 395

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 396

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 397

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 398

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 399

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 400

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 401

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 402

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 403

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 404

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 405

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 406

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 407

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 408

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 409

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 410

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 411

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 412

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 413

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 414

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 415

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 416

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 417

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 418

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 419

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 420

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 421

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 422

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 423

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 424

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 425

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 426

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 427

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 428

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 429

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 430

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 431

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 432

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 433

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 434

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 435

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 436

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 437

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 438

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 439

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 440

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 441

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 442

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 443

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 444

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 445

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 446

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 447

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

# Office of the Principal Legal Advisor (OPLA)

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

[Redacted]

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

[Redacted]



Homeland  
Security  
Investigations

~~OPLA HSIIID - Criminal Law Section~~

~~Law Enforcement Sensitive~~

2020-ICLI-00013 448

**From:** OPLA-CLS  
**Sent:** 24 May 2017 17:24:18 -0400

**To:** (b)(6); (b)(7)(C)

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

**Subject:** Cell-Site Simulator Training to (b) (7)(E)  
**Attachments:** Cell-Site Simulator training to the client

Tech Ops just updated its agenda and OPLA will be presenting in the afternoon now.



**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 18:39:16 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Cell-Site Simulator training to the client

(b) (7)(E) Team,

We have been asked to provide an hour long training on ICE's cell-site simulator policy on behalf of (b) (7)(E) to its field TEOs. There are four sessions that will be held this summer at the Lorton VA facility. After discussing with (b)(6); (b)(7)(C) the following was decided:

On Thursday May 25<sup>th</sup>, from 11-12, all of the Tech Ops team will travel to Lorton and watch me give the presentation on cell-site simulators.  
On Thursday, June 8<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.  
On Thursday June 26<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.  
On Thursday July 27<sup>th</sup>, from 11-12, either (b)(6); (b)(7)(C) will give the presentation, and it can be left to the two of you to decide who will go.

I believe the presentation and policy is on the S:Drive, and if it isn't, I will make sure it is this afternoon. Please let me know if you have any questions or comments, calendar invites will be forthcoming.

Sincerely,

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-73 (b)(6); (b)(7)(C) (office)  
202-50 (b)(7)(C) (mobile)

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

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 18:16:41 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** cell-site  
**Attachments:** Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf

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

I've attached the DHS policy for cell-site.

(b)(6); (b)(7)(C); (b)(5)

I'll stop by to touch base as well,

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732- (b)(6); (b)(7)(C) office)  
(202) 308- (b)(6); (b)(7)(C) cell)

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



~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~



**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 20:41:11 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: (b)(5); (b)(6) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(5); (b)(6) Tracking Warrant + (b)(5); (b)(6) Cir. decision)  
**Attachments:** Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf, Tracking Warrant - (b)(6); (b)(7)(C) pdf, (b)(5); (b)(6) -opn[1].pdf

FYSA

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 4:38 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** (b)(5); (b)(6) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(5); (b)(6) Cir. decision)

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

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

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

(b)(5); (b)(6); (b)(7)(C)

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

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732-(b)(6); (w)  
202-904-(b)(7)(c)

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

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

Page 455

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 456

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 457

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 458

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 459

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 460

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 461

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 462

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 463

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 464

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 465

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 466

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 467

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 468

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 469

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 470

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 471

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 472

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 473

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 474

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 475

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 476

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 477

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 478

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 479

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 480

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 481

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

**From:** OPLA-CLS  
**Sent:** 9 Jun 2017 11:11:44 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: query - CLS SME re Cell Site Simulator  
**Attachments:** 12-2258\_opn[1].pdf

Good Morning,

Please note the email below from (b)(6); (b)(7)(C) to the CLS inbox seeking guidance on the use of cell site simulator technology. Recommend someone from (b) (7)(E) team provide assistance.

Best,

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) office)  
202-494-(b)(6); (b)(7)(C) mobile)

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

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 10:41 AM  
**To:** OPLA-CLS  
**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5)

(b)(5)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you

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

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

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (w)  
202-904-(b)(7)(c)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 20 Jul 2016 11:32:57 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: [CCIPS Electronic Evidence Tips] Cell-site simulators  
**Attachments:** 9.3.15 Final Issued Cell Site Simulator Guidance.pdf, Cell-site simulator canvassing warrant go-by 2015 09 10.docx, Cell-site simulator locating warrant go-by 2015 09 10.docx

(b)(6); (b)(7)(C)  
Assistant Chief Counsel  
Office of the Chief Counsel - Orlando  
U.S. Immigration and Customs Enforcement  
U.S. Department of Homeland Security  
13077 Veveras Drive #213A  
Jacksonville, Florida 32258  
(904) 288 (b)(6); (b)(7)(C) Office)  
(202) 436 (b)(6); (b)(7)(C) Cell)  
(b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, June 22, 2016 3:44 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: [CCIPS Electronic Evidence Tips] Cell-site simulators

(b)(6); (b)(7)(C)  
Assistant Chief Counsel  
Office of the Chief Counsel - Orlando  
U.S. Immigration and Customs Enforcement  
U.S. Department of Homeland Security  
13077 Veveras Drive (b)(6);  
Jacksonville, Florida 32258  
(904) 288 (b)(6); (b)(7)(C) Office)  
(202) 436 (b)(6); (b)(7)(C) Cell)  
(b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its~~



---

**From:** CCIPS Tips [mailto:CCIPS.Tips@usdoj.gov]  
**Sent:** Tuesday, April 26, 2016 1:25 PM  
**To:** CCIPS Tips  
**Subject:** [CCIPS Electronic Evidence Tips] Cell-site simulators

# CCIPS Electronic Evidence Newsletter

*Cell-site simulators (April 2016)*

## Go-by of the Month

Attached are two go-bys for affidavits in support of search warrants that authorize the use of a cell-site simulator. The first go-by is designed to be used when law enforcement intends to utilize the cell-site simulator to locate a cellular phone or device whose unique identifiers are already known to law enforcement. The second go-by is designed to be used when law enforcement intends to utilize the cell-site simulator to determine the unique identifiers assigned to a particular phone or device.

Also attached is a copy of the Department of Justice's policy regarding the use of cell-site simulator technology, which is discussed in more detail below.

## Practice Tip

Cell-site simulators are mobile devices that law enforcement agents can use to locate a cellular device whose unique identifiers are already known to law enforcement or to determine the identifiers of an unknown device. As part of their normal operations, cellular devices seek to connect to the cell tower that offers the strongest signal, and devices thus regularly scan for signals transmitted by cell towers in order to identify the best tower to which to connect. Once it identifies the tower with the strongest signal, a cellular device transmits its unique identifiers - assigned either by the device manufacturer or the device's wireless provider - to that cell tower to register with it and thus to connect to the cellular network. Cell-site simulators mimic cell towers; in response to signals emitted by the simulator, the cellular devices in the proximity of the cell-site simulator identify the simulator as the cell tower with the strongest signal in the area. Those devices thus transmit their unique identifiers to the cell-site simulator in the same way that they would with a networked tower. Cell-site simulators can also provide the relative signal strength and general direction from which a target cellular device emitted signals. Cell-site simulators used by the Department must be configured as pen registers and thus cannot be used to collect the contents of any communication.

In September 2015, the Department of Justice promulgated a policy, which applies both to its investigative agencies and prosecutors, relating to the use of cell-site simulator technology. Among other things, the policy requires that a search warrant be obtained prior to the use of a cell-site simulator except (1) when there are exigent circumstances or (2) in very limited circumstances in which the law does not require a warrant, approval is first obtained from the relevant U.S. Attorney and a Criminal Division Deputy Assistant Attorney General, and the

provisions of the Pen Register Statute are complied with. Furthermore, because the information collected by a cell-site simulator constitutes dialing, routing, addressing, and signaling information for purposes of the Pen Register Statute, the policy also requires that the search warrant contain all the information that must be included in pen-trap order pursuant to 18 U.S.C. 3123(b) or that a pen-trap order be obtained concurrently with the search warrant. In addition, the policy requires that any application to a court seeking authorization to use a cell-site simulator state: (1) a description, in general terms, of the way that cell-site simulators collect information from cellular devices and the purpose for which the simulator will be used (i.e. to locate or identify a target device); (2) that cellular devices in proximity to the cell-site simulator might experience a temporary disruption of cellular service; and (3) how law enforcement intends to address deletion of data not associated with the target phone. Finally, the policy establishes requirements applicable to DOJ investigative agencies pertaining to, inter alia, agency approvals that must be obtained prior to using cell-site simulators, deletion of data, and reporting about the use of cell-site simulators.

## Key Case

*Magistrate Judge Refuses to Sign Pen/Trap Order that Would Authorize the Use of a Cell-Site Simulator.* In *In re Application of the U.S.*, 890 F.Supp.2d 747 (S.D.Tex. 2012), the magistrate judge was presented with an application for a pen-trap order that would have authorized the use of a cell-site simulator to identify the cellular phone being used by the target of an investigation. The magistrate denied the application. As an initial matter, the magistrate criticized the government's application for failing to "explain the technology, or the process by which the technology will be used to engage in electronic surveillance to gather the Subject's cell phone number" and for failing to "address what the government would do with the cell phone numbers and other information concerning seemingly innocent cell phone users whose information was recorded by the equipment." More significantly, the magistrate reasoned that the government could not rely upon the Pen Register Act when seeking to identify an unknown phone using a cell-site simulator because the government cannot provide a phone number or other numerical identifier associated with the target phone, which the magistrate believed must be included in a pen-trap order pursuant to 18 U.S.C. 3123(b). Citing to *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012), the magistrate judge also suggested that cell-site simulators are mobile tracking devices for which warrants are required.

CCIPS' Take: As this opinion demonstrates, some judges feel that a pen-trap order is insufficient to authorize the use of a cell-site simulator. By generally requiring the use of a warrant, the Department's policy minimizes the litigation risk associated with the use of cell-site simulators.

---

*This newsletter is a publication of the Computer Crime and Intellectual Property Section, in the Department of Justice's Criminal Division. If you would like additional guidance on electronic evidence issues, you can:*

- Consult the go-bys and guidance available on CCIPS Online at <http://dojnet.doj.gov/criminal/ccips/online/evidence.htm> (this link will work only if you can connect to the DOJ intranet);

- *Consult the the CCIPS manual on Searching and Seizing Computers and Obtaining Electronic Evidence, which is publicly available at <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>.*
- *Call the CCIPS duty attorney at (202) 514-1026.*

*To subscribe or unsubscribe to future newsletters, please email [CCIPS.Tips@usdoj.gov](mailto:CCIPS.Tips@usdoj.gov). Unless there is a problem or question about your subscription request, you will not receive a confirmation email. This email list is restricted to federal prosecutors and federal law enforcement agents, and you must use a federal government email address to subscribe.*



U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General


Washington, D.C. 20530

September 3, 2015

MEMORANDUM FOR HEADS OF LAW ENFORCEMENT COMPONENTS

ALL UNITED STATES ATTORNEYS

FROM:

Sally Quillian Yates   
Deputy Attorney General

SUBJECT:

Department Policy Regarding the  
Use of Cell-Site Simulator Technology

The attached document establishes policy for the Department of Justice regarding the use of cell-site simulator technology. This technology supports critical public safety objectives, such as apprehending fugitives, locating kidnapping victims, and assisting in drug investigations. As with other technological tools, cell-site simulators must be used effectively and in accordance with the law. The attached document establishes consistent policy for the legal process that must be obtained for use of this technology, the information that must be provided to courts in connection with seeking court authority, handling and deletion of data collected by cell-site simulators, and various management and training requirements. The new policy will enhance transparency and accountability, improve our training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this technology.

I ask that you ensure that this policy is shared with all relevant personnel and that appropriate steps are taken to provide the necessary training and ensure compliance with the policy. Any questions regarding this policy should be directed to (b)(6); (b)(7)(C) Office of the Deputy Attorney General, at (202) 514-(b)(6);

Attachment

## **Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology**

---

Cell-site simulator technology provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child, cell-site simulators fulfill critical operational needs.

As with any law enforcement capability, the Department 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. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data.

As technology evolves, the Department must continue to assess its tools to ensure that practice and applicable policies reflect the Department's law enforcement and national security missions, as well as the Department's commitments to accord appropriate respect for individuals' privacy and civil liberties. This policy provides additional guidance and establishes common principles for the use of cell-site simulators across the Department.<sup>1</sup> The Department's individual law enforcement components may issue additional specific guidance consistent with this policy.

### ***BACKGROUND***

Cell-site simulators, on occasion, have been the subject of misperception and confusion. To avoid any confusion here, this section provides information about the use of the equipment and defines the capabilities that are the subject of this policy.

#### *Basic Uses*

Law enforcement agents can 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. This technology is one tool among many traditional law enforcement techniques, and is deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

---

<sup>1</sup> This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. When acting pursuant to the Foreign Intelligence Surveillance Act, Department of Justice components will make a probable-cause based showing and appropriate disclosures to the court in a manner that is consistent with the guidance set forth in this policy.

### *How They Function*

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 device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the 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 phone. 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.

### *What They Do and Do Not Obtain*

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department 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 any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

### **MANAGEMENT CONTROLS AND ACCOUNTABILITY<sup>2</sup>**

Cell-site simulators require training and practice to operate correctly. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. Department personnel must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their agency to use the technology and whose training has been administered by a qualified agency component or expert.

---

<sup>2</sup> This policy guidance is intended only to improve the internal management of the Department of Justice. It 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.

2. Within 30 days, agencies shall designate an executive-level point of contact at each division or district office responsible for the implementation of this policy, and for promoting compliance with its provisions, within his or her jurisdiction.
3. Prior to deployment of the technology, use of a cell-site simulator by the agency must be approved by an appropriate individual who has attained the grade of a first-level supervisor. Any emergency use of a cell-site simulator must be approved by an appropriate second-level supervisor. Any use of a cell-site simulator on an aircraft must be approved either by the executive-level point of contact for the jurisdiction, as described in paragraph 2 of this section, or by a branch or unit chief at the agency's headquarters.

Each agency shall identify training protocols. These protocols must include training on privacy and civil liberties developed in consultation with the Department's Chief Privacy and Civil Liberties Officer.

### ***LEGAL PROCESS AND COURT ORDERS***

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

As a practical matter, because prosecutors will need to seek authority pursuant to Rule 41 *and* the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, 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 also must reflect the information noted in the immediately following section of this policy ("Applications for Use of Cell-Site Simulators").

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 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. In addition, the operator must obtain the requisite internal approval to use a pen register before using a cell-site simulator. In order to comply with the terms of this policy and with 18 U.S.C. § 3125,<sup>3</sup> the operator must contact the duty AUSA in the local U.S. Attorney's Office, who will then call the DOJ Command Center to reach a supervisory attorney in the Electronic Surveillance Unit (ESU) of the Office of Enforcement Operations.<sup>4</sup> Assuming the parameters of the statute are met, the ESU attorney will contact a DAAG in the Criminal Division<sup>5</sup> and provide a short briefing. If the DAAG approves, the ESU attorney will relay the verbal authorization to the AUSA, who must also 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.

## 2. Exceptional Circumstances Where the Law Does Not Require a Warrant

There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. In such cases, which we expect to be very limited, agents must first obtain approval from executive-level personnel at the agency's headquarters and the relevant U.S. Attorney, and then from a Criminal Division DAAG. The Criminal Division shall keep track of the number of times the use of a cell-site simulator is approved under this subsection, as well as the circumstances underlying each such use.

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,

---

<sup>3</sup> 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).

<sup>4</sup> In non-federal cases, the operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

<sup>5</sup> In requests for emergency pen authority, and for relief under the exceptional circumstances provision, the Criminal Division DAAG will consult as appropriate with a National Security Division DAAG on matters within the National Security Division's purview.



if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required (see provisions in section 1 directly above).

### ***APPLICATIONS FOR USE OF CELL-SITE SIMULATORS***

When making any application to a court, the Department's lawyers and law enforcement officers must, as always, disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement agents must consult with prosecutors<sup>6</sup> 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.<sup>7</sup>

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 investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators 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 might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.
3. 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 phone. 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.

---

<sup>6</sup> While this provision typically will implicate notification to Assistant United States Attorneys, it also extends to state and local prosecutors, where such personnel are engaged in operations involving cell-site simulators.

<sup>7</sup> 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 Criminal Division. To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS, which will coordinate with appropriate Department components.

## ***DATA COLLECTION AND DISPOSAL***

The Department is committed to ensuring that law enforcement practices concerning the collection or retention<sup>8</sup> of data are lawful, and appropriately respect the important privacy interests of individuals. As part of this commitment, the Department's law enforcement agencies operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying 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,<sup>9</sup> the Department's use of cell-site simulators shall include the following practices:

1. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.
2. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days.
3. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

Agencies shall implement an auditing program to ensure that the data is deleted in the manner described above.

## ***STATE AND LOCAL PARTNERS***

The Department often works closely with its State and Local law enforcement partners and provides technological assistance under a variety of circumstances. This policy applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies.

## ***TRAINING AND COORDINATION, AND ONGOING MANAGEMENT***

Accountability is an essential element in maintaining the integrity of our Federal law enforcement agencies. Each law enforcement agency shall provide this policy, and training as appropriate, to all relevant employees. Periodic review of this policy and training shall be the

---

<sup>8</sup> 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.

<sup>9</sup> 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 investigators know or have reason to believe that information is exculpatory or impeaching they have a duty to memorialize that information.

responsibility of each agency with respect to the way the equipment is being used (*e.g.*, significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). We expect that agents will familiarize themselves with this policy and comply with all agency orders concerning the use of this technology.

Each division or district office shall report to its agency headquarters annual records 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 in emergency circumstances.

Similarly, it is vital that all appropriate Department attorneys familiarize themselves with the contents of this policy, so that their court filings and disclosures are appropriate and consistent. Model materials will be provided to all United States Attorneys' Offices and litigating components, each of which shall conduct training for their attorneys.

\* \* \*

Cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives. As with other capabilities, the Department must always use the technology in a manner that is consistent with the Constitution and all other legal authorities. This policy provides additional common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way.

# WARRANT FOR THE USE OF A CELL-SITE SIMULATOR TO OBTAIN IDENTIFIERS OF A CELL PHONE OR OTHER CELLULAR DEVICE AT PARTICULAR LOCATIONS (“CANVASSING”)

THIS GO-BY IS CURRENT AS OF SEPTEMBER 2015. TO GET THE MOST CURRENT VERSION OF THIS GO-BY AND THE LATEST GUIDANCE, VISIT CCIPS ONLINE:

<http://dojnet.doj.gov/criminal/ccips/online/location.htm>

For help with any issues involving the search and seizure of computers, cell phones, and electronic evidence, call the Computer Crime and Intellectual Property Section (“CCIPS”), Criminal Division, United States Department of Justice, at (202) 514-1026.

## USAGE NOTES:

- Use this go-by to enable law enforcement to use its own cell-site simulator equipment (sometimes called “triggerfish” or “stingray”) to collect signals emitted by wireless phones or other cellular devices and use these signals only to determine the identifiers of a particular person’s cellular device. This order should not be served on a provider.
- For Departmental policy regarding use cell-site simulators, please refer to the September 3, 2015, memorandum *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* available on CCIPS online.
- Because a cell-site simulator falls within the statutory definitions of a “pen register” or a “trap and trace device,” see 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. The warrant therefore includes all the information required to be included in a pen register order. See 18 U.S.C. § 3123(b)(1). In addition, an attorney for the government should complete an AO 106 Application for a Search Warrant as specified below to comply with the application requirements of 18 U.S.C. § 3123 for a pen register order.
- To the extent possible, configure the equipment so that it collects information from as few cellular devices as practical.
- Be sure to follow the procedures described in the application for limiting additional uses of the data collected.
- This go-by is intended to be used with a standard AO 93 Search Warrant form. Do NOT use the AO 102 Application for a Tracking Warrant. Fill out your district’s AO 93 Search Warrant form this way:

1. Caption the warrant “In the Matter of the Use of a Cell-Site Simulator to Identify the Cellular Device Used by [[suspect]].” To caption the warrant in this manner, strike out “the Search of” in the existing caption of the AO 93.
  2. Below the parenthetical that asks you to “identify the person or describe the property to be searched and give its location,” write “See Attachment A.”
  3. Below the parenthetical that asks you to “identify the person or describe the property to be seized,” write “See Attachment B.”
  4. The AO 93 form includes spaces for the district in which the property to be searched is located. Rule 41(b) generally requires that the cellular device that you are targeting be in the issuing district either at the time of search, or at the time the warrant is issued. Pursuant to Rule 41(b)(2), investigators may use this technique outside the district provided the cellular device is within the district when the warrant is issued.
  5. Check the box that indicates that “immediate notification may have an adverse result listed in 18 U.S.C. § 2705,” and fill out the appropriate sub-boxes and blanks to indicate the length of delay that you are seeking under 18 U.S.C. § 3103a(b). If you use the standard language contained in this go-by, you should check the first sub-box and indicate the number of days as “30.”
- To ensure compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, an attorney for the government should complete an AO 106 Application for a Search Warrant. *See* 18 U.S.C. §§ 3122(a), 3127(5). In the “The application is based on these facts” box, write: “See Affidavit in Support of an Application for a Search Warrant. To ensure technical compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, this warrant also functions as a pen register order. Consistent with the requirement for an application for a pen register order, I certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [investigative agency]. *See* 18 U.S.C. §§ 3122(b), 3123(b).” Other boxes of the AO 106 should be completed in the same manner as the AO 93.
  - To ensure compliance with the notice requirements of Rule 41, CCIPS recommends giving notice of the warrant to the target of the canvassing operation. However, this notice can be delayed under 18 U.S.C. § 3103a(b). This go-by includes language seeking a 30-day delay of notice under 18 U.S.C. § 3103a(b), which permits notice to be delayed up to 30 days initially as long as certain statutory requirements are satisfied. If you need a longer delay, you can attempt to seek a delay to a “later date certain if the facts of the case justify a longer period of delay,” 18 U.S.C. § 3103a(b)(3), or can seek an extension of the original 30-day delay under 18 U.S.C. § 3103(a)(c).

- Include the following information in the warrant return/inventory: (1) the date and time when the acquisition of identifying information began, and (2) the period during which the government acquired identifying information.

- The Department of Justice Policy issued September 3, 2015, states:

Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (e.g., tradecraft, capabilities, limitations or specifications). ... To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS, which will coordinate with appropriate Department components.

IN THE UNITED STATES DISTRICT COURT  
FOR \_\_\_\_\_

IN THE MATTER OF THE USE OF A  
CELL-SITE SIMULATOR TO IDENTIFY  
THE CELLULAR DEVICE CARRIED BY  
[[SUSPECT]]

Case No. \_\_\_\_\_

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, [AGENT NAME], being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to employ an electronic investigative technique further described in Attachment B, in order to identify the cellular device or devices carried by [[name and/or physical description of the suspect]] (the “Target Cellular Device”), described in Attachment A.

2. I am a Special Agent with the [Agency], and have been since [Date].  
**[DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS  
QUALIFICATION TO SPEAK ABOUT THIS INVESTIGATION, CELLULAR  
DEVICES, AND OTHER TECHNICAL MATTERS].**

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. This Court has authority to issue the requested warrant under Federal Rule of Criminal Procedure Rule 41(b)(1) & (2) because the Target Cellular Device is currently believed to be located inside this district because **[Provide evidence suggesting that Target Cellular Device is currently located in this district, e.g. the Target Cellular Device’s owner is known to spend most of his time in this district; the Target Cellular Device’s owner was seen in this district X days ago; etc.]**. Pursuant to Rule 41(b)(2), law enforcement may use the technique described in Attachment B outside the district provided the device is within the district when the warrant is issued.

5. **[USE THIS PARAGRAPH IF THE UNIQUE IDENTIFIERS ARE EVIDENCE OF A CRIME.]** Based on the facts set forth in this affidavit, there is probable cause to believe that violations of **[statutes]** have been committed, are being committed, and will be committed by **[suspect]**. There is also probable cause to believe that the identity of the Target Cellular Device will constitute evidence of those criminal violations. In addition, in order to obtain additional evidence relating to the Target Cellular Device, its user, and the criminal violations under investigation, law enforcement must first identify the Target Cellular Device. There is probable cause to believe that the use of the investigative technique described by the warrant will result in officers learning that identifying information.

6. Because collecting the information authorized by this warrant may fall within the statutory definitions of a “pen register” or a “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. *See* 18 U.S.C. §§ 3121-3127. This warrant therefore includes all the information required to be included in a pen register order. *See* 18 U.S.C. § 3123(b)(1).



### **PROBABLE CAUSE**

7. **[[Give facts establishing probable cause. At a minimum, it is necessary to establish probable cause to believe that the suspect is likely to be carrying the Target Cellular Device, and that records about that cellular device's use will be pertinent to the investigation. If the Target Cellular Device is being carried by someone who is also a suspect, which will often be the case, then it is likely also necessary to identify the suspect and establish a connection between the suspect and the suspected crime. Also, explain why there is probable cause to collect identifying information for the next thirty days (or for some shorter period of time, if you amend this request to cover a period less than thirty days). If you specify particular locations in Attachment A for use of the technique, establish probable cause to believe that the Target Cellular Device will be present at those locations.]]**

### **MANNER OF EXECUTION**

8. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

9. To facilitate execution of this warrant, law enforcement may use an investigative device that sends signals to nearby cellular devices, including the Target Cellular Device, and in

reply, the nearby cellular devices will broadcast signals that include their unique identifiers. The investigative device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell to communicate with others. Law enforcement will use this investigative device when they have reason to believe that **[[name and/or physical description of the suspect]]** is present. Law enforcement will collect the identifiers emitted by cellular devices in the immediate vicinity of the Target Cellular Device when the subject is in multiple locations and/or multiple times at a common location and use this information to identify the Target Cellular Device, as only the Target Cellular Device's unique identifiers will be present in all or nearly all locations. Once investigators ascertain the identity of the Target Cellular Device, they will cease using the investigative technique. Because there is probable cause to determine the identity of the Target Cellular Device, there is probable cause to use the investigative technique described by the warrant to determine the identity of the Target Cellular Device.

10. The investigative device may interrupt cellular service of cellular devices within its immediate vicinity. Any service disruption will be brief and temporary, and all operations will attempt to limit the interference cellular devices. Once law enforcement has identified the Target Cellular Device, it will delete all information concerning non-targeted cellular devices. Absent further order of the court, law enforcement will make no investigative use of information concerning non-targeted cellular devices other than distinguishing the Target Cellular Device from all other devices.

## AUTHORIZATION REQUEST

11. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed warrant also will function as a pen register order under 18 U.S.C. § 3123.

12. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days from the end of the period of authorized surveillance. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the person carrying the Target Cellular Device would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

13. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to identify the Target Cellular Device outside of daytime hours.

14. **[[If your district does not have standard forms/procedures for filing under seal, you can insert this language in the affidavit:** I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is

neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.]]

15. A search warrant may not be legally necessary to compel the investigative technique described herein. Nevertheless, I hereby submit this warrant application out of an abundance of caution.

Respectfully submitted,

---

**[AGENT NAME]**  
Special Agent  
**[AGENCY]**

Subscribed and sworn to before me  
on \_\_\_\_\_:

---

UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B when the officers to whom it is directed have reason to believe that **[[name and/or physical description of the suspect]]** is present.

**[[Include the following if locations where the technique will be used are readily ascertainable at the time of drafting.]]** This technique may be used at the following locations: **[[List the locations at which you intend to use the canvassing technique. When possible, limit the locations included to the vicinity of precisely described areas. For locations that do not have an immediate, apparent connection to the suspect, it may be helpful to include a reference to why you believe the suspect will be present at the location. For example: the suspect's home (home address); the suspect's place of employment (work address); the suspect's daily commute between his home and place of employment.]]**

## ATTACHMENT B

The “Target Cellular Device” is the cellular device or devices carried by **[[name and/or physical description of the suspect]]**. Pursuant to an investigation of [identify of **subject of investigation**, if known] for a violation of [offense], this warrant authorizes the officers to whom it is directed to identify the Target Cellular Device by collecting radio signals, including the unique identifiers, emitted by the Target Cellular Device and other cellular devices in its vicinity for a period of thirty days, during all times of day and night.

Absent further order of a court, law enforcement will make no affirmative investigative use of any identifiers collected from cellular devices other than the Target Cellular Device, except to identify the Target Cellular Device and distinguish it from the other cellular devices. Once investigators ascertain the identity of the Target Cellular Device, they will end the collection, and any information collected concerning cellular devices other than the Target Cellular Device will be deleted.

This warrant does not authorize the interception of any telephone calls, text messages, or other electronic communications, and this warrant prohibits the seizure of any tangible property. The Court finds reasonable necessity for the use of the technique authorized above. *See* 18 U.S.C. § 3103a(b)(2).

# WARRANT FOR THE USE OF A CELL-SITE SIMULATOR TO IDENTIFY THE LOCATION OF A KNOWN CELL PHONE OR OTHER CELLULAR DEVICE

THIS GO-BY IS CURRENT AS OF SEPTEMBER 2015. TO GET THE MOST CURRENT VERSION OF THIS GO-BY AND THE LATEST GUIDANCE, VISIT CCIPS ONLINE:

<http://dojnet.doj.gov/criminal/ccips/online/location.htm>

For help with any issues involving the search and seizure of computers, cell phones, and electronic evidence, call the Computer Crime and Intellectual Property Section (“CCIPS”), Criminal Division, United States Department of Justice, at (202) 514-1026.

## USAGE NOTES:

- Use this go-by to enable law enforcement to use its own cell-site simulator equipment (sometimes called “triggerfish” or “stingray” and also including additional “finishing tool” devices) to collect signals emitted by wireless phones or other cellular devices and use these signals to determine the location of a particular person’s cellular device. This warrant should not be served on a provider.
- For Departmental policy regarding use cell-site simulators, please refer to the September 3, 2015, memorandum *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* available on CCIPS online.
- Because a cell-site simulator falls within the statutory definitions of a “pen register” or a “trap and trace device,” see 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. The warrant therefore includes all the information required to be included in a pen register order. See 18 U.S.C. § 3123(b)(1). In addition, an attorney for the government should complete an AO 106 Application for a Search Warrant as specified below to comply with the application requirements of 18 U.S.C. § 3123 for a pen register order.
- This go-by is intended to be used with a standard AO 93 Search Warrant form. Do NOT use the AO 102 Application for a Tracking Warrant. Fill out your district’s AO 93 Search Warrant form this way:
  1. Caption the warrant “In the Matter of the Use of a Cell-Site Simulator to Locate the Cellular Device Assigned Call Number [(xxx) xxx-xxxx].” To caption the warrant in this manner, strike out “the Search of” in the existing caption of the AO 93. Note: If you have another identifier for the cellular device, such as the

International Mobile Subscriber Identity (IMSI) or Electronic Serial Number (ESN), you should include that identifier as well. You may also identify the cellular device by only its IMSI or ESN, rather than by call number, if that approach better suits the needs of your case.

2. Below the parenthetical that asks you to “identify the person or describe the property to be searched and give its location,” write “See Attachment A.”
  3. Below the parenthetical that asks you to “identify the person or describe the property to be seized,” write “See Attachment B.”
  4. The AO 93 form includes spaces for the district in which the property to be searched is located. Rule 41(b) generally requires that the cellular device that you are targeting be in the issuing district either at the time of search, or at the time the warrant is issued. If you are uncertain of the district in which the device is located, you may be able to locate it through a range of techniques, including by using a 2703(d) order for obtaining historical cell-site information. A go-by for this is available on CCIPS online:  
[http://dojnet.doj.gov/criminal/ccips/online/2703/2703\(d\)Orders/2703d go-by for non-content \(ISP list\).doc](http://dojnet.doj.gov/criminal/ccips/online/2703/2703(d)Orders/2703d%20go-by%20for%20non-content%20(ISP%20list).doc). Pursuant to Rule 41(b)(2), investigators may locate the device outside the district provided the device is within the district when the warrant is issued.
  5. Check the box that indicates that “immediate notification may have an adverse result listed in 18 U.S.C. § 2705,” and fill out the appropriate sub-boxes and blanks to indicate the length of delay that you are seeking under 18 U.S.C. § 3103a(b). If you use the standard language contained in this go-by, you should check the first sub-box and indicate the number of days as “30.”
- To ensure compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, an attorney for the government should complete an AO 106 Application for a Search Warrant. *See* 18 U.S.C. §§ 3122(a), 3127(5). In the “The application is based on these facts” box, write: “See Affidavit in Support of an Application for a Search Warrant. To ensure technical compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, this warrant also functions as a pen register order. Consistent with the requirement for an application for a pen register order, I certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [investigative agency]. *See* 18 U.S.C. §§ 3122(b), 3123(b).” Other boxes of the AO 106 should be completed in the same manner as the AO 93.
  - To ensure compliance with the notice requirements of Rule 41, CCIPS recommends giving notice of the warrant either to the



person(s) who actually used the target cellular device or to the registered owner (if different). However, this notice can be delayed under 18 U.S.C. § 3103a(b). This go-by includes language seeking a 30-day delay of notice under 18 U.S.C. § 3103a(b), which permits notice to be delayed up to 30 days initially as long as certain statutory requirements are satisfied. If you need a longer delay, you can attempt to seek a delay to a “later date certain if the facts of the case justify a longer period of delay,” 18 U.S.C. § 3103a(b)(3), or can seek an extension of the original 30-day delay under 18 U.S.C. § 3103(a)(c).

- Include the following information in the warrant return/inventory: (1) the date and time when the acquisition of identifying information began, and (2) the period during which the government acquired identifying information.
- If you are seeking only an order directing a cell phone service provider to disclose prospective cell tower/sector records (sometimes called “cell-site data”) or more precise location information, this is the wrong go-by. Appropriate go-bys are available on CCIPS online:  
[http://dojnet.doj.gov/criminal/ccips/online/location.htm#Applications\\_and\\_Orders](http://dojnet.doj.gov/criminal/ccips/online/location.htm#Applications_and_Orders).
- The Department of Justice Policy issued September 3, 2015, states:  

Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (e.g., tradecraft, capabilities, limitations or specifications). ... To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS, which will coordinate with appropriate Department components.

IN THE UNITED STATES DISTRICT COURT  
FOR \_\_\_\_\_

IN THE MATTER OF THE USE OF A  
CELL-SITE SIMULATOR TO LOCATE  
THE CELLULAR DEVICE ASSIGNED  
CALL NUMBER [(xxx) xxx-xxxx], [WITH  
INTERNATIONAL MOBILE SUBSCRIBER  
IDENTITY / ELECTRONIC SERIAL  
NUMBER xxxxxxxx]

Case No. \_\_\_\_\_

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, [AGENT NAME], being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to employ an electronic investigative technique, which is described in Attachment B, to determine the location of the cellular device assigned call number [[(xxx) xxx-xxxx]], (the "Target Cellular Device"), which is described in Attachment A.

2. I am a [Special Agent] with the [Agency], and have been since [Date].  
**[DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS  
QUALIFICATION TO SPEAK ABOUT THIS INVESTIGATION, CELLULAR  
DEVICES, AND OTHER TECHNICAL MATTERS].**

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. One purpose of applying for this warrant is to determine with precision the Target Cellular Device's location. However, there is reason to believe the Target Cellular Device is currently located somewhere within this district because **[Provide evidence suggesting that Target Cellular Device is currently located in this district, e.g. the Target Cellular Device's owner is known to spend most of his time in this district; the telephone number area code associated with the Target Cellular Device corresponds to this district; the Target Cellular Device's owner was seen in this district X days ago; Cell-site data obtained for the Target Cellular Device indicated that it was normally to be found in this district, or found in this district X days ago; etc.]**. Pursuant to Rule 41(b)(2), law enforcement may locate the Target Cellular Device outside the district provided the device is within the district when the warrant is issued.

5. **[USE THIS PARAGRAPH IF THE LOCATION INFORMATION IS EVIDENCE OF A CRIME.]** Based on the facts set forth in this affidavit, there is probable cause to believe that violations of **[statutes]** have been committed, are being committed, and will be committed by **[suspects or unknown persons]**. There is also probable cause to believe that the location of the Target Cellular Device will constitute evidence of those criminal violations **[[, including leading to the identification of individuals who are engaged in the commission of these offenses and identifying locations where the target engages in criminal activity]]**.

6. **[USE THIS PARAGRAPH IF THE LOCATION INFORMATION WILL HELP TO EFFECTUATE AN ARREST]**

**AND/OR LOCATE A FUGITIVE.]** Based on the facts set forth in this affidavit, there is probable cause to believe that **[Fugitive]** has violated **[statutes]**. **[Fugitive]** was charged with these crimes on **[date]** and is the subject of an arrest warrant issued on **[date]**. **[[If appropriate: There is also probable cause to believe that [Fugitive] is aware of these charges and has fled.]]** There is also probable cause to believe that the Target Cellular Device's location will assist law enforcement in arresting **[Fugitive]**, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

7. Because collecting the information authorized by this warrant may fall within the statutory definitions of a "pen register" or a "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. *See* 18 U.S.C. §§ 3121-3127. This warrant therefore includes all the information required to be included in a pen register order. *See* 18 U.S.C. § 3123(b)(1).

#### **PROBABLE CAUSE**

8. **[[Give facts establishing the probable cause described above. Among other things, this section generally should (1) establish a connection between the Target Cellular Device and the suspected crime and/or targeted individual, (2) identify the subscriber name and address for the Target Cellular Device [this information can be obtained with a subpoena to the wireless provider for the call number], (3) identify the primary user(s) of the Target Cellular Device, if known, and (4) explain why there is probable cause to monitor the cellular device's location for the next thirty days (or for some shorter period of time, if you amend this request to cover a period less than thirty days).]]**

## MANNER OF EXECUTION

9. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

10. To facilitate execution of this warrant, law enforcement may use an investigative device or devices capable of broadcasting signals that will be received by the Target Cellular Device or receiving signals from nearby cellular devices, including the Target Cellular Device. Such a device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell phone to communicate with others. The device may send a signal to the Target Cellular Device and thereby prompt it to send signals that include the unique identifier of the device. Law enforcement may monitor the signals broadcast by the Target Cellular Device and use that information to determine the Target Cellular Device's location, even if it is located inside a house, apartment, or other building.

11. The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law

enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

### **AUTHORIZATION REQUEST**

12. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed warrant also will function as a pen register order under 18 U.S.C. § 3123.

13. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days from the end of the period of authorized surveillance. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cellular Device would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and [continue to] flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

14. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cellular Device outside of daytime hours.

15. **[[If your district does not have standard forms/procedures for filing under seal, you can insert this language in the affidavit:** I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.]]

16. A search warrant may not be legally necessary to compel the investigative technique described herein. Nevertheless, I hereby submit this warrant application out of an abundance of caution.

Respectfully submitted,

---

**[AGENT NAME]**  
Special Agent  
**[AGENCY]**

Subscribed and sworn to before me  
On: \_\_\_\_\_

---

UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number (xxx) xxx-xxxx, [with International Mobile Subscriber Identity / Electronic Serial Number xxxxxxxx], whose wireless provider is [WIRELESS PROVIDER], and whose listed subscriber is [name/unknown].



**ATTACHMENT B**

Pursuant to an investigation of [identify of subject of investigation, if known] for a violation of [offense], this Warrant authorizes the officers to whom it is directed to determine the location of the cellular device identified in Attachment A by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to radio signals sent to the cellular device by the officers;

for a period of thirty days, during all times of day and night. This warrant does not authorize the interception of any telephone calls, text messages, other electronic communications, and this warrant prohibits the seizure of any tangible property. The Court finds reasonable necessity for the use of the technique authorized above. *See* 18 U.S.C. § 3103a(b)(2).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 20:16:25 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Cell-Site Simulator training to the client

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

Can I work from (b) (7)(E) on 5/25?

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

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, April 19, 2017 2:39 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Cell-Site Simulator training to the client

(b) (7)(E) Team,

We have been asked to provide an hour long training on ICE's cell-site simulator policy on behalf of (b) (7)(E) to its field TEOs. There are four sessions that will be held this summer at the Lorton VA facility. After discussing with Joe and Anne, the following was decided:

On Thursday May 25<sup>th</sup>, from 11-12, all of the Tech Ops team will travel to Lorton and watch me give the presentation on cell-site simulators.

On Thursday, June 8<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.

On Thursday June 26<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.

On Thursday July 27<sup>th</sup>, from 11-12, either (b)(6); (b)(7)(C) will give the presentation, and it can be left to the two of you to decide who will go.

I believe the presentation and policy is on the S:Drive, and if it isn't, I will make sure it is this afternoon. Please let me know if you have any questions or comments, calendar invites will be forthcoming.

Sincerely,  
(b)(6); (b)(7)(C)

---

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-73 (b)(6); (b)(7)(C) office)

202-500-(b)(6);  
(b)(7) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 6 Sep 2018 15:00:57 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** DTAS presentation; FLETC; Sept. 12, 2018  
**Attachments:** Drone.docx, DTAS Presentation 9.12.18 FLETC.PPTX  
**Importance:** High

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

I am still cleaning these up today prior to sending them to the DTAS coordinator.

I worked from the docs (b)(6); (b)(7)(C) forwarded to me.

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

I used the current TFO slides as much as possible as the basis for the presentation.

Specifically:

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

I'll keep working to clean these up. I'll get through this presentation, and, hopefully from the questions from students and discussion with class coordinators I can continue to revise it in case CLS is asked to do it again.

Thanks,

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

Associate Legal Advisor

Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

(202) 732-(b)(6);  
(b)(7)(C) (office)  
(202) 308-(b)(6);  
(b)(7)(C) (cell)

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

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient.~~

~~Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

*ICE Office of the Principal Legal  
Advisor*

**U.S. Department of Homeland  
Security**

500 12th Street, S.W.

Washington, DC 20536-5900



**U.S. Immigration  
and Customs  
Enforcement**

MEMORANDUM FOR:

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

Chief  
Criminal Law Section  
Office of the Principal Legal Advisor

FROM:

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

Associate Legal Advisor  
Criminal Law Section

SUBJECT:

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

DATE:

July 17, 2018

This Memorandum to file is in response to several meetings the Criminal Law Section (CLS) has had with U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) regarding (b)(5); (b)(7)(E)

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

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

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

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



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

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

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

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

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

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

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

**From:** (b)(6); (b)(7)(C)  
**Sent:** 1 Jun 2017 14:08:52 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Emailing: Draft HSI Cell-Site - Memo  
**Attachments:** Draft HSI Cell-Site - Memo.doc

Your message is ready to be sent with the following file or link attachments:

Draft HSI Cell-Site - Memo

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

**U.S. Department of Homeland Security**  
500 12th Street, SW  
Washington, D.C. 20536



**U.S. Immigration  
and Customs  
Enforcement**

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

FROM: Peter T. Edge  
Executive Associate Director

SUBJECT: Use of Cell-Site Simulator Technology

Purpose:

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

SUBJECT: Use of Cell-Site Simulator Technology  
Page 2 of 7

Background:

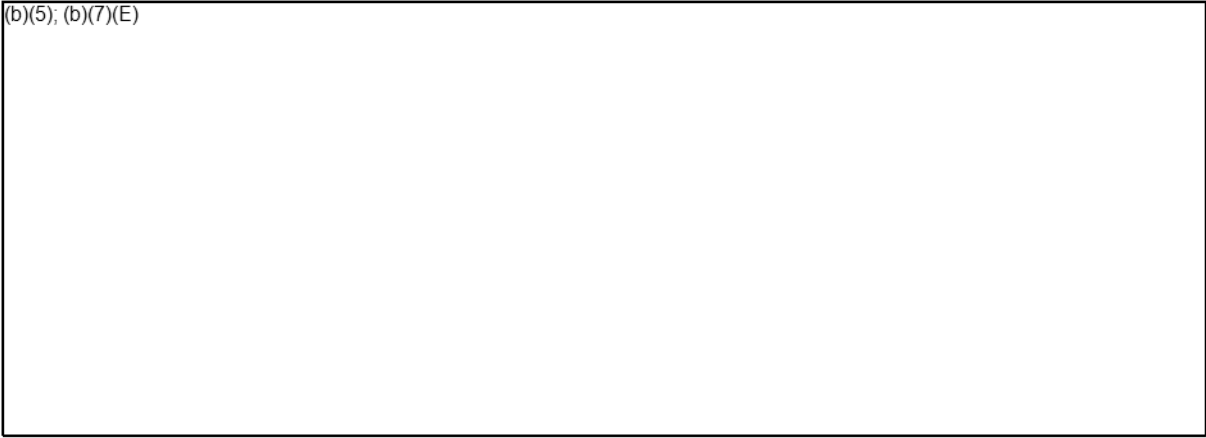
(b)(5); (b)(7)(E)

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

~~LAW ENFORCEMENT SENSITIVE~~

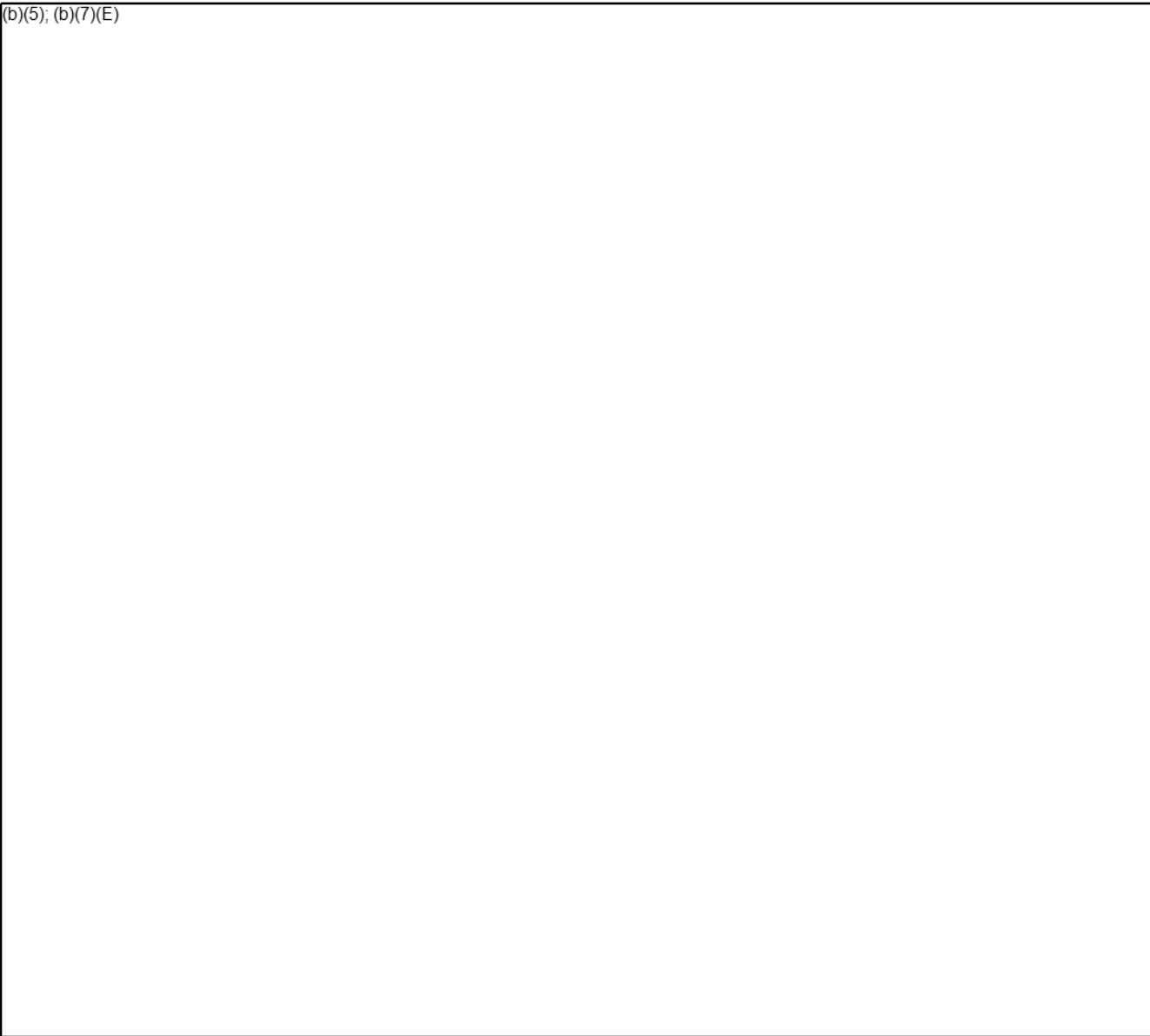


(b)(5); (b)(7)(E)



Legal Process and Court Orders

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



SUBJECT: Use of Cell-Site Simulator Technology  
Page 4 of 7

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

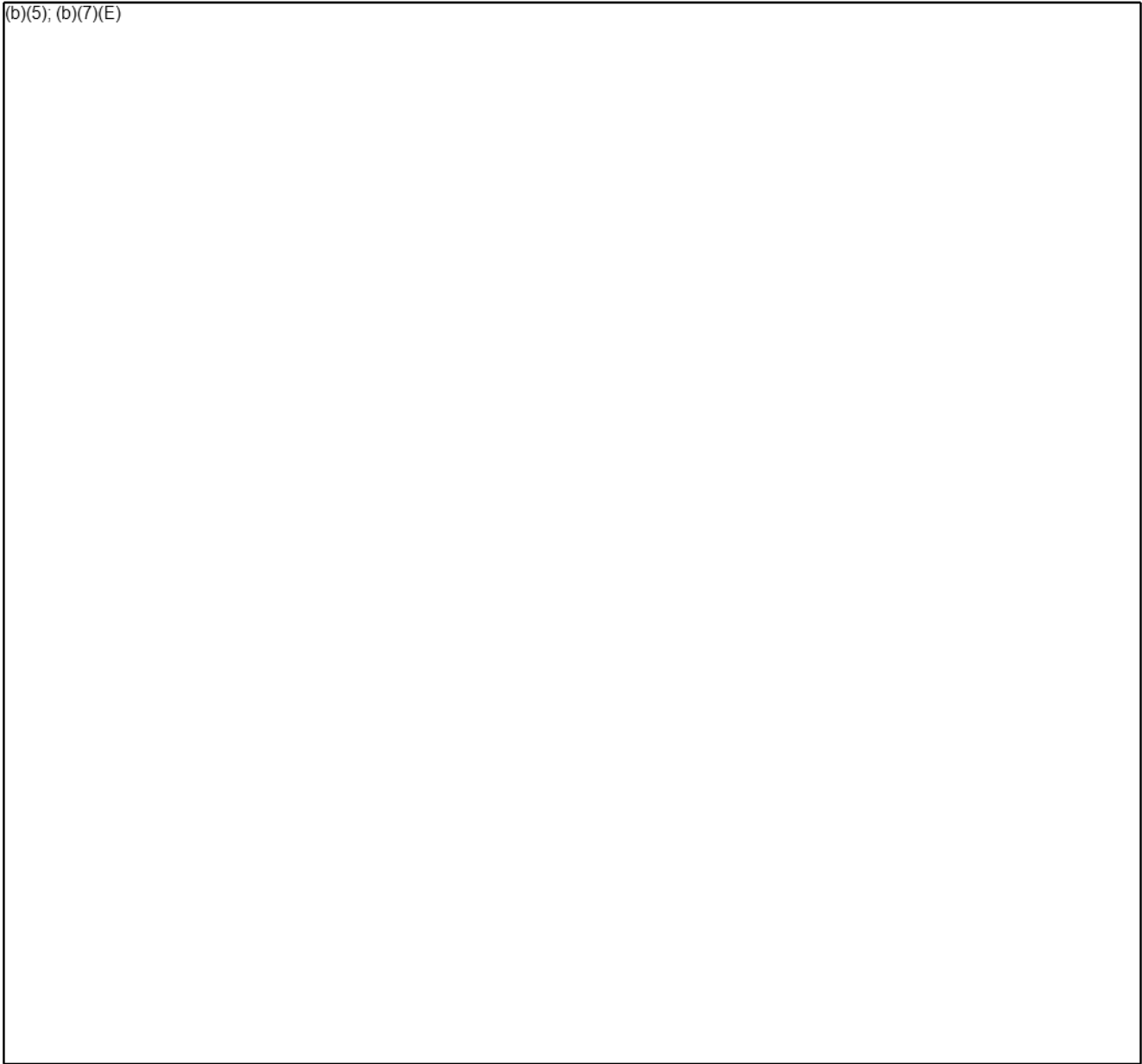
(b)(5); (b)(7)(E)

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


~~LAW ENFORCEMENT SENSITIVE~~

Applications for Use of Cell-Site Simulators

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



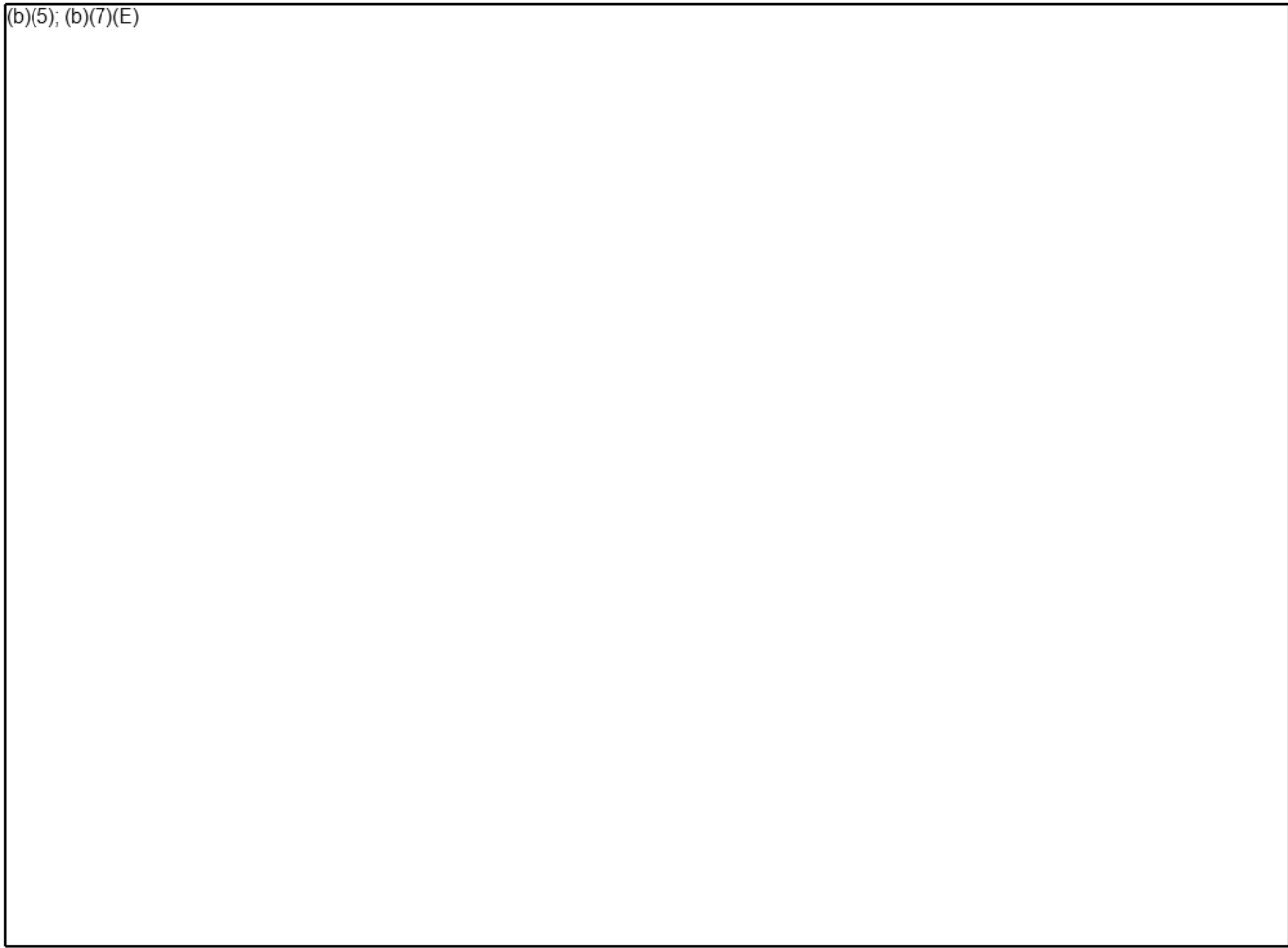
(b)(5); (b)(7)(E)



~~LAW ENFORCEMENT SENSITIVE~~


Data Collection, Recordkeeping, and Disposal

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



State and Local Partners

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



Coordination and Ongoing Management

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

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.

(b)(5); WIF Draft

**LAW ENFORCEMENT SENSITIVE**

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 16:28:51 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Cell-Site Simulator training to the client

Works for me.

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

Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) Desk)  
202-536-(b)(7)(C) Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Date:** Wednesday, Apr 19, 2017, 4:16 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** FW: Cell-Site Simulator training to the client

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

Can I work from Tech Ops on 5/25?

Thanks, (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, April 19, 2017 2:39 PM  
**To:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 2 Mar 2017 13:10:47 -0500  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: DOJ Video Surveillance Storage Challenges  
**Attachments:** DOJ Video Surveillance Storage Challenges.pdf, HSI Surveillance Technologies PIA (IGP 02 06 2017).docx

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (office)  
202-500-(b)(7) (mobile)

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

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*  
This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, February 28, 2017 8:37 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: DOJ Video Surveillance Storage Challenges

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

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

Thanks,

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

Section Chief / Supervisory Special Agent

Homeland Security Investigations  
Technical Operations Unit - Investigative Intercept Section

703-551-(b)(6); (b)(7)(C) fffice)

716-510-(b)(7)(C) ell)

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

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Thursday, February 23, 2017 3:56 PM

**To:** (b)(6); (b)(7)(C)

**Subject:** DOJ Video Surveillance Storage Challenges

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

Don't know if you have a copy of this document.

I think it is beneficial for OPLA folks to see and review the policy for us.

(b)(7)(E)

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

(A) National Program Manager - Spectrum  
Department of Homeland Security  
ICE/HSI/Technical Operations (TechOps) HQ  
10501 Furnace Road Suite (b)(6); (b)(7)(C)  
Lorton, Virginia 22079  
Desk: 703-551-(b)(6); (b)(7)(C)  
Cell: 619-665-(b)(6); (b)(7)(C)  
Email: (b)(6); (b)(7)(C)

**MAILING ADDRESS FOR ALL SPECTRUM EQUIPMENT:**

HSI Spectrum  
ATTN (b)(6); (b)(7)(C)  
10501 Furnace Road, Suite (b)(6); (b)(7)(C) Lorton, Virginia 22079

**HELPDESK CONTACT INFO:**

**VECADS 24/7 Support Desk: (844) 4VECADS (1-844-483-2237) o** (b)(5); WIF Draft

**Spectrum Support Desk: (703) 551-(b)(6); (b)(7)(C) pr** (b)(5); WIF Draft

**ICE Service Desk: (888) 347-7762**

**Feeny Wireless (now known as Novatel) at [PROSupport@nvtl.com](mailto:PROSupport@nvtl.com)**





~~**CONFIDENTIALITY NOTICE:** This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.~~



**Department of Justice**  
*Office of the Chief Information Officer*

# Department of Justice Video Surveillance Storage Challenges

*May 27, 2016*

For Official Use Only

Page 543

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 544

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 545

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 546

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 547

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 548

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 549

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 550

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 551

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 552

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 553

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 554

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 555

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 556

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 557

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

**From:** (b)(6); (b)(7)(C)  
**Sent:** 11 Aug 2016 15:59:54 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** (b)(5); (b)(7)(E)  
**Attachments:** [Redacted] OGC  
op....pdf

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (office)  
202-500-(b)(7)(C) (mobile)  
[Redacted] (b)(6); (b)(7)(C)

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***  
This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 9, 2016 5:54 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** FW: (b)(5); (b)(7)(E)

[Redacted] (b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Deputy Assistant Director (A)  
Information Management Directorate  
ICE, Homeland Security Investigations  
703-551-(b)(6); (Tech Ops)  
202-732-(b)(7)(C) (PCN)  
202-486- [Redacted] (C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 09, 2016 4:53:27 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(5); (b)(7)(E)

All,

Attached is the guidance from OGC in 2009 that HSI SA mentioned in their discussions with us this afternoon.

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

500 12<sup>th</sup> Street SW | Mail Stop 5106 | Washington, D.C. 20536  
Cell: (214) 882-(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 09, 2016 3:47 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(5); (b)(7)(E)

(b)(6); (b)(7)(C) will wait for your response on this request – thanks

(b)(6); (b)(7)(C)  
Unit Chief  
ICE/HSI (b)(6); (b)(7)(C) desk | 202-341-(b)(6); (b)(7)(C) cell  
703-877-(b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 09, 2016 3:38 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(5); (b)(7)(E)

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

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

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

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

Deputy Assistant Director (A)  
Information Management Directorate  
ICE, Homeland Security Investigations  
703-551-(b)(6);  
(b)(7)(C) Tech Ops)  
202-732-(b)(6);  
(b)(7)(C) PCN)  
202-486-(b)(6);  
(b)(7)(C) C)

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, August 08, 2016 10:43 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: (b)(5); (b)(7)(E)

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

Please verify that this equipment is authorized to be purchased Tech Ops, OPLA, OCIO, OAQ, etc.

Thanks

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

Unit Chief  
ICE/HSI  
703-877-(b)(6);  
(b)(7)(C) desk | 202-341-(b)(6);  
(b)(7)(C) cell

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, August 08, 2016 10:32 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** (b)(5); (b)(7)(E)

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

Thanks

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

500 12<sup>th</sup> Street SW | Mail Stop (b)(6);  
(b)(7)(C) Washington, D.C. 20536  
Cell: (214) 882-(b)(6);  
(b)(7)(C)



**Homeland  
Security**

**PRIVILEGED AND CONFIDENTIAL - ATTORNEY-CLIENT COMMUNICATION**

May 27, 2009

MEMORANDUM FOR:

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

Senior Advisor to the Deputy Under Secretary for Mission Integration  
~~Office of Intelligence and Analysis~~

FROM:

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

Associate General ~~Counsel~~ for Operations and Enforcement

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

Attorney-Advisor (Enforcement)

SUBJECT:

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

**Question Presented**

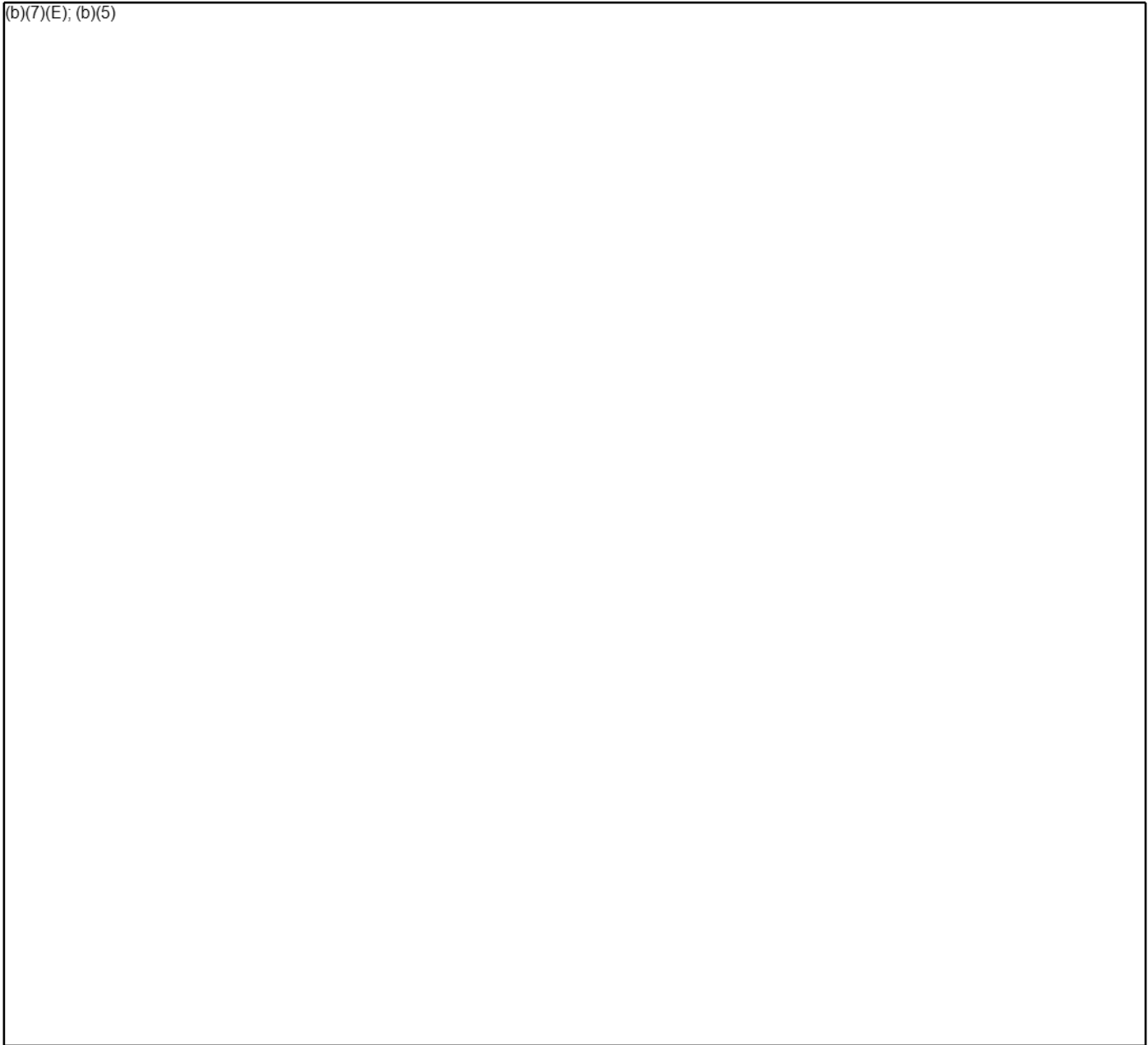
(b)(5); (b)(7)(E)

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

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



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



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



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

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 09:43:24 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) Phone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:38 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** New Adverse on Cell Site Simulators?

(b)(5)

# Police use of ‘StingRay’ cellphone tracker requires search warrant, appeals court rules

By [Tom Jackman](#) September 21 at 5:20 PM



A “StingRay II,” made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that’s an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by police and federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city’s highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a “StingRay” cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone’s GPS function. Civil liberties advocates say the StingRay, by providing someone’s location to police without court approval, is a violation of an individual’s Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

“This opinion,” said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, “joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people’s phones. ... We applaud today’s opinion for erecting sensible and strong protections against the government violating people’s privacy in the digital age.”

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones,

instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government's capacity to invade his or her privacy."

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay "likely violates the legitimate expectation of privacy." But Thompson said Jones forfeited that privacy when he drove around with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone's historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person's whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU's Wessler said that Thursday's ruling was a "recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme

Court takes up the issue of police requests for historical cellphone location data.”

**From:** (b)(6); (b)(7)(C)  
**Sent:** 26 Sep 2016 15:18:42 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Intro to Computers Networks and Cybercrime Presentation (updated as of 8.4.16).pptx  
**Attachments:** Intro to Computers Networks and Cybercrime Presentation (updated as of 8.4.16).pptx

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

As discussed, please take a look at this PPT (updated through August). This is the training CLS has to give on Tuesday, October 4. I will plan to present with you watching, but if you feel comfortable with the material and want to present any of it, that works too!

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) Desk)  
202-536-(b)(7)(C) Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~



**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Nov 2017 19:57:34 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Just FYSA; Article re: Cell Site Simulators

Tech Ops:

(b)(7)(E)

11/17 Article re: HSI use of Cell Site Simulators; just FYSA

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732 (b)(6); (b)(7)(C) (office)  
(202) 308 (b)(6); (b)(7)(C) (cell)  
(b)(6); (b)(7)(C)



~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~  
~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Jul 2016 20:51:55 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:**  
**Attachments:** US v Lambis.pdf

(b)(5)

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

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

Associate Legal Advisor  
U.S. Immigration and Customs Enforcement  
Office of the Principal Legal Advisor  
Homeland Security Investigations Law Division  
Criminal Law Section  
(202) 732-(b)(6); (b)(7)(C) (office)  
(202) 308-(b)(6); (b)(7)(C) (iPhone)

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

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, July 13, 2016 3:20 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Technical Question

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

Please see the message below from the FBI concerning authority to covertly record two party consent in states without a LE exception.

(b)(6); (b)(7)(C)  
Section Chief  
Title III Investigative Programs

Technical Operations Unit  
ICE Homeland Security Investigations  
U.S. Department of Homeland Security  
703.551-(b)(6);  
(b)(7)(C) (Office)  
571.238.1(C) (Cell)

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

*With honor and integrity, we will safeguard the American people, our homeland, and our values.*

~~Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, June 07, 2016 3:34 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Technical Question

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, June 06, 2016 2:17 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Technical Question

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

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, June 06, 2016 12:56 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Technical Question

(b)(6);

What does OIA stand for?

Thanks,

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

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

---

**From:** [redacted]  
**Sent:** Wednesday, June 01, 2016 4:39 PM  
**To:** [redacted]  
**Subject:** RE: Technical Question

[redacted]

Sorry for my delay this morning. I am glad you had a nice weekend in NYC. I had a great time here in Oahu. I did some hiking and of course some shopping!

I thought the best way to answer your question was to provide the attached chart. I made some notations on it as well to clarify a few things. Please take a look and let me know if it is helpful or if you have any further questions.

[redacted]

---

**From:** [redacted]  
**Sent:** Wednesday, June 01, 2016 6:36 AM  
**To:** [redacted]  
**Subject:** Technical Question

[redacted]

I hope you had a good holiday weekend. I was sad to have to return to work after a nice weekend in NYC.

[redacted]

Thanks,

[redacted]

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----	:	
UNITED STATES OF AMERICA,	:	
	:	
-against-	:	15cr734
	:	
RAYMOND LAMBIS,	:	<u>OPINION &amp; ORDER</u>
	:	
Defendant.	:	
-----	:	

WILLIAM H. PAULEY III, District Judge:

Raymond Lambis moves to suppress narcotics and drug paraphernalia recovered by law enforcement agents in connection with a search of his apartment. Lambis’s motion to suppress is granted.

BACKGROUND

In 2015, the Drug Enforcement Administration (the “DEA”) conducted an investigation into an international drug-trafficking organization. As a part of that investigation, the DEA sought a warrant for pen register information and cell site location information (“CSLI”) for a target cell phone. Pen register information is a record from the service provider of the telephone numbers dialed from a specific phone. CSLI is a record of non-content-based location information from the service provider derived from “pings” sent to cell sites by a target cell phone. CSLI allows the target phone’s location to be approximated by providing a record of where the phone has been used.

Using CSLI, DEA agents were able to determine that the target cell phone was located in the general vicinity of “the Washington Heights area by 177th and Broadway.” (April 12, 2016 Suppression Hearing Transcript (“Supp. Tr.”), at 39.) However, this CSLI was not precise enough to identify “the specific apartment building,” much less the specific unit in the

apartment complexes in the area. (Supp. Tr. at 39.)

To isolate the location more precisely, the DEA deployed a technician with a cell-site simulator to the intersection of 177th Street and Broadway. A cell-site simulator—sometimes referred to as a “StingRay,” “Hailstorm,” or “TriggerFish”—is a device that locates cell phones by mimicking the service provider’s cell tower (or “cell site”) and forcing cell phones to transmit “pings” to the simulator. The device then calculates the strength of the “pings” until the target phone is pinpointed. (See Supp. Tr. at 40.) Activating the cell-site simulator, the DEA technician first identified the apartment building with the strongest ping. Then, the technician entered that apartment building and walked the halls until he located the specific apartment where the signal was strongest. (Supp. Tr. at 41.)

The cell-site simulator identified Lambis’s apartment as the most likely location of the target cell phone. That same evening, DEA agents knocked on Lambis’s apartment door and obtained consent from Lambis’s father to enter the apartment. (Supp. Tr. at 8–9.) Once in the apartment, DEA agents obtained Lambis’s consent to search his bedroom. (Supp. Tr. at 13.) Ultimately, the agents recovered narcotics, three digital scales, empty zip lock bags, and other drug paraphernalia. (Supp. Tr. at 14.) Lambis seeks to suppress this evidence.

## DISCUSSION

### I. Fourth Amendment Search

The Fourth Amendment guarantees that all people shall be “secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. CONST. amend. IV. “[T]he underlying command of the Fourth Amendment is always that searches and seizures be reasonable.” New Jersey v. T.L.O., 469 U.S. 325, 337 (1985). “[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that

society recognizes as reasonable.” Kyllo v. United States, 533 U.S. 27, 33 (2001). Barring a few narrow exceptions, “warrantless searches ‘are per se unreasonable under the Fourth Amendment.’” City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)). The home has special significance under the Fourth Amendment. “‘At the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’” Kyllo, 533 U.S. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

In Kyllo, the Supreme Court held that a Fourth Amendment search occurred when Government agents used a thermal-imaging device to detect infrared radiation emanating from a home. 533 U.S. at 40. In so holding, the Court rejected the Government’s argument that because the device only detected “heat radiating from the external surface of the house,” there was no “search.” Kyllo, 533 U.S. at 35. The Court reasoned that distinguishing between “off-the-wall” observations and “through-the-wall surveillance” would “leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home.” Kyllo, 533 U.S. at 35–36. Thus, the Court held that “[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.” Kyllo, 533 U.S. at 40.

Here, as in Kyllo, the DEA’s use of the cell-site simulator to locate Lambis’s apartment was an unreasonable search because the “pings” from Lambis’s cell phone to the nearest cell site were not readily available “to anyone who wanted to look” without the use of a cell-site simulator. See United States v. Knotts, 460 U.S. 276, 281 (1983); see also State v. Andrews, 227 Md. App. 350, \*23 (Md. Ct. Spec. App. 2016) (holding that the use of a cell site

simulator requires a search warrant based on probable cause, and finding that the trial court properly suppressed evidence obtained through the use of the cell-site simulator). The DEA's use of the cell-site simulator revealed "details of the home that would previously have been unknowable without physical intrusion," Kyllo, 533 U.S. at 40, namely, that the target cell phone was located within Lambis's apartment. Moreover, the cell-site simulator is not a device "in general public use." Kyllo, 533 U.S. at 40. In fact, the DEA agent who testified at the hearing had never used one.

The Government counters that Kyllo is not implicated here. In Kyllo, the Court expressed concern that the Government could employ devices, like a thermal imaging device, to learn more intimate details about the interior of the home, such as "at what hour each night the lady of the house takes her daily sauna and bath." Kyllo, 533 U.S. at 38. The Government contends that because the only information to be gleaned from a cell-site simulator is the location of the target phone (for which the Government had already obtained a warrant for CSLI), no intimate details of the apartment would be revealed and Lambis's expectation of privacy would not be implicated. But the Second Circuit has rejected a similar argument even when the search at issue could "disclose only the presence or absence of narcotics" in a person's home. United States v. Thomas, 757 F.2d 1359, 1366-67 (2d Cir. 1985) (holding that a canine sniff that "constitutes a search under the Fourth Amendment . . . when employed at a person's home").

The Government attempts to diminish the power of Second Circuit precedent by noting that Thomas represents a minority position among circuit courts. But this Court need not be mired in the Serbonian Bog of circuit splits. An electronic search for a cell phone inside an apartment is far more intrusive than a canine sniff because, unlike narcotics, cell phones are neither contraband nor illegal. In fact, they are ubiquitous. Because the vast majority of the



population uses cell phones lawfully on a daily basis, “one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful.” Kyllo, 533 U.S. at 38; see also United States v. Jacobsen, 466 U.S. 109, 124 (1984) (“[T]he reason [a canine sniff of luggage at the airport does] not intrude upon any legitimate privacy interest was that the governmental conduct could reveal nothing about noncontraband items.”).

The Supreme Court adopted a similar rationale in United States v. Karo, 468 U.S. 705, 717 (1984). There, the Court held that “[t]he monitoring of a beeper in a private residence, a location not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.” Karo, 468 U.S. at 706. The Government argued that “it should be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper wherever it goes is likely to produce evidence of criminal activity.” Karo, 468 U.S. at 717. In rejecting the Government’s argument, the Court explained that “[t]he primary reason for the warrant requirement is to interpose a neutral and detached magistrate between the citizen and the officer engaged in the often competitive enterprise of ferreting out crime,” and that “[r]equiring a warrant will have the salutary effect of ensuring that use of beepers is not abused, by imposing upon agents the requirement that they demonstrate in advance their justification for the desired search.” Karo, 468 U.S. at 717 (quotations omitted). Thus, even though the DEA believed that the use of the cell-site simulator would reveal the location of a phone associated with criminal activity, the Fourth Amendment requires the Government to obtain a warrant from a neutral magistrate to conduct that search.

The fact that the DEA had obtained a warrant for CSLI from the target cell phone does not change the equation. “If the scope of the search exceeds that permitted by the terms of

a validly issued warrant . . . , the subsequent seizure is unconstitutional without more.” Horton v. California, 496 U.S. 128, 140 (1990); see also United States v. Voustianiouk, 685 F.3d 206, 212 (2d Cir. 2012). Here, the use of the cell-site simulator to obtain more precise information about the target phone’s location was not contemplated by the original warrant application. If the Government had wished to use a cell-site simulator, it could have obtained a warrant. See Karo, 468 U.S. 705, 718 (“The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.”). And the fact that the Government previously demonstrated probable cause and obtained a warrant for CSLI from Lambis’s cell phone suggests strongly that the Government could have obtained a warrant to use a cell-site simulator, if it had wished to do so.

The use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of Kyllo. Absent a search warrant, the Government may not turn a citizen’s cell phone into a tracking device. Perhaps recognizing this, the Department of Justice changed its internal policies, and now requires government agents to obtain a warrant before utilizing a cell-site simulator. See Office of the Deputy Attorney General, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, 2015 WL 5159600 (Sept. 3, 2015); Deputy Assistant Attorney General Richard Downing Testifies Before House Oversight and Government Reform Committee at Hearing on Geolocation Technology and Privacy, 2016 WL 806338 (Mar. 2, 2016) (“The Department recognizes that the collection of precise location information in real time implicates different privacy interests than less precise information generated by a provider for its business purposes.”).

## II. Fourth Amendment Considerations

The Government argues that, even if the use of the cell-site simulator constituted

a Fourth Amendment “search,” exceptions apply. The Government contends that any taint arising from the search dissipated when the agents gained consent to enter the apartment. The Government also argues that there was no reasonable expectation of privacy under the “third party doctrine.”

A. *The Attenuation Doctrine*

Under the attenuation doctrine, “[e]vidence is admissible when the connection between unconstitutional police conduct and the evidence is remote or has been interrupted by some intervening circumstance.” Utah v. Strieff, --- S. Ct. ----, 2016 WL 3369419, at \*5 (June 20, 2016). In applying the doctrine, courts must determine whether the evidence at issue “was come at by exploitation of that [unconstitutional conduct] or instead by means sufficiently distinguishable to be purged of the primary taint.” Wong Sun v. United States, 371 U.S. 471, 488 (1963). The Government maintains that the seizure of evidence from Lambis’s apartment was sufficiently attenuated to dissipate the taint from any Fourth Amendment violation because the agents obtained consent from Lambis’s father to enter the apartment and obtained consent from Lambis himself to search his bedroom.

However, “the procurement of a ‘voluntary’ consent to search based upon a prior illegal search may taint the consent.” United States v. Tortorello, 533 F.2d 809, 815 (2d Cir. 1976) (citing United States v. Hearn, 496 F.2d 236 (6th Cir. 1974)). “When consent to search is preceded by an unlawful [Fourth Amendment violation], the evidence obtained from the search must ordinarily be suppressed unless the Government shows both that the consent was voluntary and that ‘the taint of the initial [seizure] has been dissipated.’” United States v. Murphy, 703 F.3d 182, 190 (2d Cir. 2012) (quoting United States v. Snype, 441 F.3d 119, 132 (2d Cir. 2006)); see also United States v. Cordero-Rosario, 786 F.3d 64, 76–77 (1st Cir. 2015) (“[C]ourts must

determine whether the causal link between a prior unlawful search and consent (voluntary though it may have been) to a subsequent search is so tight that the evidence acquired pursuant to that consent must be suppressed . . . . [T]he fact that the prior unlawful searches by the . . . police led . . . to a . . . party who then consented does not in and of itself show that the taint and exploitation concern simply disappears.”); United States v. Washington, 387 F.3d 1060, 1072 n.12 (9th Cir. 2004) (“For purposes of the Fourth Amendment, a determination that a consent was voluntarily made only satisfies a threshold requirement. The mere fact of voluntariness does not mean that a consent is not tainted by a prior Fourth Amendment violation.”) (internal quotation marks and citations omitted).

Because the Government obtained consent to enter and search the apartment, the analysis focuses on whether the Fourth Amendment violation was sufficiently attenuated such that obtaining the consent was not an exploitation of the unlawful search. To evaluate attenuation, courts consider four factors: (1) whether the defendant was given Miranda warnings, (2) the temporal proximity of the illegal action to the alleged consent, (3) the presence of intervening circumstances, and (4) the purpose and flagrancy of the official misconduct.<sup>1</sup> Snype, 441 F.3d at 132 (citing Kaupp v. Texas, 538 U.S. 626, 633 (2003)); see also Strieff, 2016 WL 3369419, at \*5. Balancing the relevant factors, this Court determines that they weigh in favor of suppression.

The “temporal proximity” factor weighs strongly in favor of suppression. In evaluating this factor, the pertinent question is whether there was sufficient intervening time “to break the chain of illegality.” United States v. Ceballos, 812 F.2d 42, 50 (2d Cir. 1987); Murphy, 703 F.3d at 191. Courts “decline[] to find that this factor favors attenuation unless

---

<sup>1</sup> The first factor is irrelevant to this analysis as consent was not given while the party was in custody. See Snype, 441 F.3d at 134.

‘substantial time’ elapses.” Strieff, 2016 WL 3369419, at \*6 (quoting Kaupp, 538 U.S. at 633); see also Brown v. Illinois, 422 U.S. 590, 604 (1975) (finding suppression appropriate where the search occurred “less than two hours” after unconstitutional arrest). Here, the DEA’s technician used the cell-site simulator on “the evening of August 27, 2015” (Supp. Tr. at 7) and the agents knocked on Lambis’s door at “[a]pproximately 8:00 p.m.” of the same evening (Supp. Tr. at 8). In the time leading up to the agents’ knock on the apartment door, the technician had to scan the streets surrounding Lambis’s apartment complex to identify the correct building and then scan each hallway of the building to identify Lambis’s apartment. (Supp. Tr. at 41.)

Based on these facts, this Court finds that the “chain of illegality” was not broken for two reasons. First, although the record is not clear as to the exact amount of time that elapsed between the violation and the consent, the two events were in close temporal proximity. And at least some portion of any time lapse could be attributable to the need for the technician to convey the cell-site simulator results to DEA agents, who then had to come up to the apartment from the street. Second, a surreptitious Fourth Amendment violation should reasonably extend the time necessary to dissipate the taint. Because neither Lambis nor his father were aware of the DEA’s use of the cell-site simulator, the DEA could have taken their time in securing consent without much risk that Lambis would dispose of the contraband.

Similarly, the “intervening circumstances” factor supports suppression: no intervening circumstances occurred between the use of the cell-site simulator and the consent to search. As Agent Glover explained, the cell-site simulator led the agents to Lambis’s apartment, where they knocked on the door and obtained consent to enter. (Supp. Tr. at 41–42.) Thus, the consent was obtained as a direct result of the illegal Fourth Amendment search and was tainted. Cf. Strieff, 2016 WL 3369419, at \*8 (finding intervening circumstance in a valid arrest warrant

that “predated [the officer’s] investigation[] and . . . was entirely unconnected with the [unlawful] stop.”).

The Sixth Circuit addressed an analogous situation in Hearn. There, the police obtained a search warrant to locate a stolen bulldozer on the defendant’s farm. When they arrived at the farm, the defendant was not present. After locating the bulldozer in the first outbuilding they searched, the police then exceeded the scope of the warrant by going on to search a barn 150 yards away. There, the police located a stolen traxcavator. Hearn, 496 F.2d at 239. When the defendant appeared on the scene, police asked him to consent to a search of the barn. Unaware that the police had already entered the barn and discovered the traxcavator, defendant consented to the search. Hearn, 496 F.2d at 242.

The Sixth Circuit held that “information gained by law enforcement officers during an illegal search cannot be used in a derivative manner to obtain other evidence” and set aside the conviction of the defendant on the count relating to the stolen traxcavator. Hearn, 496 F.2d at 244; see also United States v. Hernandez, 279 F.3d 302 (5th Cir. 2002) (prior illegal “squeezing” of defendant’s luggage while in luggage compartment of bus, although unknown to defendant, taints subsequent consent because the officer “became sufficiently suspicious to engage [defendant] in conversation” in order to obtain consent to a full search of the luggage); United States v. Cordero-Rosario, 786 F.3d 64, 77 (1st Cir. 2015) (finding relevant “whether absent the illegal search, the investigators would have known the identity of all of the third parties or what to ask them.”) (citation and quotations omitted)); United States v. Politano, 491 F. Supp. 456, 463 (W.D.N.Y. 1980) (“[T]he request by Agent Peterson to see the money could only be based upon the information obtained through the prior illegal search at the airport checkpoint by the security personnel and the Cheektowaga police officer.”); LaFave, Wayne R.,

Search and Seizure: A Treatise on the Fourth Amendment, § 8.2(d) (5th ed.) (noting that exploitation of a Fourth Amendment violation “may occur by the police taking advantage of earlier illegal acts which are unknown to the consenting party and thus could not have had a coercive effect upon him.”) (emphasis in original). Accordingly, the consent obtained by the agents, however voluntary, remained tainted by the Fourth Amendment violation.

The only factor militating in favor of the Government is the “purpose and flagrancy” factor. The Second Circuit has approvingly noted that its “sister circuits have held that purposeful and flagrant police misconduct exists where ‘(1) the impropriety of the official’s misconduct was obvious or the official knew, at the time, that his conduct was likely unconstitutional but engaged in it nevertheless; and (2) the misconduct was investigatory in design and purpose and executed in the hope that something might turn up.’” United States v. Murphy, 703 F.3d 182, 192 (2d Cir. 2012) (quoting United States v. Fox, 600 F.3d 1253, 1261 (10th Cir. 2010)). The DEA agents did not intentionally commit any misconduct. However, the search, “both in design and in execution, was investigatory,” Brown, 422 U.S. at 605, and its purpose was clear: identify the apartment unit containing the target phone. As such, this factor only weighs weakly in favor of admission.

#### B. *The Third Party Doctrine*

Finally, the Government argues for the application of the “third party doctrine.” This Court need not address whether the third party doctrine is “ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks,” United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayer, J., concurring), because even under the historic framework of the doctrine, it is not available to the Government here. The doctrine applies when a party “voluntarily turns over [information] to

third parties.” Smith v. Maryland, 442 U.S. 735, 744 (1979); Hoffa v. United States, 385 U.S. 293 (1966) (finding third party doctrine applicable where defendant voluntarily turned over information to Government agent). For instance, in Smith, the Supreme Court found that pen register information is subject to the third party doctrine because “[a]ll telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” Smith, 442 U.S. at 742. However, the location information detected by a cell-site simulator is different in kind from pen register information: it is neither initiated by the user nor sent to a third party.

First, “[c]ell phone users do not actively submit their location information to their service provider.” Andrews, 227 Md. App 350 at \*25. “When a cell phone is powered up, it acts as a scanning radio, searching through a list of control channels for the strongest signal. The cell phone re-scans every seven seconds or when the signal strength weakens, regardless of whether a call is placed.” In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005). These “pings” are sent automatically by the phone to maintain its connection to the network. While the Second Circuit has yet to address whether these passive, CSLI “pings” fall outside the protections of the Fourth Amendment under the third party doctrine,<sup>2</sup> other Circuits have concluded that they do. See United States v. Graham, No. 12-4659, --- F.3d ----, 2016 WL 3068018 (4th Cir. May 31, 2016); United States v.

---

<sup>2</sup> In an unpublished opinion, the Second Circuit hinted that if presented with the question, it may find that CSLI is not protected by the Fourth Amendment. See United States v. Pascual, 502 F. App’x 75, 80 (2d Cir. 2012) (reviewing under a plain error standard because issue was not raised below and finding that “[i]t certainly was not plain error for the district court not to anticipate this innovative argument and sua sponte exclude the evidence, when no governing precedent from this Court or the Supreme Court required exclusion, and the general principles adopted by those courts pointed the other way”). Courts within the Circuit have tended to find CSLI exempt from the Fourth Amendment. See United States v. Serrano, No. 13-cr-58 (KBF), 2014 WL 2696569, at \*7 (S.D.N.Y. June 10, 2014). But see In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (“[A]n exception to the third-party-disclosure doctrine applies here because cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records.”).



Carpenter, No. 14-1572, 2016 WL 1445183 (6th Cir. Apr. 13, 2016); United States v. Davis, 785 F.3d 498 (11th Cir. 2015); In re U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013). But see In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (“A cell phone customer has not ‘voluntarily’ shared his location information with a cellular provider in any meaningful way.”); Tracey v. State, 152 So. 3d 504 (Fla. 2014); and State v. Earls, 214 N.J. 564, 583, 70 A.3d 630, 641 (N.J. 2013).

Nevertheless, the arguments that can be made for the application of the third party doctrine to CSLI do not extend to the distinct technology used by a cell-site simulator, which has an additional layer of involuntariness. Unlike CSLI, the “pings” picked up by the cell-site simulator are not transmitted in the normal course of the phone’s operation. Rather, “cell site simulators actively locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed.” Andrews, 227 Md. App. 350 at \*3 n.4 (emphasis added); State v. Tate, 357 Wis. 2d 172, 182 n.8 (Wis. 2014); Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 2 (Sept. 3, 2015), available at <https://www.justice.gov/opa/file/767321/download>; Brian L. Owsley, Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions, 66 HASTINGS L.J. 183, 192 (2014) (“[T]here is a vulnerability in the authentication process that enables cell site simulators . . . to breach the system. . . . In other words, the cell site simulator tricks the nearby cell phone into transmitting information to it as it would the nearest cell tower.”). The involuntariness of this act is further confirmed by the fact that when the user is actively accessing the network, i.e., placing a call, “the cell site simulator will not be able to access the phone.” Andrews, 227 Md. App. 350 at \*25. (See also May 23, 2016 Post-

Suppression Hearing Conference Transcript, at 12 (“[I]t is true that when a person is actually speaking into the phone, our cell site simulator cannot send or receive the ping from that phone.”).)

Second, unlike pen register information or CSLI, a cell-site simulator does not involve a third party. “Th[e] question of who is recording an individual’s information initially is key.” In re U.S. for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013) (distinguishing between “whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information”). For both pen register information and CSLI, the Government ultimately obtains the information from the service provider who is keeping a record of the information. With the cell-site simulator, the Government cuts out the middleman and obtains the information directly. Without a third party, the third party doctrine is inapplicable.

CONCLUSION

Lambis’s motion to suppress the evidence recovered by DEA agents from his apartment is granted. The Clerk of Court is directed to terminate the motion pending at ECF No. 19.

Dated: July 12, 2016  
New York, New York

SO ORDERED:

  
WILLIAM H. PAULEY III  
U.S.D.J.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 12 Oct 2017 13:55:18 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Latest cybersmuggling slides  
**Attachments:** Cybersmuggling Investigations (Updated 10.11.17).pptx

Here's the latest version of the Cybersmuggling presentation. There are a couple of new slides, some of which have placeholders for real text so be careful what you copy over. Hope it helps!

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (office)  
202-731-(b)(7)(C) (mobile)  
(b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney-Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential or sensitive attorney/client privileged information or attorney work product or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:**

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

**Sent:**

17 Nov 2017 10:32:55 -0500

**To:**

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

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

**Subject:**

News: If NYPD cops want to snoop on your phone, they need a warrant, judge rules

Just a state trial court decision, but thought it was noteworthy.

<https://arstechnica.com/tech-policy/2017/11/if-nypd-cops-want-to-snoop-on-your-phone-they-need-a-warrant-judge-rules/>

# If NYPD cops want to snoop on your phone, they need a warrant, judge rules

NY State Supreme Court: Stingrays act as "an instrument of eavesdropping."

CYRUS FARIVAR - 11/17/2017, 5:03 AM

A New York state judge has concluded that a powerful police surveillance tool known as a stingray, a device that spoofs legitimate mobile phone towers, performs a "search" and therefore requires a warrant under most circumstances.

As a New York State Supreme Court judge in Brooklyn ruled earlier this month in an attempted murder case, New York Police Department officers should have sought a standard, probable cause-driven warrant before using the invasive device.

The Empire State court joins others nationwide in reaching this conclusion. In September, the District of Columbia Court of Appeals also found that stingrays normally require a warrant, as did a federal judge in Oakland, California, back in August.

According to *The New York Times*, which first reported the case on Wednesday, *People v. Gordon* is believed to be the first stingray-related case connected to the country's largest city police force.

"By its very nature, then, the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, acting as an instrument of eavesdropping and requires a separate warrant

supported by probable cause rather than a mere *pen register/trap and trace* order such as the one obtained in this case by the *NYPD*, Justice Martin Murphy wrote in the November 3 [decision](#).

A "pen register" warrant, sometimes known as a "pen/trap order," which typically only provides a call log for a particular number, has been used in the era of stingrays to also include location information. Historically, law enforcement officers nationwide have not been forthright with judges when explaining what the devices do.

As Ars has long reported, [stingrays](#) can be used to determine a mobile phone's location by spoofing a cell tower. In some cases, stingrays can also intercept calls and text messages. Once deployed, the devices [intercept data from a target phone](#) along with information from other phones within the vicinity. At times, police have [falsely claimed](#) the use of a confidential informant when they have actually deployed these particularly sweeping and intrusive surveillance tools.

In this case, the suspect, Shuquan Gordon, was located in a Brooklyn apartment building seemingly out of nowhere. This was "an address not previously identified as of any interest to this investigation," as the judge noted.

[Brian Owsley](#), a law professor at the University of North Texas and a former federal magistrate judge, whose 2014 [law review article](#) on stingrays was cited numerous times by the Brooklyn judge, told Ars that this ruling fell in line with what he called "positive momentum" toward proper regulation.

"There is still a long way to go," he e-mailed. "Moreover, as good as this decision is, the current progress is more aptly described as two steps forward followed by one step back."

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (office)  
202-731-(b)(7)(C) (mobile)

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

\*\*\* Warning \*\*\* Attorney-Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential or sensitive attorney/client privileged information or attorney work product or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This~~

~~document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 17:33:08 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** question on Stingrays

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

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732 (b)(6); (b)(7)(C) (office)  
(202) 308 (b)(6); (b)(7)(C) (cell)

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



~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 26 Aug 2016 18:25:07 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Cell-site Simulator for Palms  
**Attachments:** ICE draft memo Use of Cell-Site Simulator Technology.doc

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

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

All the best,

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (office)  
202-500-(b)(7) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 23, 2016 12:00 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell-site Simulator for Palms



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

(b)(6);  
(b)(7)(C) wanted us to put in some FAQs at the end of the power point. When you have a moment, can you please take a look and let me know if you have any objections?

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

Thanks,

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

Section Chief / Supervisory Special Agent

Homeland Security Investigations  
Technical Operations Unit - Investigative Intercept Section

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

Lorton, VA 22079  
703-551-(b)(6); Office)  
716-510-(b)(7)(C) Cell)  
(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, August 22, 2016 6:39 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell-site Simulator for Palms

Okay, will do.

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); office)  
202-500-(b)(7)(C) mobile)  
(b)(6); (b)(7)(C)

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT  
\*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, August 22, 2016 6:29:14 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell-site Simulator for Palms

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

I believe that once it gets the blessing from HSI policy, it will be sent to you for your official review. If you have anything that you feel should be edited, I can make the modifications prior to sending it back to policy. That may make it easier for the process in the long run...

Thanks,

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

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

Section Chief / Supervisory Special Agent

Homeland Security Investigations  
Technical Operations Unit - Investigative Intercept Section

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

Lorton, VA 22079

703-551 (b)(6); (b)(7)(C) (Office)

716-510 (b)(6); (b)(7)(C) (Cell)

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

**From** (b)(6); (b)(7)(C)

**Sent:** Monday, August 22, 2016 6:27 PM

**To** (b)(6); (b)(7)(C)

**Subject:** RE: Cell-site Simulator for Palms

Thanks (b)(6); (b)(7)(C) do you need an official review of this from our office, or just an informal opinion?

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

Sincerely,

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732 (b)(6); (b)(7)(C) (office)

202-500 (b)(6); (b)(7)(C) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any

~~disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, August 22, 2016 6:16 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell-site Simulator for Palms

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

Attached is the draft. I have a few edits to make before sending it back to HSI policy. Please take a look and let me know what you think. I'll let Policy know that you're our POC on this project.

Thanks again,

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

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, August 22, 2016 6:04 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell-site Simulator for Palms

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

I just wanted to see if you had your hands on a copy of the HSI policy. Thanks a lot,

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

---

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) office)  
202-500-(b)(6); (b)(7)(C) mobile)  
(b)(6); (b)(7)(C)

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, August 19, 2016 10:06 AM

**To:** (b)(6); (b)(7)(C)

**Subject:** RE: Cell-site Simulator for Palms

There's an HSI draft, which is almost identical to the DHS version, which has not yet been signed by the EAD. I met with HSI policy last week for some edits. I'll send you a copy on Monday, to make sure you're in the loop.

Thanks,

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

Take care,

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

Section Chief / Supervisory Special Agent

Homeland Security Investigations  
Technical Operations Unit - Investigative Intercept Section  
10450 Furnace Road  
Lorton, VA 22079  
703-551 (b)(6); (b)(7)(C) (Office)  
716-510 (b)(6); (b)(7)(C) (Cell)  
(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, August 19, 2016 10:02:11 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell-site Simulator for Palms

The actual policy from DHS or the ICE policy just recently signed? I wasn't involved in either, before my time as well, but I may know who was. However, I am now the POC on this along with (b)(6); (b)(7)(C)

Best,

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

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

Associate Legal Advisor

Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732-(b)(6);  
(b)(7)(C) (office)  
202-500-(b)(6);  
(b)(7)(C) (mobile)

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

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, August 19, 2016 9:36:51 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell-site Simulator for Palms

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

(b)(5)

Thanks,

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

Take care,

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

Section Chief / Supervisory Special Agent

Homeland Security Investigations  
Technical Operations Unit - Investigative Intercept Section

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

Lorton, VA 22079

703-551-(b)(6); (b)(7)(C) (Office)  
716-510-(b)(7)(C) (Cell)  
(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, August 19, 2016 9:25:11 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Cell-site Simulator for Palms

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

I reviewed the PPT you sent me and I made a bunch of edits and comments. It is with my management for approval. I'm hoping I get it back by today, but it may be early next week.

Sincerely,

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

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) (office)  
202-500-(b)(7)(C) (mobile)

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

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

*Homeland Security Investigations  
Office of the Executive Associate Director*

**U.S. Department of Homeland Security**  
500 12th Street, SW  
Washington, D.C. 20536



**U.S. Immigration  
and Customs  
Enforcement**

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

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

FROM: Peter T. Edge  
Executive Associate Director

SUBJECT: Use of Cell-Site Simulator Technology

Purpose:

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

www.ice.gov



SUBJECT: Use of Cell-Site Simulator Technology  
Page 2

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

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

~~LAW ENFORCEMENT SENSITIVE~~

SUBJECT: Use of Cell-Site Simulator Technology  
Page 3

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

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

~~LAW ENFORCEMENT SENSITIVE~~

SUBJECT: Use of Cell-Site Simulator Technology  
Page 4

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

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

~~LAW ENFORCEMENT SENSITIVE~~

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

SUBJECT: Use of Cell-Site Simulator Technology  
Page 6

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

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

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

~~LAW ENFORCEMENT SENSITIVE~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 6 Jun 2017 18:05:31 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: 3L?

I am and I am (only thing I see that day is one of the Cell-site Simulator trainings at Tech Ops but I'm not presenting any of those).

Thanks,

(b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, June 06, 2017 2:01 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: 3L?

You betcha! You up for it? You available that day?

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, June 6, 2017 1:59 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: 3L?

A 3L w/ CALD on WSE?

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, June 06, 2017 1:58 PM  
**To:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 May 2017 15:50:01 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: 5/25 (b) (7)(E) visit

(b)(6);

Absolutely. I am here usually everyday by 7:30 a.m. Just give me a heads up the night before you plan to arrive for the day so I can plan accordingly. Right now, that carrel outside of (b)(6); old office is being used, but I'm sure we can find a place for you.

Waiting on next stage for that TIII WG. The draft "present day" breakdown of operations and staffing has been circulated for review and comments. I'll let you know what else comes up.

Thanks -

SA (b)(6); (b)(7)(C)  
*HSI Title-III Investigative Programs*  
(202) 359-(b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, May 9, 2017 3:37 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** 5/25 (b) (7)(E) visit

(b)(6);

Let me know if OPLA can assist in any way on the TIII WG at this stage.

Also, I was on a schedule to spend a day over at (b) (7)(E) each month (sometimes 2). I would usually use the carrel outside (b)(6); office but if that was being used I could usually find a carrel / conference room to sit in. (b)(7)(C)

I am scheduled to come to (b) (7)(E) or Cell Site Simulator training on 5/25. I would like to spend the entire day out there (training is at 1 p.m.; I live in Springfield so not really worth going back and forth to PCN).

Let me know if I can work that out through you on 5/25 and in the future – I think (b)(6) had to let someone at the downstairs desk I'm was coming.

Thanks, (b)(6);

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

(202) 732- (b)(6) (office)

(202) 308- (b)(7) (cell)

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



**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).



**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 16:28:51 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Cell-Site Simulator training to the client

Works for me.

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

Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); Desk  
202-536-(b)(7)(C) Cell

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Date:** Wednesday, Apr 19, 2017, 4:16 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** FW: Cell-Site Simulator training to the client

(b)(6);

Can I work from Tech Ops on 5/25?

Thanks, (b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, April 19, 2017 2:39 PM  
**To:** (b)(6); (b)(7)(C)

**Cc:** (b)(6); (b)(7)(C)  
**Subject:** Cell-Site Simulator training to the client

(b) (7)(E) team,

We have been asked to provide an hour long training on ICE's cell-site simulator policy on behalf of Tech-Ops to its field TEOs. There are four sessions that will be held this summer at the Lorton VA facility. After discussing with (b)(6); (b)(7)(C) and (b)(6); (b)(7)(C), the following was decided:

On Thursday May 25<sup>th</sup>, from 11-12, all of the Tech Ops team will travel to Lorton and watch me give the presentation on cell-site simulators.

On Thursday, June 8<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6) will join him.

On Thursday June 26<sup>th</sup>, from 11-12, Will will give the presentation and (b)(6); (b)(7)(C) will join him.

On Thursday July 27<sup>th</sup>, from 11-12, either (b)(6) or (b)(6); (b)(7)(C) will give the presentation, and it can be left to the two of you to decide who will go.

I believe the presentation and policy is on the S:Drive, and if it isn't, I will make sure it is this afternoon. Please let me know if you have any questions or comments, calendar invites will be forthcoming.

Sincerely,

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

---

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (office)  
202-500-(b)(7)(C) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 28 Mar 2019 15:27:04 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: DTAS Legal Block of Instruction  
**Attachments:** DTAS 901 Schedule.xls

See attached. We have you presenting at 1-4 p.m. on Tuesday 4/2/19.

(b)(6); (b)(7)(C) | Program Manager  
Advanced Training / HSI Academy  
Federal Law Enforcement Training Center, Glynco, GA 31524  
Office: 912.267.(b)(6); iPhone: 520.631.(b)(6); (b)(6); (b)(7)(C)



**Homeland  
Security**

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, March 28, 2019 11:22 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: DTAS Legal Block of Instruction

Thank you (b)(6); (b)(7)(C) Working on it now. Can you please send me the agenda and during what time block I will be presenting?

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732.(b)(6); office)  
(716) 553.(b)(7)(C) cell)  
(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, March 28, 2019 11:20 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: DTAS Legal Block of Instruction

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

Good morning. If you can, submit your travel authorization today. Refer to trip as Guest Instructor for DTAS-901. This is a way for us to track. The authorization will need to be approved by your supervisor and a MSS at the Academy will fund and complete the authorization. Let me know when you submit it and if you have any questions.

Thank you for assisting with this class.

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

Program Manager

Advanced Training / HSI Academy

Federal Law Enforcement Training Center, Glynco, GA 31524

Office: 912.267.(b)(6); (b)(7)(C) iPhone: 520.631.(b)(6); (b)(7)(C)



Homeland Security

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Wednesday, March 27, 2019 2:50 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: DTAS Legal Block of Instruction

Hi (b)(6);

CLS attorney (b)(6); (b)(7)(C) (cc'd here) will be coming to FLETC to present the OPLA block of DTAS.

To confirm, Monday (4/1) and Wednesday (4/3) are travel days w/ (b)(6); (b)(7)(C) presenting a three (3) hour block of instruction on Tuesday 4/2.

Please send the funding string to (b)(6); as soon as possible.

Can you also please send her the current agenda and any other information she needs prior to traveling to FLETC?

Thanks!

(b)(6);

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

Associate Legal Advisor

Criminal Law Section

Homeland Security Investigations Law Division

Office of the Principal Legal Advisor

U.S. Immigration and Customs Enforcement

(202) 732-(b)(6) (office)

(202) 308-(b)(6) (cell)

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



\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient.

Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information.

Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL

GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, March 26, 2019 4:29 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** DTAS Legal Block of Instruction

(b)(6);

Good afternoon. We have a DTAS class scheduled to start next week. I've been dealing with a lot of different classes issues here and I completely forgot to reach out to you and check your availability for next Tuesday April 2. Please give me a call when you return to the office tomorrow.

Take care,

(b)(6); (b)(7)(C) | Program Manager  
Advanced Training / HSI Academy  
Federal Law Enforcement Training Center, Glynco, GA 31524  
Office: 912.267.(b)(6); | iPhone: 520.631.(b)(6); (b)(6); (b)(7)(C)



Homeland  
Security

DHS, Homeland Security Investigations Academy

3/28/2019

Federal Law Enforcement Training Center - Glynco, GA

Designated Technical Agent School 1901

TIME	Monday 4/1	Tuesday 4/2	Wednesday 4/3	Thursday 4/4	Friday 4/5	Saturday 4/6
8:00	Students TRAVEL DAY	Welcome HSI Academy Management (b)(6); (b)(7)(C)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)		
9:00		Orientation / Administration (Hands-on) Program Overview (b)(6); (b)(7)(C)				
10:00	Instructors CLASS PREPARATION	TechOps Presentation (b)(6); (b)(7)(C)	(b)(5); (b)(7)(E)			
11:00		(b)(5); (b)(7)(E) Training (PowerPoint)				
12:00	Lunch					
1:00	Students TRAVEL DAY	Legal 4th Amendment Electronic Surveillance Law (b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E) (Lecture and Hands-on)	
2:00			(b)(5); (b)(7)(E) (Hands-on and Project)			
3:00				(b)(6); (b)(7)(C)		
3:00	Instructors	(b)(6); (b)(7)(C)		(b)(5); (b)(7)(E) (Hands-on)	Cell-Site Simulator (Lecture)	
4:00	CLASS PREPARATION	HQ OPLA Associate Legal Advisor (b)(5); (b)(7)(E)				
4:00		(b)(6); (b)(7)(C)				
5:00						
5:00	AFTER HOURS					
6:30						

Notes:

APPROVED, (Title of Approving Official)

Bldg. 65 Room 202 Class Coordinator: (b)(6); (b)(7)(C) Week 2

TIME	Monday 4/8	Tuesday 4/9	Wednesday	Thursday 4/10	Friday 4/12	Saturday 4/13
8:00	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	Final Practical Exerci (b)(5); (b)(7)(E)	(b)(5); Overview (b)(7)(E)	T
9:00	(Hands-on)	(Hands-on)	(b)(5); (b)(7)(E)	Group A (b)(5); (b)(7)(E)	(b)(6); (b)(7)(C)	R
10:00	(Hands-on)	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C)	Group B (b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	A
11:00		(Hands-on)	(b)(5); (b)(7)(E)	All Instructors	(b)(6); (b)(7)(C)	V
12:00	Lunch (b)(6); (b)(7)(C)			All Instructors		E
1:00	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	Final Practical Exerci	Course (b)(5); (b)(7)(E)	T
2:00	(Hands-on)	(Hands-on)	(b)(6); (b)(7)(C)	Group B (b)(5); (b)(7)(E)		R
3:00	(Hands-on)	Optional Project (b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	Group A (b)(5); (b)(7)(E)	All Instructors	A
4:00			(b)(5); (b)(7)(E)	All Instructors	GRADUATION	V
5:00	(b)(6); (b)(7)(C)		(b)(5); (b)(7)(E)	All Instructors		E
AFTER HOURS						D
6:30						A
						Y

Notes: Breakout Rooms  
 APPROVED, (Title of Approving Official) \_\_\_\_\_

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 13:08:38 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

- 1) Not HSI.
- 2) DC Metropolitan Police Department (MPD).
- 3) *Jones v. United States*, No. 15-CF-322 (D.C. Cir. Sept. 21, 2017) [strange citation since not case not yet published in a reporter]

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (Desk)  
202-839-(b)(7) (Cell)  
(C)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:42 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

Hit send too soon. Two questions:

- 1) This was not an HSI case, right? What agency was it?
- 2) Can you please send me the cite?

I know. That's three questions. But I only had two numbers so back off. Thanks.



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

Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:40 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** RE: New Adverse on Cell Site Simulators?

Thank you both.

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6)  
202-538-(b)(7)(iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:33 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (Desk)  
202-839-(b)(7) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, September 22, 2017 12:06 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5)

(b)(5)

Sent with BlackBerry Work ([www.blackberry.com](http://www.blackberry.com))

**From:** (b)(6); (b)(7)(C)

**Date:** Friday, Sep 22, 2017, 10:41 AM

**To:** (b)(6); (b)(7)(C)

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

**Cc:** (b)(6); (b)(7)(C)

**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

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

Chief

CLS, HSILD, OPLA, ICE

202-732-(b)(6);

202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, September 22, 2017 9:43 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

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

Chief

CLS, HSILD, OPLA, ICE

202-732-(b)(6);

202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:38 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** New Adverse Off Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

# Police use of 'StingRay' cellphone tracker requires search warrant, appeals court rules

By [Tom Jackman](#) September 21 at 5:20 PM

<< OLE Object: Picture (Device Independent Bitmap) >>

A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by police and federal agents for

years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

"This opinion," said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, "joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people's phones. ... We applaud today's opinion for erecting sensible and strong protections against the government violating people's privacy in the digital age."

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but

believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the

search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government's capacity to invade his or her privacy."

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay "likely violates the legitimate expectation of privacy." But Thompson said Jones forfeited that privacy when he drove around with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone’s historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person’s whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU’s Wessler said that Thursday’s ruling was a “recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data.”



**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 12:41:56 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

Hit send too soon. Two questions:

- 1) This was not an HSI case, right? What agency was it?
- 2) Can you please send me the cite?

I know. That's three questions. But I only had two numbers so back off. Thanks.

(b)(6); (b)(7)(C) erta  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:40 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

Thank you both.

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and~~

copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6);  
**Sent:** Friday, September 22, 2017 12:33 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (Desk)  
202-839-(b)(7)(C) (Cell)  
C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:06 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work ([www.blackberry.com](http://www.blackberry.com))

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Sep 22, 2017, 10:41 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732 (b)(6);  
202-538 (b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** Liberta, Joseph M  
**Sent:** Friday, September 22, 2017 9:43 AM  
**To:** Laytin, Alexander; Burke, Sean P; Harrold, Marc M; Rubens, William B  
**Cc:** Beck Tokoph, Anne ([Anne.BeckTokoph@ice.dhs.gov](mailto:Anne.BeckTokoph@ice.dhs.gov)); Falcone, Michael  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

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

Chief

CLS, HSILD, OPLA, ICE

202-732 (b)(6);

202-538 (b)(7)(C) (iPhone)

(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** Davis, Mike P

**Sent:** Friday, September 22, 2017 9:38 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

# Police use of 'StingRay' cellphone tracker requires

# search warrant, appeals court rules

By [Tom Jackman](#) September 21 at 5:20 PM

<< OLE Object: Picture (Device Independent Bitmap) >>

A “StingRay II,” made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that’s an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by police and federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city’s highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a “StingRay” cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone’s GPS function. Civil liberties advocates say the StingRay, by providing someone’s location to police without court approval, is a violation of an individual’s Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

“This opinion,” said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, “joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people’s phones. ... We applaud today’s opinion for erecting sensible and strong protections against the government violating people’s privacy in the digital age.”

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The

StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or

she is made aware of the government's capacity to invade his or her privacy.”

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay “likely violates the legitimate expectation of privacy.” But Thompson said Jones forfeited that privacy when he drove around with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone's historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person's whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU's Wessler said that Thursday's ruling was a “recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data.”



**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 12:39:50 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

Thank you both.

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732 (b)(6);  
202-538 (b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:33 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
Criminal Law Section

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732-(b)(6); Desk)

202-839-(b)(7)(C) Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, September 22, 2017 12:06 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work ([www.blackberry.com](http://www.blackberry.com))

**From:** (b)(6); (b)(7)(C)

**Date:** Friday, Sep 22, 2017, 10:41 AM

**To:** (b)(6); (b)(7)(C)

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

**Cc:** (b)(6); (b)(7)(C)

**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

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

Chief

CLS, HSILD, OPLA, ICE

202-732-(b)(6);

202-538-(b)(6);  
(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:43 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:38 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

# Police use of 'StingRay' cellphone tracker requires search warrant, appeals court rules

By [Tom Jackman](#) September 21 at 5:20 PM

<< OLE Object: Picture (Device Independent Bitmap) >>

A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by police and federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1

ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

“This opinion,” said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, “joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people’s phones. ... We applaud today’s opinion for erecting sensible and strong protections against the government violating people’s privacy in the digital age.”

The U.S. attorney’s office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones’s trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims’ cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, “the use of a cell-site simulator to locate Mr. Jones’s phone invaded a reasonable expectation of privacy and was thus a search.”

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that “a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government’s capacity to invade his or her privacy.”

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government’s use of a StingRay “likely violates the legitimate expectation of privacy.” But Thompson said Jones forfeited that privacy when he drove around with the victims’ stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone’s historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person’s whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU’s Wessler said that Thursday’s ruling was a “recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data.”

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 12:32:33 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (Desk)  
202-839-(b)(7) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:06 PM



**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work ([www.blackberry.com](http://www.blackberry.com))

**From:** (b)(6); (b)(7)(C) ▶  
**Date:** Friday, Sep 22, 2017, 10:41 AM  
**To:** (b)(6); (b)(7)(C) ▶  
(b)(6); (b)(7)(C) ▶  
**Cc:** (b)(6); (b)(7)(C) ▶  
**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:43 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

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

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

CLS, HSILD, OPLA, ICE

202-732 (b)(6);

202-538 (b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, September 22, 2017 9:38 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

# Police use of 'StingRay' cellphone tracker requires search warrant, appeals court rules

By [Tom Jackman](#) September 21 at 5:20 PM

<< OLE Object: Picture (Device Independent Bitmap) >>

A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower

antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by police and federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

"This opinion," said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, "joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people's phones. ... We applaud today's opinion for erecting sensible and strong protections against the government violating people's privacy in the digital age."

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government's capacity to invade his or her privacy."

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay "likely violates the legitimate expectation of privacy." But Thompson said Jones forfeited that privacy when he drove around

with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone's historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person's whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU's Wessler said that Thursday's ruling was a "recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data."

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 12:06:09 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work (www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Sep 22, 2017, 10:41 AM  
**To:** (b)(6); (b)(7)(C)  
<(b)(6); (b)(7)(C)>  
<  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:43 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

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

Chief

CLS, HSILD, OPLA, ICE

202-732

(b)(6);

202-538

(b)(7)(C)

(iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, September 22, 2017 9:38 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

# Police use of 'StingRay' cellphone tracker requires search



**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 11:52:54 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

I've asked (b)(6); (b)(7)(C) to look into, but if you can ask tech Ops, that would be great.

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (Phone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 11:47 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

I had no visibility on this case. I'll reach out to Tech Ops to see if they heard of it.

Sent with BlackBerry Work ([www.blackberry.com](http://www.blackberry.com))

**From:** (b)(6); (b)(7)(C) ▶  
**Date:** Friday, Sep 22, 2017, 10:41 AM  
**To:** (b)(6); (b)(7)(C) ▶,  
(b)(6); (b)(7)(C) ▶  
**Cc:** (b)(6); (b)(7)(C) ▶  
**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:43 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732- (b)(6);  
202-538- (b)(7)(C) (Phone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:38 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** New Adverse on Cell Site Simulators?

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 11:47:08 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

I had no visibility on this case. I'll reach out to Tech Ops to see if they heard of it.

Sent with BlackBerry Work (www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Sep 22, 2017, 10:41 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732 (b)(6);  
202-538 (b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:43 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

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

Chief

CLS, HSILD, OPLA, ICE

202-732 (b)(6);

202-538 (b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, September 22, 2017 9:38 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

# Police use of 'StingRay' cellphone tracker requires search

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 13:10:37 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

Thanks again.

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 1:09 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

- 1) Not HSI.
- 2) DC Metropolitan Police Department (MPD).
- 3) *Jones v. United States*, No. 15-CF-322 (D.C. Cir. Sept. 21, 2017) [*strange citation since not case not yet published in a reporter*]

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-3832 (Desk)  
202-839-1672 (Cell)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:42 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** RE: New Adverse on Cell Site Simulators?

Hit send too soon. Two questions:

- 1) This was not an HSI case, right? What agency was it?
- 2) Can you please send me the cite?

I know. That's three questions. But I only had two numbers so back off. Thanks.

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:40 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [Redacted]  
**Subject:** RE: New Adverse on Cell Site Simulators?

Thank you both.

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

Chief

CLS, HSILD, OPLA, ICE

202-732-(b)(6)

202-538-(b)(7) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, September 22, 2017 12:33 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Associate Legal Advisor

Criminal Law Section

Homeland Security Investigations Law Division

Office of the Principal Legal Advisor

U.S. Immigration and Customs Enforcement

202-732-(b)(6); Desk)

202-839-(b)(7)(Cell)

C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 12:06 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work ([www.blackberry.com](http://www.blackberry.com))

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Sep 22, 2017, 10:41 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

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

Chief  
CLS, HSILD, OPLA, ICE  
202-732 (b)(6);  
202-538 (b)(7)(C) (Phone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient.



Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** Liberta, Joseph M  
**Sent:** Friday, September 22, 2017 9:43 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732 (b)(6);  
202-538 (b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:38 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 18:58:10 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, I spoke w/ (b)(6) and am getting more info on it – I forwarded them the DHS policy and spoke w/ (b)(6); (b)(7)(C) at Tech Ops who provided (b)(6); (b)(7)(C) as the POC in (b)(7)(E) that they are already working with it appears) for the practical aspects / access to the technology, itself, language for pen / R41 warrant, etc. I'll keep you posted – if you know of that case out of NY let me know.

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

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 2:53 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: query - CLS SME re Cell Site Simulator

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

There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

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

Sent with BlackBerry Work  
(www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 11:35 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C), (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 11:17 AM  
**To:** OPLA-CLS; (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks (b)(6); (b)(7)(C) you're the only one on the team here today so can you get in touch with (b)(6); (b)(7)(C)

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

Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (Desk)  
202-536-(b)(7)(C) (Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** OPLA-CLS (b)(6); (b)(7)(C)

**Date:** Friday, Jun 09, 2017, 11:11 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

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

**Subject:** FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell site simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (office)  
202-494-(b)(6) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 10:41 AM  
**To:** OPLA-CLS  
**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

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

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you, (b)(6);

(b)(6):

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732-(b)(6) (w)  
202-904-(b)(6) (c)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 14:53:13 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: query - CLS SME re Cell Site Simulator

(b)(6);

There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

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

Sent with BlackBerry Work  
(www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 11:35 AM  
**To:** (b)(6); (b)(7)(C),  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 11:17 AM  
**To:** OPLA-CLS; (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6); (b)(7)(C)

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

Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); Desk  
202-536-(b)(7)(C) Cell

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~  
~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement~~

sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** OPLA-CLS (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 11:11 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); (b)(7)(C) to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

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

(b)(6); (b)(7)(C)  
Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); office)  
202-494-(b)(7) mobile)  
(b)(6); (b)(7)(C)

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***  
This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 10:41 AM  
**To:** OPLA-CLS  
**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

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

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you, (b)(6);

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

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732 (b)(6) (w)  
202-904 (c)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***  
This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 11:17:13 -0400  
**To:** OPLA-CLS (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) you're the only one on the team here today so can you get in touch with (b)(6)

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

Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (Desk)  
202-536-(b)(7) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** OPLA-CLS (b)(6); (b)(7)(C) >  
**Date:** Friday, Jun 09, 2017, 11:11 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C) >  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,



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

---

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (office)  
202-494-(b)(6) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, June 09, 2017 10:41 AM

**To:** OPLA-CLS

**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

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

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you (b)(6);  
(b)(6): (b)(7)(C)

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6)(w)  
202-904-(b)(6)(c)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***  
This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 15:35:27 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 11:17 AM  
**To:** OPLA-CLS; (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)  
Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) Desk  
202-536-(b)(6); (b)(7)(C) Cell

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** OPLA-CLS (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017 11:11 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); (b)(7)(C) to the CLS inbox seeking guidance on the use of cell site simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

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

---

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-73 (b)(6); (office)  
202-49 (b)(7)(C) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 10:41 AM  
**To:** OPLA-CLS  
**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

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

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

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you (b)(6):

(b)(6):

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732- (b)(6) (w)  
202-904- (b)(6) (c)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 19:04:05 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Where is it, I've been sitting at your desk all day until a few minutes ago.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 3:01 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

If you go into my office, on the desk behind my chair, on the far right side, there is a folder divider with folders in it. One should be labeled cell site, ignore the one labeled (b)(6); (b)(7)(C) In it should be the NY case printed out. If it can wait, I'll find it on Monday.

Sent with BlackBerry Work  
(www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 2:58 PM  
**To:** (b)(6); (b)(7)(C),  
OPLA-CLS (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, I spoke w/ (b)(6) and am getting more info on it – I forwarded them the DHS policy and spoke w/ (b)(6); (b)(7)(C) at Tech Ops who provided (b)(6); (b)(7)(C) as the POC in (b)(7)(E) that they are already working with it appears) for the practical aspects / access to the technology, itself, language for pen / R41 warrant, etc. I'll keep you posted – if you know of that case out of NY let me know.

(b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 2:53 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: query - CLS SME re Cell Site Simulator

(b)(6);

There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

(b)(6);

Sent with BlackBerry Work  
(www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 11:35 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C),  
(b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks (b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 11:17 AM  
**To:** OPLA-CLS; (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6)

(b)(6); (b)(7)(C)  
Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732 (b)(6); Desk)  
202-536 (b)(7)(C) Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** OPLA-CLS (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 11:11 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
(b)(6); (b)(7)(C)  
**Subject:** FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell site simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);

---

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (office)  
202-494-(b)(7)(C) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Friday, June 09, 2017 10:41 AM

**To:** OPLA-CLS

**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)



**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 14:53:13 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: query - CLS SME re Cell Site Simulator

(b)(6);

There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

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

Sent with BlackBerry Work  
(www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 11:35 AM  
**To:** (b)(6); (b)(7)(C),  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 11:17 AM  
**To:** OPLA-CLS; (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6);

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

Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732 (b)(6); (Desk)  
202-536 (b)(7)(C) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement

sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** OPLA-CLS <(b)(6); (b)(7)(C)>  
**Date:** Friday, Jun 09, 2017, 11:11 AM  
**To:** (b)(6); (b)(7)(C)  
 <(b)(6); (b)(7)(C)>  
**Cc:** (b)(6); (b)(7)(C)  
 (b)(6); (b)(7)(C)  
**Subject:** FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);

(b)(6); (b)(7)(C)  
 Associate Legal Advisor  
 Criminal Law Section  
 Homeland Security Investigations Law Division  
 Office of the Principal Legal Advisor  
 U.S. Immigration and Customs Enforcement  
 202-732-(b)(6) (office)  
 202-494-(b)(6) (mobile)  
 (b)(6); (b)(7)(C)

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***  
 This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 10:41 AM  
**To:** OPLA-CLS  
**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you, (b)(6);

(b)(6);

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (w)  
202-904-(b)(6) (c)

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

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*  
This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 15:00:48 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

If you go into my office, on the desk behind my chair, on the far right side, there is a folder divider with folders in it. One should be labeled cell site, ignore the one labeled (b)(6); (b)(7)(C) In it should be the NY case printed out. If it can wait, I'll find it on Monday.

Sent with BlackBerry Work  
(www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 2:58 PM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, I spoke w/ (b)(6) and am getting more info on it – I forwarded them the DHS policy and spoke w/ (b)(6); (b)(7)(C) at Tech Ops who provided (b)(6); (b)(7)(C) as the POC in (b)(7)(E) (that they are already working with it appears) for the practical aspects / access to the technology, itself, language for pen / R41 warrant, etc. I'll keep you posted – if you know of that case out of NY let me know.

(b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 2:53 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: query - CLS SME re Cell Site Simulator

(b)(6);

There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

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

Sent with BlackBerry Work  
(www.blackberry.com)

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 11:35 AM

**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6):

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 11:17 AM  
**To:** OPLA-CLS; (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6)?

(b)(6); (b)(7)(C)  
Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) Desk  
202-536-(b)(7)(C) Cell

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** OPLA-CLS <(b)(6); (b)(7)(C)>  
**Date:** Friday, Jun 09, 2017, 11:11 AM  
**To:** (b)(6); (b)(7)(C)  
<(b)(6); (b)(7)(C)>  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** FW: query - CLS SME re Cell Site Simulator

Good Morning,

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 13:34:39 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: question on Stingrays

Is about 20 min ok?

(b)(6); (b)(7)(C)  
Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-(b)(6) Desk  
571-839-(b)(6) Mobile

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

Technical Support: ICE Service Desk: (888) 347-(b)(6);  
VECADS Support: VECADS 24/7 Support Desk: (888) 4VE-(b)(6); 1-888-483-(b)(6); or

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

CVN Support: Spectrum Support Desk: (703) 551-(b)(6); or

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

~~Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.~~

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 1:33 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** question on Stingrays

(b)(6);

(b)(6); (b)(7)(C) thought you might be able to assist – I have an inquiry through our embed in (b)(7)(E) about current practices involving cell-site simulators – do you have time for a call?

Thanks, (b)(6);

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732-(b)(6) (office)  
(202) 308-(b)(6) (cell)  
(b)(6); (b)(7)(C)



~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 17:31:00 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(7)(E) decision)

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

Many thanks for the guidance and all the supporting information in this message. It definitely will lend itself to a productive discussion with ERO Leadership. I believe this gives us the necessary ammunition to tackle this head-on. This is a marquee case for us, and we are extremely grateful for your counsel.

I'll be in touch with further developments as they surface.

Regards,

(b)(6); (b)(7)(C)  
ICE-ERO-TLEO  
Deputy Assistant Director  
Global Police Services Division  
USNCB-INTERPOL Washington  
Mobile: 202-697-(b)(6);

**From:** (b)(6); (b)(7)(C) >  
**Date:** Friday, Jun 09, 2017, 4:38 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** >  
**Subject:** (b)(6); and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(7)(C) Cir. decision)

(b)(6); -

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)



(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6)  
202-904-(b)(6)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 18:15:44 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: (b)(6); (b)(7)(C) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(7)(E) Cir. decision)

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

Thanks so much for your generosity, advice, and time today. I really appreciate it. Have a wonderful weekend.

(b)(6);  
202-904-(b)(6); c

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Date:** Friday, Jun 09, 2017, 5:31 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** >  
**Subject:** RE: (b)(6); (b)(7)(C) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(E) Tracking Warrant + (b)(7)(E) Cir. decision)

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

Many thanks for the guidance and all the supporting information in this message. It definitely will lend itself to a productive discussion with ERO Leadership. I believe this gives us the necessary ammunition to tackle this head-on. This is a marquee case for us, and we are extremely grateful for your counsel.

I'll be in touch with further developments as they surface.

Regards,

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

ICE-ERO-TLEO  
Deputy Assistant Director  
Global Police Services Division  
USNCB-INTERPOL Washington

Mobile: 202-697-(b)(6);  
(b)(7)(C)

**From:** (b)(6); (b)(7)(C)

**Date:** Friday, Jun 09, 2017, 4:38 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**  

**Subject:** (b)(6);  
(b)(7)(C) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C)  
Tracking Warrant + (b)(7)  
(C) Cir. decision)

(b)(6);  
(b)(7)(C) —

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 17 Nov 2017 10:46:53 -0500  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)

**Subject:** RE: News: If NYPD cops want to snoop on your phone, they need a warrant, judge rules

Wait – what? (See my highlights, below.)

And what the heck are you reading???

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

Chief  
CLS, HS, I, D, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) (iPhone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6);  
**Sent:** Friday, November 17, 2017 10:33 AM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)

**Subject:** News: If NYPD cops want to snoop on your phone, they need a warrant, judge rules

Just a state trial court decision, but thought it was noteworthy.

<https://arstechnica.com/tech-policy/2017/11/if-nypd-cops-want-to-snoop-on-your-phone-they-need-a-warrant-judge-rules/>

# If NYPD cops want to snoop on your phone, they need a warrant, judge rules

NY State Supreme Court: Stingrays act as "an instrument of eavesdropping."

CYRUS FARIVAR - 11/17/2017, 5:03 AM

A New York state judge has concluded that a powerful police surveillance tool known as a stingray, a device that spoofs legitimate mobile phone towers, performs a "search" and therefore requires a warrant under most circumstances.

As a New York State Supreme Court judge in Brooklyn ruled earlier this month in an attempted murder case, New York Police Department officers should have sought a standard, probable cause-driven warrant before using the invasive device.

The Empire State court joins others nationwide in reaching this conclusion. In September, the District of Columbia Court of Appeals also found that stingrays normally require a warrant, as did a federal judge in Oakland, California, back in August.

According to *The New York Times*, which first reported the case on Wednesday, *People v. Gordon* is believed to be the first stingray-related case connected to the country's largest city police force.

"By its very nature, then, the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, acting as an instrument of eavesdropping and requires a separate warrant supported by probable cause rather than a mere *pen register/trap and trace* order such as the one obtained in this case by the *NYPD*," Justice Martin Murphy wrote in the November 3 decision.

A "pen register" warrant, sometimes known as a "pen/trap order," which typically only provides a call log for a particular number, has been used in the era of stingrays to also include location information. Historically, law enforcement officers nationwide have not been forthright with judges when explaining what the devices do.

(b)(5)

(b)(5)

In this case, the suspect, Shuquan Gordon, was located in a Brooklyn apartment building seemingly out of nowhere. This was "an address not previously identified as of any interest to this investigation," as the judge noted.

Brian Owsley, a law professor at the University of North Texas and a former federal magistrate judge, whose 2014 law review article on stingrays was cited numerous times by the Brooklyn judge, told Ars that this ruling fell in line with what he called "positive momentum" toward proper regulation.

"There is still a long way to go," he e-mailed. "Moreover, as good as this decision is, the current progress is more aptly described as two steps forward followed by one step back."

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) office)  
202-731-(b)(6) mobile)

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

\*\*\* Warning \*\*\* Attorney-Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential or sensitive attorney/client privileged information or attorney work product or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~



**From:** (b)(6); (b)(7)(C)  
**Sent:** 3 Aug 2017 15:09:29 -0400  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: Noteworthy tech news

Thanks (b)(6); This bitcoin issue just came up on an AFU call about whether this impacts our current forfeiture procedures.

(b)(6); (b)(7)(C)  
Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732 (b)(6); (b)(7)(C) Desk  
202-536 (b)(6); (b)(7)(C) Cell

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

---

**From:** (b)(6);  
**Sent:** Wednesday, August 2, 2017 1:54 PM  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** Noteworthy tech news

Sharing with Cyber, Tech Ops, and Financial.

8. TR Daily– “Four Senators Press DOJ on Cell-Site Simulator Disclosures” – Four senators wrote AG Sessions today to urge DOJ to inform judges about the impacts of cell-site simulators such as Stingrays on 911 calls and other communications of Americans.
  
11. Ars Technica– “Why the Bitcoin network just split in half and why it matters” – The confusing result is that if you owned one bitcoin before the split you own two bitcoins now: one coin on

the original Bitcoin network, and a second coin on the new Bitcoin Cash network. The two coins have the same cryptographic credentials, but they have very different values if you sell them for old-fashioned dollars. Long read.

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

Associate Legal Advisor  
Criminal Law Section|Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (desk)  
202-731-(b)(6) (mobile)

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

**\*\*\* Warning \*\*\* Attorney-Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential or sensitive attorney/client privileged information or attorney work product or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, retransmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 27 Jul 2017 13:16:39 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Cell-site simulator canvassing warrant go-by 2015 09 10.docx  
**Attachments:** Cell-site simulator canvassing warrant go-by 2015 09 10.docx

Here you go.. let me know if you need anything else.

WARRANT FOR THE USE OF A CELL-SITE SIMULATOR TO  
OBTAIN IDENTIFIERS OF A CELL PHONE OR OTHER CELLULAR  
DEVICE AT PARTICULAR LOCATIONS (“CANVASSING”)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

IN THE UNITED STATES DISTRICT COURT  
FOR \_\_\_\_\_

IN THE MATTER OF THE USE OF A CELL-  
SITE SIMULATOR TO IDENTIFY THE  
CELLULAR DEVICE CARRIED BY  
[[SUSPECT]]

Case No. \_\_\_\_\_

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

(b)(5)

F  
i  
c  
I  
l  
c  
I  
e  
t  
f

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

**ATTACHMENT A**

(b)(5)



**ATTACHMENT B**

(b)(5)



**From:** (b)(6); (b)(7)(C)  
**Sent:** 30 Aug 2016 14:16:03 +0000

**To:** (b)(6); (b)(7)(C)

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

**Cc:** (b)(6); (b)(7)(C)

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

**Subject:** State v. Andrews

**Attachments:** andrews-maryland\_court\_of\_special\_appeals\_opinion.pdf

[Sending to Tech Ops, Cyber and Cyber Forensics and cc'ing all CLS]

Attached is a Md Ct. of Appeals Dec., *State v. Andrews*, on cell-site simulators. From the Homeland Sec. Inst. conference (b)(6) and I attended last week (and just generally) this is a hot topic; expect there to be more litigation. This case is fairly recent – 3/16.

(b)(5); (b)(6); (b)(7)(C)

Very general breakdown (of course); just FYI,

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

Associate Legal Advisor  
U.S. Immigration and Customs Enforcement  
Office of the Principal Legal Advisor  
Homeland Security Investigations Law Division  
Criminal Law Section  
(202) 732-(b)(6) office  
(202) 308-(b)(7) iPhone  
(b)(6); (b)(7)(C)



**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).



REPORTED  
IN THE COURT OF SPECIAL APPEALS  
OF MARYLAND

No. 1496

September Term, 2015

---

STATE OF MARYLAND

v.

KERRON ANDREWS

---

Leahy,  
Friedman,  
Thieme, Raymond G., Jr.  
(Retired, Specially Assigned)

JJ.

---

Opinion by Leahy, J.

---

Filed: March 30, 2016

“[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”

*Riley v. California*, 134 S. Ct. 2473, 2484 (2014).

This case presents a Fourth Amendment issue of first impression in this State: whether a cell phone—a piece of technology so ubiquitous as to be on the person of practically every citizen—may be transformed into a real-time tracking device by the government without a warrant.

On the evening of May 5, 2014, the Baltimore City Police Department (BPD) used an active cell site simulator, without a warrant, to locate Appellee Kerron Andrews who was wanted on charges of attempted murder. The cell site simulator, known under the brand name “Hailstorm,” forced Andrews’s cell phone into transmitting signals that allowed the police to track it to a precise location inside a residence located at 5032 Clifton Avenue in Baltimore City. The officers found Andrews sitting on the couch in the living room and arrested him pursuant to a valid arrest warrant. The cell phone was in his pants pocket. After obtaining a warrant to search the residence, the police found a gun in the cushions of the couch.

In the Circuit Court for Baltimore City, Andrews successfully argued that the warrantless use of the Hailstorm device was an unreasonable search under the Fourth Amendment of the United States Constitution. The court suppressed all evidence obtained by the police from the residence as fruit of the poisonous tree. The State, pursuant to Maryland Code (1973, 2013 Repl. Vol., 2015 Supp.), Courts and Judicial Proceedings Article (“CJP”), § 12-302(c)(4), now appeals the court’s decision to suppress that evidence.

The specific questions before us, as framed by the State, are:

- 1) Did the motions court err in finding that the use of a cellular tracking device to locate Andrews's phone violated the Fourth Amendment?
- 2) Did the motions court err in finding that Andrews did not have to show standing before challenging the search of the home where he was arrested?
- 3) Did the motions court err in finding that the search warrant for the home where Andrews was located was invalid?
- 4) Did the motions court err in excluding the items recovered in this case?

We conclude that people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement, and—recognizing that the Fourth Amendment protects people and not simply areas—that people have an objectively reasonable expectation of privacy in real-time cell phone location information. Thus, we hold that the use of a cell site simulator requires a valid search warrant, or an order satisfying the constitutional requisites of a warrant, unless an established exception to the warrant requirement applies.

We hold that BPD's use of Hailstorm was not supported by a warrant or an order requiring a showing of probable cause and reasonable limitations on the scope and manner of the search. Once the constitutionally tainted information, obtained through the use of Hailstorm, was excised from the subsequently issued search warrant for 5032 Clifton Avenue, what remained was insufficient to establish probable cause for a search of that residence. Because the antecedent Fourth Amendment violation by police provided the only information relied upon to establish probable cause in their warrant application, those

same officers cannot find shelter in the good faith exception, and the evidence seized in that search withers as fruit of the poisoned tree. We affirm.

## **BACKGROUND**

Andrews was positively identified via photographic array as the person who shot three people on April 27, 2014, as they were attempting to purchase drugs on the 4900 block of Stafford Street in Baltimore City.<sup>1</sup> He was charged with attempted first-degree murder and attendant offenses in connection with the shooting, and a warrant for his arrest was issued on May 2, 2014.

### **Pen Register and Trap & Trace Order**

Unable to locate Andrews, Detective Michael Spinnato of the BPD confirmed Andrews's cell phone number through a confidential informant, and then submitted an application in the Circuit Court for Baltimore City for a pen register/trap & trace order for Andrews's cell phone.<sup>2</sup> Specifically, Det. Spinnato requested authorization for the

---

<sup>1</sup> The State later admitted that there were also two negative photo arrays.

<sup>2</sup> As discussed further *infra*, pursuant to the Maryland Pen Register, Trap and Trace Statute, found at CJP § 10-4B-01 *et seq.* (“Maryland pen register statute”), a court having jurisdiction over the crime being investigated may authorize the use of a “pen register” and/or a “trap and trace device,” defined as:

‘Pen register’ means a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.

CJP § 10-4B-01(c)(1). The statute continues, stating:

‘Trap and trace device’ means a device or process that captures the incoming electronic or other impulses that identify the originating number or other

“installation and use of device known as a “Pen Register\Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, which registers telephone numbers dialed or pulsed from or to the telephone(s) having the number(s) . . . .” The application stated that Andrews was aware of the arrest warrant, and that to hide from police

suspects will contact family, girlfriends, and other acquaintances to assist in their day to day covert affairs. Detective Spinnato would like to track/monitor Mr. Andrews’[s] cell phone activity to further the investigation an [sic] assist in Mr. Andrews’[s] apprehension.

\* \* \*

Your Applicant hereby certifies that the information likely to be obtained concerning the aforesaid individual’s location will be obtained by learning the numbers, locations and subscribers of the telephone number(s) being dialed or pulsed from or to the aforesaid telephone and that such information is relevant to the ongoing criminal investigation being conducted by the Agency.

On May 5, 2014, Det. Spinnato’s application was approved in a signed order stating, in part:

**[T]he Court finds that probable cause exists and that the applicant has certified that the information likely to be obtained by the use of the above listed device(s) is relevant to an ongoing criminal investigation, To wit: Attempted Murder.**

\* \* \*

(Emphasis in original). And, as requested in the application, the court,

---

dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.

CJP § 10-4B-01(d)(1). Under Maryland law, an order for a pen register/trap & trace is issued without a warrant and on something less than probable cause.

**ORDERED**, pursuant to Section 10-4B-04 of the Courts and Judicial Proceedings Article . . . [Applicants] are authorized to use for a period of sixty (60) days from the date of installation, a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits . . .

\* \* \*

**ORDERED**, . . . [t]he Agencies are *authorized to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register \ Trap & Trace and Cellular Tracking Device*, unobtrusively and with a minimum of interference to the service of subscriber(s) of the aforesaid telephone, and *shall initiate a signal to determine the location of the subject's mobile device . . .*

(Emphasis added).

### **Cell Phone in a Hailstorm**

As soon as Det. Spinnato obtained the pen register\trap & trace order on May 5, he sent a copy to the BPD's Advanced Technical Team (the "ATT"). The ATT then issued a form request to the service provider (Sprint) for the following: subscriber information; historical cell site location information ("CSLI") for the period from April 5 to May 5, 2014; pen register data for 60 days; and precision GPS data from Andrews's phone.<sup>3</sup> An additional request followed for "GPS Precise Locations and email."

---

<sup>3</sup> Two broad categories of CSLI may be sought from the service provider. The first is historical CSLI, which is used to look back through service provider records to determine a suspect's location at a given point in the past. *See, e.g., United States v. Graham*, 796 F.3d 332, 343 (4th Cir. 2015) ("Historical CSLI identifies cell sites, or 'base stations,' to and from which a cell phone has sent or received radio signals, and the particular points in time at which these transmissions occurred, over a given timeframe. . . . The cell sites listed can be used to interpolate the path the cell phone, and the person carrying the phone, travelled during a given time period."), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015). Law enforcement frequently uses historical CSLI to prove that a defendant was in the area where a crime of which he is accused occurred. The second category of CSLI is real-time data, used to track the whereabouts and movements of a suspect by using the cell

Later on the same day—May 5—Det. Spinnato began receiving emails from ATT with GPS coordinates for Andrews’s cell phone (within a range of a 200 to 1600 meter radius). Det. Spinnato and officers from the Warrant Apprehension Task Force (“WATF”) proceeded to the general area and waited until they received information from ATT that the cell phone was in the area of 5000 Clifton Avenue, Baltimore City. They proceeded to an area where there were approximately 30 to 35 apartments around a U-shaped sidewalk. Detective John Haley from ATT arrived and, using a cell site simulator known by the brand name “Hailstorm,” was able to pinpoint the location of the cell phone as being inside the residence at 5032 Clifton Avenue.<sup>4</sup>

Det. Spinnato knocked on the door and, after obtaining the consent of the woman who answered, entered the residence along with several other officers. They found Andrews seated on the couch in the living room with the cell phone in his pants pocket.

---

phone as a tracking device. *See, e.g., Tracey v. State*, 152 So. 3d 504, 507 (Fla. 2014), *reh’g denied* (Dec. 8, 2014). Here, the BPD obtained real-time location information from the service provider when it received the GPS coordinates associated with the cell phone from Sprint. Andrews’s motion to suppress, however, was focused primarily on the BPD’s ensuing use of a cell site simulator to directly obtain pin-point location data. Therefore, on appeal we do not address whether the real-time location information from Sprint should have been obtained under a warrant or special order.

<sup>4</sup> True to its brand name, the Hailstorm device generates an electronic barrage that impacts all the mobile devices within its range. As noted in the *amicus* brief filed by the American Civil Liberties Union (“ACLU”) and Electronic Frontier Foundation (“EFF”) at page 3, the fact that cell site simulators actively locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed, is found in several recent federal publications and cases, including a Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 2 (Sept. 3, 2015), *available at* <https://www.justice.gov/opa/file/767321/download> [<https://perma.cc/K99L-H643>].

Det. Spinnato arrested Andrews and secured the location until a search warrant could be obtained. Once they had the warrant, the BPD searched the home and found a gun in the couch cushions.

### **Initial Hearings**

Andrews was indicted by a grand jury on May 29, 2014, on numerous charges related to the April 27, 2014 shooting. On July 1, 2014, the Assistant Public Defender representing Andrews filed an “omnibus” motion including requests for discovery and the production of documents. The State responded with an initial disclosure and supplemental disclosure on July 9 and 11, respectively. Those disclosures, however, failed to reveal the method used to locate Andrews on the date of his arrest.

On November 3, 2014, defense counsel filed a supplemental discovery request seeking, *inter alia*, “[a]ll evidence indicating how Andrews was located at 5032 Clifton Avenue.” The State’s response to that request, dated January 8, 2015, stated, “[a]t this time the State does not possess information related to the method used to locate [Andrews] at 5032 Clifton Avenue.” However, five months later defense counsel received an email from the Assistant State’s Attorney (“ASA”) assigned to the case indicating that it was her understanding that “the ATT used a stingray to locate[] your client via his cell phone,” but she was waiting for “the paperwork.” The next day, May 7, the ASA also notified defense counsel of exculpatory evidence in the form of a negative photo array that was conducted the previous January.

On May 12, 2015, defense counsel requested that the court dismiss the case based on discovery violations and moved for suppression of evidence, including the gun, phone



records, and identification testimony. A few days later, on May 15, the State filed a supplemental disclosure, which provided:

WATF did not have the Clifton Ave address as a possible location until ATT provided that information. Det. Spinnato recalls that he was in touch with Det. Haley from ATT. ATT was provided that information from Sprint in the form of GPS coordinates, Det. Spinnato received the same information either from Sprint directly, or forwarded from ATT. Det. Spinnato provided ATT with the phone number associated to Defendant from the shooting investigation and, [redacted in original]-Det. Spinnato recalls that ATT gave Det. Spinnato the Clifton Ave address in the afternoon/early evening on May 5, 2014. . . .

The State's supplemental disclosure also identified a second negative photo array conducted on May 4, 2014.

Andrews's initial motions were heard in the circuit court on May 12, 21, and June 4, 2015. At the conclusion of the hearing on June 4, the circuit court found that one of the lead investigators intentionally withheld exculpatory evidence—including both negative photo arrays. As a result, the circuit court partially granted the pending defense motion for sanctions and excluded that detective's testimony from trial. The court declined to dismiss the case and denied the motion to exclude the gun and cell phone on the basis of the State's withholding of discoverable materials. However, as a consequence of the State's failure to timely disclose information concerning Hailstorm surveillance technology that was used by the BPD, the Court granted the defense additional time to file a motion to suppress.

### **Motion to Suppress**

Andrews filed a Motion to Suppress—over 50 pages including exhibits—on June 30, 2015, in which he challenged the BPD's surreptitious use of the Hailstorm cell site simulator to search Andrews's phone, without a warrant, under the Fourth Amendment to

the United States Constitution. Andrews moved to suppress all evidence obtained from 5032 Clifton Avenue.

During the ensuing hearing on the motion to suppress, held August 20, 2015, the State suggested, and the defense agreed, that the circuit court rely on the transcripts and exhibits from the earlier motions hearings for an understanding of the function of the Hailstorm device and its use by the BPD:

[STATE'S ATTORNEY]: . . . The exact testimony that we're going to hear about with regard to the Fourth Amendment issue Counsel heard as it related to the discovery issue because the discovery issue bled into the Fourth Amendment issue. So there is nothing new. There is nothing -- Counsel's aware that the equipment is called Hailstorm not Stingray because of the testimony that Counsel heard and extracted from the detective as it relates to this very case. So there simply is, there is nothing new. We're at the exact same issue that we were two months ago.

THE COURT: So do we even need, do you need to call the witness or can I just rely on the transcript?

[STATE'S ATTORNEY]: It would seem to me to rely on the transcript.

\* \* \*

THE COURT: . . . So the State is indicating that the testimony that the State would present today is the same testimony that was presented --

[DEFENSE COUNSEL]: Right.

THE COURT: -- there.

[DEFENSE COUNSEL]: Right.

THE COURT: And that's in the transcript, and the Court can just rely on the transcript to rule on your motion.

[DEFENSE COUNSEL]: Right.

THE COURT: You're fine with that?

[DEFENSE COUNSEL]: Yep.

The court took a recess for several hours to review the motions and transcripts. The following excerpts from the June 4<sup>th</sup> hearing, entered as Defendant's Exhibit 1C, pertain to the function of the cell site simulator:

[DETECTIVE HALEY]: What happened in this case was, Detective Sp[innato] from our WATF, which is the Warrant Apprehension Unit, apparently interviewed somebody -- got a phone number. He then responds down here to the Circuit Court . . . and gets a Court Order signed.

He then sends the Court order down to our office, depending on what the carrier is, Verizon, Sprint, T-Mobile, AT&T. We then send it to them. I ask for subscriber information, call-detail records.

They provide us with GPS locations, in this case. And once we get all the information, then we have equipment that we can go out and locate cell phones.

[DEFENSE COUNSEL]: Okay. When you say, we have equipment that we can locate cell phones, you're talking about the Stingray equipment, is that what was used in this case?

[DETECTIVE HALEY]: Yeah, it's called the Hailstorm. It used to be -- Stingray is kind of first generation.

\* \* \*

[DEFENSE COUNSEL]: Tell me what the Hailstorm does.

[DETECTIVE HALEY]: What we get from the phone company is the subscriber information. So, when we get the subscriber information, it has a [sic] identifier on there, if you will, a serial number. We put that into the Hailstorm equipment. And the Hailstorm equipment acts like a cell tower. So, we go into a certain area, and basically, the equipment is looking for that particular identifier, that serial number.

[DEFENSE COUNSEL]: Okay. And so, if a person is inside of a home, that equipment peers over the wall of the home, to see if that cell phone is behind the wall of that house, right?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: And it sends an electronic transmission through the wall of that house, correct?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: Did you get a separate search warrant for that search into the home?

[DETECTIVE HALEY]: You'd have to talk to Detective Spinnato about that. Because he's the one that got the Court Order signed.

[DEFENSE COUNSEL]: Did you do the search? You conducted the equipment in this -- you operated --

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: -- the equipment?

[DETECTIVE HALEY]: Yes.

\* \* \*

[DEFENSE COUNSEL]: Tell me all of the information the Hailstorm can retrieve from a phone.

[DETECTIVE HALEY]: It's going to retrieve, like I said before, the serial number of the phone, depending on what kind of phone it is. It's going to -- there's [sic] different identifiers. Like for Sprint, in this case, it's called the MSID. And that's like a ten-digit -- like a ten-digit number. So, it's retrieving that. And there's also the electronic serial number. It's retrieving that. And that's really it.

[DEFENSE COUNSEL]: Can you capture the telephone calls as they're being made?

[DETECTIVE HALEY]: No.

[DEFENSE COUNSEL]: And how do you know where the phone -- and it doesn't capture any data on the phone?

[DETECTIVE HALEY]: No.

[DEFENSE COUNSEL]: Are you sure?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: So, how do you get information about where the phone is on the machine?

[DETECTIVE HALEY]: Because when it captures that identifier that you put into the machine or the equipment, it then tells you -- it looks like a clock on the equipment. And it tells you where the signal's coming from, like 12, 1, 2, 3 o'clock (indicating). And it will give you like a reading. Like if it says 1:00 at like an 80, well, then you know that you're kind of close to it. But if it says 1:00 at like a 40, then you know that you're probably within, I don't know, probably, you know, 20 yards of it.

[DEFENSE COUNSEL]: The person doesn't have to be using their phone for you to get that information, do they?

[DETECTIVE HALEY]: Actually, if they're on their phone, then they're already connected to -- in this case, the Sprint network. And we're not going to be able to pull them off of that until they're -- until they hang -- until they hang the call up.

[DEFENSE COUNSEL]: So, they hang the call up. And the phone can be in their pocket, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: And then you're reaching in to grab an electronic signal about where that phone is? It's not pinging, in other words, right?

\* \* \*

MR. HALEY: Like I said, our equipment acts like a cell tower. So, it draws the phone to our equipment.

[DEFENSE COUNSEL]: But you just said, if the person's on the phone, your equipment won't work, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: So, it doesn't act like a cell tower, because you can find the phone only when they are not on the phone, correct?

[DETECTIVE HALEY]: Well, I would say it does act like a cell tower, because the only time that you're going to connect -- the only time that you're going to connect to the network, or to a tower is when you go to try to use it.

[DEFENSE COUNSEL]: But you're connecting to where the phone is, when they're not on the phone, didn't you just say that

[DETECTIVE HALEY]: Maybe I'm getting confused, or I'm not understanding what you're asking me.

[DEFENSE COUNSEL]: My question to you was, for example, I have my phone in my pocket. And I'm sitting in my house, right?

[DETECTIVE HALEY]: Okay.

[DEFENSE COUNSEL]: And you want to know where I am, correct?

[DETECTIVE HALEY]: Okay.

\* \* \*

[DEFENSE COUNSEL]: When I am not on my phone, you will drive by my house, and you will get a signal from my phone indicating where I am, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: If I am using the phone, you won't get that signal, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: So, the phone cannot be in use. You are searching for my phone as you're driving through my neighborhood, right?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: And in order to get to my phone, you are sending an electronic signal into my house, right?

[DETECTIVE HALEY]: Yes.

When the hearing resumed, the court made several preliminary findings, and invited counsel to respond. In regard to the pen register/trap & trace order, the court observed:

I don't find that Judge Williams' order is invalid as a pen register or trap and trace, but I do find that the order does not authorize the use of Hailstorm and I . . . invite the State to tell me otherwise.

\* \* \*

So this is very different from an order authorizing, for example, GPS or cell site information, because that is information that's generated by the phone. And my understanding of this equipment is essentially that it's forcing the phone to emit information, or its taking information from the phone that the phone is not sort of on its own generating at the time which is very different.

On the issue of whether Andrews's arrest was lawful, the parties acknowledged that a valid warrant was outstanding for his arrest. However, the court questioned whether, as argued by defense counsel, Andrews's presence at 5032 Clifton Avenue "or the warrant they got as a result of him being there is fruit of the poisonous tree because there was a violation of his Fourth Amendment rights by [Det. Haley] using the Hailstorm on this phone to locate him at that residence in the first place." Looking then to the application for the warrant to search 5032 Clifton Avenue, the court noted that there was no independent corroboration for the warrant because, "all it says he was located at this address and so we want to search this address. I mean that's really all it says."

After hearing argument, the circuit court found that "the use of the Hailstorm violates the Defendant's Fourth Amendment rights," and "any information generated from the use of the Hailstorm [must] be suppressed." The court continued on the record:

And so just so that I'm clear, it means that the jury cannot hear any testimony or evidence about information obtained from the Hailstorm, obtained through the Hailstorm device. And just so that I'm clear, it's my

understanding that the Hailstorm device is what told the police that the Defendant was at that location.

And so that includes any testimony or evidence then that the Defendant was at that location, if that's what -- because that's what the Hailstorm told the police. And so the jury would be prohibited from hearing evidence or testimony of that. It does not invalidate the arrest or the search [incident to] the arrest with the phone that's in his pocket.<sup>[5]</sup>

Now anything that came off the phone, again if it came through the Hailstorm device it is suppressed. There can be no evidence or testimony about it. And then again, any police knowledge that the Defendant was at that location again also suppressed, so the jury would not be able to hear any evidence or testimony of that.

So then that leaves us with the fruit of the poisonous tree argument for the search and seizure warrant. I reviewed the warrant and it literally says the Defendant was in there so now we need a warrant. And information generated from the use of the Hailstorm be suppressed, that's all that it is. And so I analyze this different, a little bit different from a normal sort of motion to suppress a search and seizure warrant or even *Franks* in terms of standing.

I don't -- I understand the State's argument in terms of standing and this not being his residence, and the Defense's argument that he was at a minimum an overnight guest and has some reasonable expectation of privacy. I don't think I need to reach those issues because the warrant is really just fruit of the poisonous tree of the illegally obtained information about the Defendant's location. That's what it is.

And so I am granting the suppression of that for that very reason. And so that the record is clear -- and I know that the State is asking to take an appeal, the record is clear. The ruling of the Court is that the government violated the Defendant's Fourth Amendment rights by essentially using the Hailstorm to locate him at that residence.

The State noticed its appeal on September 3, 2015.

---

<sup>5</sup> Mr. Andrews did not challenge the legality of his arrest or search incident to arrest, either in the circuit court or before this Court. He did, however, seek to suppress the cell phone, but that motion was denied and Mr. Andrews did not file a cross-appeal to contest that ruling.



## DISCUSSION

### Motion to Dismiss

Before turning to the merits, we must address Andrews’s motion to dismiss this appeal on the ground that the notice of appeal was defective, and therefore, not filed within the time prescribed by Rule 8-202.

The State filed its notice of appeal on September 3, 2015; however, the signed certificate of service—indicating that a copy of the notice was “mailed first-class, postage prepaid” on that same day—failed to list the party that was served. Andrews acknowledges that a copy of the notice was delivered to the Office of the Public Defender on September 4, 2015. Nevertheless, Andrews argues that the State’s notice did not comply with the certificate of service requirements of Maryland Rule 1-323, and that the clerk should not have accepted the filing. Consequently, according to Andrews, no valid notice of appeal was filed in this case. The State concedes that the failure to name the party to be served was a defect in the certificate of service, but maintains the clerk was required to accept the filing because the certificate complied with the literal requirements of Rule 1-323. The State urges that it would be improper to dismiss the appeal because there is no dispute that the opposing party was served in a timely fashion.

Maryland Rule 1-323 directs that the court clerk may not accept for filing a pleading or other paper requiring service, unless it is accompanied by “an admission or waiver of service or a signed certificate showing the date and manner of making service.” In *Director of Finance of Baltimore City v. Harris*, this Court addressed whether a certificate of service that failed to identify all the persons upon whom service was required should have been

rejected for filing by the court clerk. 90 Md. App. 506, 513-14 (1992). Looking to the 1984 revision of the Maryland Rules that produced the current Rule 1-323, this Court observed:

Under the old Rule, the clerk may have had some obligation to determine whether the certificate actually showed service on the “opposite party.” But, as noted, that obligation, if it ever did exist, has been eliminated. . . . The obligation of the clerk under the current Rule is simply to assure that there is, in fact, an admission, a waiver, or a certificate showing the date and manner of service. If such a certificate is attached to the paper, the clerk must file the paper, leaving it then to the parties or the court to deal with any deficiency.<sup>[6]</sup>

More recently, in *Lovero v. Da Silva*, this Court clarified that, by mandating that proof of service (or a waiver of service) appear on each pleading or paper, “Rule 1-323 assures the court . . . that each party has been duly notified before action is taken by the court in response to or as a result of the subject pleading or paper.” 200 Md. App. 433,

---

<sup>6</sup> This Court further illuminated the evolution of Rule 1-323 stating:

Rule 1-323 is derived ultimately from Rule 1(a)(2), Part Two, V, of the General Rules of Practice and Procedure, adopted by the Court of Appeals and approved by the General Assembly pursuant to 1939 Md. Laws, ch. 719, § 35A. Rule 1(a)(2) provided, in relevant part, that a paper “shall not be received and filed by the clerk of the court unless accompanied by an admission or proof of service of a copy thereof *upon the opposite party or his attorney of record* in accordance with this rule.” (Emphasis added.) Other parts of the Rule prescribed how service was to be made. That Rule was carried over into the Maryland Rules of Procedure as Rule 306 a.2., which stated that “[t]he clerk shall not accept or file any paper requiring service other than an original pleading unless it is accompanied by an admission or proof of service of a copy thereof *upon the opposite party, or his attorney of record.*” (Emphasis added.)

Until the 1984 revision of the Maryland Rules, the Rule remained in that form.

*Harris*, 90 Md. App. at 511-12.

446 (2011). We determined that Lovero’s notice of appeal should have been rejected by the clerk, explaining that

[w]here, as in the instant case, the notice of appeal contains no proof of service whatsoever, we have no basis upon which to conclude that the notice of appeal was served on the opposing party or parties. Indeed, it is undisputed here that the Notice of Appeal was never served on Da Silva.

*Id.* at 449.

In the present case, there is no dispute that the notice was served on defense counsel. Indeed, the State made it clear at the August 20 hearing that it would be filing an appeal as reflected in the court’s ruling; “and so that the record is clear – and I know that the State is asking to take an appeal, the record is clear.” It is also clear now that, although the omission in the certificate of service is a defect, the certificate met the literal requirements of Rule 1-323—it provided the date and manner of service. Where there is no evidence that Andrews was prejudiced or that the course of the appeal was delayed by a defect, “it is the practice of this Court to decide appeals on the merits rather than on technicalities.” *Bond v. Slavin*, 157 Md. App. 340, 352-53 (2004). *Cf. Williams v. Hofmann Balancing Techniques, Ltd.*, 139 Md. App. 339, 356-57 (2001) (holding that the appellant’s failure to identify one of the appellees on his notice of appeal did not deprive this Court of jurisdiction). To be sure, the Court of Appeals has observed that “[o]ur cases, and those of the Court of Special Appeals, have generally been quite liberal in construing timely orders for appeal.” *Newman v. Reilly*, 314 Md. 364, 386 (1988); *see also Lovero*, 200 Md. App. at 450-51 n.8 (and the cases cited therein) (recognizing that where a challenged notice of

appeal was timely filed the courts of Maryland construe the notice in favor of deciding the appeal on the merits). We deny Andrews’s motion to dismiss the appeal.

### **Standard of Review**

We review the grant of a motion to suppress based on the record of the suppression hearing, and we view the facts in the light most favorable to the prevailing party. *State v. Donaldson*, 221 Md. App. 134, 138 (citing *Holt v. State*, 435 Md. 443, 457, 78 A.3d 415 (2013)), *cert. denied*, 442 Md. 745 (2015). Further, “we extend ‘great deference’ to the factual findings and credibility determinations of the circuit court, and review those findings only for clear error.” *Id.* (citing *Brown v. State*, 397 Md. 89, 98 (2007)). But we make an independent, *de novo*, appraisal of whether a constitutional right has been violated by applying the law to facts presented in a particular case. *Williams v. State*, 372 Md. 386, 401 (2002) (citations omitted); *see also Brown*, 397 Md. at 98 (“[W]e review the court’s legal conclusions *de novo* and exercise our independent judgment as to whether an officer’s encounter with a criminal defendant was lawful.” (Citation omitted)).

## **I.**

### **Fourth Amendment Search**

In 1966, in the wake of prominent Congressional hearings on government invasions of privacy, Justice Douglas, dissenting in *Osborn v. United States* and *Lewis v. United States*, and concurring in *Hoffa v. United States*, observed:

We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions. Wiretapping and ‘bugging’ run rampant, without effective judicial or legislative control.

\* \* \*

Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man’s life at will.

*Osborn v. United States*, 385 U.S. 323, 340-43 (1966) (Douglas, J., dissenting).<sup>7</sup> Fifty years later we face the same concern—to what extent have advances in technology created an “age of no privacy.”<sup>8</sup>

The Fourth Amendment to the United States Constitution, made applicable to the States by the Fourteenth Amendment, *Mapp v. Ohio*, 367 U.S. 643, 655 (1961), provides:

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.

U.S. Const. amend. IV. The first clause protects individuals against unreasonable searches and seizures,<sup>9</sup> see *Katz v. United States*, 389 U.S. 347, 359 (1967) (“Wherever a man may

---

<sup>7</sup> The question presented in *Osborn*, as cast by Justice Douglas, was “whether the Government may compound the invasion of privacy by using hidden recording devices to record incriminating statements made by the unwary suspect to a secret federal agent.” *Osborn*, 385 U.S. at 340.

<sup>8</sup> See also *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) (“Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.”).

<sup>9</sup> Although the parties do not present their arguments under the Maryland Constitution, Declaration of Rights, we note that Article 26—governing warrants for search and seizure—is generally construed to be co-extensive with the Fourth Amendment. See *Upshur v. State*, 208 Md. App. 383, 397 (2012) (citing *Hamel v. State*, 179 Md. App. 1, 18 (2008)). Article 26 of the Maryland Declaration of Rights provides:

be, he is entitled to know that he will remain free from unreasonable searches and seizures[ ]”), and the second clause requires that warrants must be particular and supported by probable cause, *see Payton v. New York*, 445 U.S. 573, 584 (1980).

A “search” within the meaning of the Fourth Amendment occurs where the government invades a matter in which a person has an expectation of privacy that society is willing to recognize as reasonable. *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). As we made clear in *Raynor v. State*, “[t]he burden of demonstrating a ‘legitimate’ or ‘reasonable’ expectation of privacy includes both a subjective and an objective component.” 201 Md. App. 209, 218 (2011), *aff’d*, 440 Md. 71 (2014) (citation and footnote omitted). “[I]n order to claim the protection of the Fourth Amendment, a defendant must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable; *i.e.*, one that has ‘a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.’” *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143-44 n.12 (1978)).

---

That all warrants, without oath or affirmation, to search suspected places, or to seize any person or property, are grievous and oppressive; and all general warrants to search suspected places, or to apprehend suspected persons, without naming or describing the place, or the person in special, are illegal, and ought not to be granted.

The Fourth Amendment protects not against all intrusions as such, “but **against intrusions which are not justified in the circumstances, or which are made in an improper manner.**” *Maryland v. King*, 133 S. Ct. 1958, 1969 (2013) (emphasis added) (quoting *Schmerber v. California*, 384 U.S. 757, 768 (1966)). “Although the underlying command of the Fourth Amendment is always that searches and seizures be reasonable, *what is reasonable depends on the context within which a search takes place.*” *State v. Alexander*, 124 Md. App. 258, 265 (1998) (emphasis added in *Alexander*) (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985)). Subject to a few well-delineated exceptions, “warrantless searches ‘are *per se* unreasonable under the Fourth Amendment.’” *Quon*, 560 U.S. at 760 (2010) (quoting *Katz*, 389 U.S. at 357); *see also United States v. Karo*, 468 U.S. 705, 717 (1984) (citations omitted).

#### **a. Effects of the Nondisclosure Agreement**

Before we examine the reasonableness of the State’s intrusion *in context*, we address the nondisclosure agreement entered into between the State’s Attorney for Baltimore City and the Federal Bureau of Investigation in early August 2011 as a condition of BPD’s purchase of certain “wireless collection equipment/technology manufactured by Harris [Corporation].” The nondisclosure agreement provided, in part:

[T]o ensure that [] wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and **use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including b[ut] not limited to: in press release, in court documents, during judicial hearings**, or during other public forums or proceedings. Accordingly, the Baltimore City Police Department agrees to the following

conditions in connection with its purchase and use of the Harris Corporation equipment/technology:

\* \* \*

5. The Baltimore City Police Department and Office of the State’s Attorney for Baltimore City **shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State’s case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI.**

...

(Emphasis added). The agreement directs that in the event of a Freedom of Information Act request, or a court order directing disclosure of information regarding Harris Corporation equipment or technology, the FBI must be notified immediately to allow them time to intervene “and potential[ly] compromise.” If necessary “the Office of the State’s Attorney for Baltimore will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to provide, any information concerning the Harris Corporation wireless collection equipment/technology[.]”

We observe that such an extensive prohibition on disclosure of information to the court—from special order and/or warrant application through appellate review—prevents the court from exercising its fundamental duties under the Constitution. To undertake the Fourth Amendment analysis and ascertain “the reasonableness in all the circumstances of the particular governmental invasion of a citizen’s personal security,” *Terry v. Ohio*, 392



U.S. 1, 19 (1968), it is self-evident that the court must understand why and *how* the search is to be conducted. The reasonableness of a search or seizure depends ““on a **balance** between the public interest and the individual’s right to personal security free from arbitrary interference by law officers.”” *Pennsylvania v. Mimms*, 434 U.S. 106, 109 (1977) (emphasis added) (quoting *United States v. Brignoni-Ponce*, 422 U.S. 873, 878 (1975)). The analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use. A nondisclosure agreement that prevents law enforcement from providing details sufficient to assure the court that a novel method of conducting a search is a reasonable intrusion made in a proper manner and “justified by the circumstances,” obstructs the court’s ability to make the necessary constitutional appraisal. *Cf. King*, 133 S. Ct. at 1970 (“Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution. Urgent government interests are not a license for indiscriminate police behavior.”). In *West v. State*, this Court stated that “to assure that the purpose of the Fourth Amendment is upheld, police officers must provide details within affidavits when attempting to acquire search warrants, even if such information would seem to the police officer of trivial consequence at the time.” 137 Md. App. 314, 331 (2001).

As discussed further in Section III *infra*, it appears that as a consequence of the nondisclosure agreement, rather than apply for a warrant, prosecutors and police obtained an order under the Maryland pen register statute that failed to provide the necessary information upon which the court could make the constitutional assessments mandated in this case. The BPD certified to the court that pursuant to the order “the information likely

to be obtained concerning the aforesaid individual’s location will be obtained by learning the numbers, locations and subscribers of the **telephone number(s) being dialed or pulsed from or to the aforesaid telephone . . .**” However, the suppression court, having the benefit of Det. Haley’s testimony (reproduced above), learned that the BPD actually employed the Hailstorm device, which is capable of obtaining active real-time location information—far different from a pen register (a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument) or track and trace device (a device or process that captures the incoming electronic or other impulses that identify the originating number). *See* fn.2 *supra*.<sup>10</sup>

We perceive the State’s actions in this case to protect the Hailstorm technology, driven by a nondisclosure agreement to which it bound itself, as detrimental to its position and inimical to the constitutional principles we revere.

**b. What Constitutes a “Search”—Level of Intrusion  
and Expectation of Privacy**

The State argues that the use of a cell site simulator does not constitute a “search” under the Fourth Amendment. The State maintains that the circuit court’s decision “was based upon both factually unreasonable conclusions about how the cell site simulator worked in this case, and legally incorrect determinations about what constitutes a ‘search.’” The State acknowledges that the factual bases for the circuit court’s rulings are found in the June 4, 2015 testimony of Det. Haley. However, the State argues that Det. Haley’s

---

<sup>10</sup> It is not clear from the record whether Det. Haley’s testimony was authorized through written approval from the FBI as required in paragraph 5 of the nondisclosure agreement.

testimony “was necessarily rather summary,” and does not support the factual conclusions of the circuit court.

According to the State, the cell site simulator “acts like a cell tower, and waits to receive a signal bearing the target IMSI” [International Mobil Subscriber Identity]. The State maintains that, properly construed, Det. Haley’s testimony reveals that “the process of a cell phone sending its identifying information to a cell tower was indistinguishable from the process of a cell phone sending its identifying information to a cell site simulator.” The State asserts that the Hailstorm device “merely reads the ID number regularly transmitted by activated cell phones as part of their ordinary use” and “[w]hen the device detects a signal from the target phone, it notifies the operator the direction of the signal and the relative strength, allowing the operator to estimate the probable location of the phone.” Therefore, the State argues that no reasonable expectation of privacy existed in the information obtained by the Hailstorm device and no intrusion or “search” occurred.

Andrews countercharges that there was ample, explicit support in the record for the circuit court’s finding that the Hailstorm device operated by emitting a signal “through the wall of a house” and “into the phone” triggering the phone to respond to the device. Andrews argues that, through the use of an “active cellular surveillance device,” the State violated his reasonable expectation of privacy in the personal information contained and generated by his cell phone, without which the government would not have been able to discover his location inside the home.

Presumably because of the nondisclosure agreement discussed above, the State provided limited information regarding the function and use of the Hailstorm device. And

presumably, the State would have limited itself in this manner regardless of whether it relied on testimony from the prior hearing or produced live testimony before the suppression court.<sup>11</sup> Notwithstanding this, it is clear from Det. Haley’s testimony that “the Hailstorm equipment acts like a cell tower,” but, unlike a cell tower awaiting incoming signals, the Hailstorm is an active device that can send an electronic signal through the wall of a house and “draw[] the phone to [the] equipment.” Based on the direction and strength of the signal the Hailstorm receives from a cell phone in response, law enforcement can pinpoint the real-time location of a cell phone (and likely the person to whom it belongs) within less than 20 yards.

These points from Det. Haley’s testimony regarding the function of the Hailstorm device are consistent with what other courts and legal scholars have been able to discern about the device. Hailstorm, along with the earlier-model cell site simulator known as “StingRay,” to which Det. Haley referred, are far from discrete, limited surveillance tools. Rather, as described in a recent article in the Harvard Journal of Law and Technology cited by Appellee and the *amici*:<sup>12</sup>

This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices known more generically as “IMSI

---

<sup>11</sup> In a suppression hearing, “[w]here . . . the defendant establishes initially that the police proceeded warrantlessly, the burden shifts to the State to establish that strong justification existed for proceeding under one of the ‘jealously and carefully drawn’ exceptions to the warrant requirement.” *Jones v. State*, 139 Md. App. 212, 226 (2001) (citation omitted). Where the evidence presented is inconclusive, the consequence for the State is that the defendant wins. *Id.*

<sup>12</sup> In addition to the ACLU and EFF, Professor David Gray of the University of Maryland Francis King Carey School of Law filed a detailed and informative amicus brief in this case.

catchers,” is used by law enforcement agencies to obtain, directly and in real time, unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier.

\* \* \*

By impersonating a cellular network base station, a StingRay—a surveillance device that can be carried by hand, installed in a vehicle, or even mounted on a drone—**tricks all nearby phones and other mobile devices into identifying themselves (by revealing their unique serial numbers)** just as they would register with genuine base stations in the immediate vicinity. As each phone in the area identifies itself, the StingRay can determine the location from which the signal came.

Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134, 142, 145-46 (2014) (emphasis added; footnotes omitted).

The Supreme Court of Wisconsin examined whether law enforcement could obtain location data through cell site information or a StingRay pursuant to a warrant and, before holding that the warrant was sufficiently particularized, based on probable cause, and passed constitutional muster, observed:

A stingray is an electronic device that mimics the signal from a cellphone tower, which causes the cell phone to send a responding signal. If the stingray is within the cell phone’s signal range, the stingray measures signals from the phone, and based on the cell phone’s signal strength, the stingray can provide an initial general location of the phone. By collecting the cell phone’s signals from several locations, the stingray can develop the location of the phone quite precisely.

*State v. Tate*, 849 N.W.2d 798, 826 n.8 (Wisc. 2014) (citation omitted), *cert. denied*, 135 S. Ct. 1166 (2015); *see also, e.g., In re Application for Pen Register and Trap/Trace Device*

with *Cell Site Location Authority*, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) (defining an earlier-model device, the “Triggerfish,” as equipment that “enables law enforcement to gather cell site location information directly, without the assistance of the service provider”). We cannot say that the factual findings of the circuit court, in this case, were erroneous; they are firmly grounded in the testimony before that court, and the State has provided no evidence to the contrary.

In determining then whether a Fourth Amendment “search” occurred, we apply the court’s factual findings to the test pronounced in *Katz*, *supra*. Rather than limit the constitutional appraisal to a trespass analysis,<sup>13</sup> the *Katz* test requires a two-fold showing: “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” 389 U.S. at 361 (Harlan, J., concurring).<sup>14</sup> Even under the more flexible *Katz* test, however, rapid

---

<sup>13</sup> In *Olmstead v. United States*, the Supreme Court held that the government’s use of a wire-tapping device over an extended period of time did not constitute a violation of the Fourth Amendment because the wires were installed in a manner that did not constitute a trespass upon the property of the petitioners. 277 U.S. 438, 464 (1928). Thus, the Court stated that a Fourth Amendment violation would occur where there was a tangible, physical intrusion by the government. *Cf. id.* at 466. *Olmstead* was overruled in part by the Court in *Katz*. 389 U.S. at 353.

<sup>14</sup> Maryland appellate courts have, so far, only addressed the admissibility of historical CSLI obtained from a service provider. *See State v. Payne*, 440 Md. 680, 690-91 (2014) (stating that whether a detective “should have been qualified as an expert before being allowed to engage in the process of identifying the geographic location of the cell towers and the locations themselves depends on understanding just what are cell phone records and what their contents reveal.”); *Hall v. State*, 225 Md. App. 72, 91 (2015) (concluding that the State’s witness was properly qualified as an expert to testify regarding the mapping of appellant’s cell phone data); *Stevenson v. State*, 222 Md. App. 118, 129-30 (determining that a *Frye-Reed* hearing on admissibility of novel scientific evidence and expert scientific testimony was not required for admission of cellular tower “ping”

advancements in technology make ascertaining what constitutes a search under the Fourth Amendment ever more challenging.<sup>15</sup>

Charles Katz was charged with transmitting wagering information by telephone in violation of federal law. *Katz*, 389 U.S. at 348. He objected during his trial to the

---

evidence), *cert. denied*, 443 Md. 737 (2015); *Wilder v. State*, 191 Md. App. 319, 364 (2010) (holding that the admission of CSLI required the qualification of the sponsoring witness as an expert); *Coleman-Fuller v. State*, 192 Md. App. 577, 619 (2010) (same). Maryland courts have not previously addressed CSLI in the context of a Fourth Amendment challenge and have never addressed police use of cell site simulators or obtaining real-time CSLI. Because key factual distinctions in this case involve the function of Hailstorm and the ability of law enforcement to track a cell phone directly and in real time, our own cases provide limited guidance.

<sup>15</sup> See generally Renée McDonald Hutchins, *Tied Up In Knotts? GPS Technology and The Fourth Amendment*, 55 UCLA L. Rev. 409 (2007). Professor Hutchins notes that the Supreme Court has developed a differential treatment in its intrusiveness analysis under the Fourth Amendment based on the type of information revealed, explaining:

When gauging the objective reasonableness of various privacy expectations, the Court has leaned heavily on its assessment of the type of information revealed to segregate challenged surveillance technologies into two rough groups: sense-augmenting surveillance and extrasensory surveillance. Sense augmenting surveillance refers to surveillance that reveals information that could theoretically be attained through one of the five human senses. With regard to this type of surveillance, the Court has tended to find that simple mechanical substitutes for or enhancements of human perception typically trigger no Fourth Amendment concerns in cases in which human perception alone would not have required a warrant.

Extrasensory surveillance, conversely, is that which reveals information otherwise indiscernible to the unaided human senses. The Court has adopted a more privacy-protective view of this form of technologically enhanced police conduct. In fact, the case law suggests that surveillance of this type is largely prohibited in the absence of a warrant.

*Id.* at 432-33.

government's introduction of evidence collected by FBI agents who overheard and recorded his end of telephone conversations from inside a public telephone booth. *Id.* The agents had placed a recording device on the outside of the phone booth from which Katz placed his calls. *Id.* The government contended on appeal that their surveillance did not constitute a search prohibited by the Fourth Amendment because Katz was in a public location that was not constitutionally protected and because the technique they employed involved no physical penetration of the telephone booth. *Id.* at 352. Writing for the majority, Justice Stewart rejected the formulation of the issues by the parties, premised on whether the telephone booth was a "constitutionally protected area," and instructed that "[t]he Fourth Amendment protects people, not places . . . what [Katz] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 361 (citations omitted). The Court continued, stating that "once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id.* at 350, 353.

Almost 20 years after establishing in *Katz* that an examination of intrusiveness under the Fourth Amendment is not simply measured by physical invasion, the Supreme Court addressed the constitutionality of the government's surreptitious use of a radio transmitter to track the movements of a container to and inside a private residence. *United States v. Karo, supra*, 468 U.S. at 709-10. The physical installation of the transmitter was not at issue; rather, the question before the Court was "whether the monitoring of a beeper in a private residence, not open to visual surveillance, violates the Fourth Amendment



rights of those who have a justifiable interest in the privacy of the residence.” *Id.* at 714. Although the Court noted that the monitoring of an electronic device is “less intrusive than a full-scale search,” it, nevertheless, reveals information about the interior of the residence that the government “could not have otherwise obtained without a warrant.” *Id.* at 715.

The Supreme Court stated:

We cannot accept the Government’s contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual’s home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.

*Id.* at 716 (footnote omitted). Notably, the Court also soundly rejected the government’s contention that it should be able to engage in warrantless monitoring of an electronic device inside a private residence “if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper **wherever it goes** is likely to produce evidence of criminal activity.” *Id.* at 717 (emphasis added). The Court recognized limited exceptions to the general rule, such as in the case of exigency, but explained why in its view the government exaggerated the difficulties associated with obtaining a warrant:

The Government argues that the traditional justifications for the warrant requirement are inapplicable in beeper cases, but to a large extent that argument is based upon the contention, rejected above, that the beeper constitutes only a minuscule intrusion on protected privacy interests. The primary reason for the warrant requirement is to interpose a ‘neutral and detached magistrate’ between the citizen and ‘officer engaged in the often competitive enterprise of ferreting out crime.’

\* \* \*

The Government contends that it would be impossible to describe the ‘place’ to be searched, because the location of the place is precisely what is sought to be discovered through the search. [ ] However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested.

*Id.* at 717-18 (citing *Johnson v. United States*, 333 U.S. 10, 14 (1948)).

In *Kyllo*, *supra*, the Supreme Court considered whether a Fourth Amendment search had occurred when the government used a thermal imaging device to detect infrared radiation inside a home. 533 U.S. at 29-30. Federal agents, suspecting that Danny Kyllo was growing marijuana inside his home, were able to confirm areas of heat coming from high intensity lamps used to grow marijuana plants indoors. *Id.* At the threshold of his analysis, Justice Scalia, writing for the majority, observed:

It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

*Id.* at 33-34. The Court then noted that, although the *Katz* test—“whether the individual has an expectation of privacy that society is prepared to recognize as reasonable”—may be difficult to apply to some locations, such as telephone booths and automobiles—the expectation of privacy in the home had “roots deep in the common law.” *Id.* at 34.

In support of the use of its thermal imaging technology, the government in *Kyllo* argued that there was no “search” because the device detected ““only heat radiating from the external surface of the house[.]”” *Id.* at 35. The Supreme Court, however, cast aside

this contention as the kind of mechanical interpretation rejected in *Katz* and stated, “so also a powerful directional microphone picks up only sound emanating from a house—and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house.” *Id.* Rather than abandon *Katz* and take such a mechanical approach, the Court sought to adopt a rule “tak[ing] account of more sophisticated [surveillance] systems that are already in use or in development.” *Id.* at 35-36 (footnote omitted). Accordingly, the Court held that “[w]here . . . the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.” *Id.* at 40. Furthermore, the Court repeated the caveat of *Silverman v. United States*, that the “protection of the home has never been tied to the measurement of the quality or quantity of information obtained” for any invasion of the home, “‘by even a fraction of an inch’ [is] too much.” *Id.* at 37 (quoting *Silverman*, 365 U.S. 505, 512 (1961)).

From *Katz* to *Kyllo*, the Supreme Court has firmly held that use of surveillance technology not in general public use to obtain information about the interior of a home, not otherwise available without trespass, is a “search” under the Fourth Amendment. These decisions resolved to protect an “expectation of privacy that society is prepared to recognize as reasonable.” After *Kyllo*, however, the question remained whether electronic tracking or surveillance outside the home could constitute a search under the Fourth Amendment.

In *United States v. Jones*, the Supreme Court reviewed the use of a GPS tracking device affixed to the undercarriage of a vehicle to track the movements of the defendant over a period of 28 days. 132 S. Ct. 945, 948 (2012). The Court unanimously affirmed the United States Court of Appeals for the District of Columbia Circuit’s holding that the electronic location surveillance over a period of 28 days was a search and that admission of evidence obtained by the warrantless use of the GPS device violated the Fourth Amendment. The Court was unable, however, to reach full agreement as to the basis for its decision. *See id.* at 953 (majority opinion); 954 (Sotomayor, J., concurring); 967 (Alito, J., concurring in the judgment). Justice Scalia’s majority opinion found that a search occurred under the traditional, pre-*Katz* “trespass” rationale, but acknowledged that “[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.” *Id.* at 953 (emphasis in original).

Agreeing with Justice Brennan’s concurrence in *Knotts v. United States*, Justice Scalia expounded that “when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.” *Id.* at 951 (quoting *Knotts*, 460 U.S. 276, 286 (1983)). When law enforcement placed the GPS tracking system on Jones’s vehicle, without a warrant, the government physically invaded a constitutionally protected area, *id.* at 949, 952, and factors beyond trespass need not be considered to find there was a Fourth Amendment violation. *Id.* at 953-54. Justice Scalia explained that the common-law trespass test was essentially a minimum test and that the *Katz* test was “*added to*, not *substituted for*, the common-law trespassory test.” *Id.* at 952.

Justice Sotomayor revisited the *Katz* analysis in her concurring opinion, stating that, “even in the absence of a trespass, ‘a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.’” *Id.* at 954-55 (Sotomayor, J., concurring) (citations omitted). Recognizing that “[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion’s trespassory test may provide little guidance[,]” Justice Sotomayor opined that the unique attributes of GPS location surveillance will require careful application of the *Katz* analysis. *Id.* She urged the Court to update its understanding of peoples’ expectations of privacy in the information age:

GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. *See, e.g., People v. Weaver*, 12 N.Y.3d 433, 441–442, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009) (“Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on”). The Government can store such records and efficiently mine them for information years into the future. [*United States v. Pineda–Moreno*, 617 F.3d[ 1120,] 1124 [(9th Cir. 2010)] (opinion of Kozinski, C.J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: “limited police resources and community hostility.” *Illinois v. Lidster*, 540 U.S. 419, 426, 124 S.Ct. 885, 157 L.Ed.2d 843 (2004).

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may “alter the relationship between citizen and government in a way that is

inimical to democratic society.” *United States v. Cuevas–Perez*, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring).

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. See *Kyllo*, 533 U.S., at 35, n.2, 121 S.Ct. 2038; *ante*, at 954 (leaving open the possibility that duplicating traditional surveillance “through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy”). I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment’s goal to curb arbitrary exercises of police power to and prevent “a too permeating police surveillance,” *United States v. Di Re*, 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948).

*Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring) (footnote omitted).

Justice Alito, concurring only in the judgment, disagreed with the majority’s reliance on a trespassory theory. *Jones*, 132 S. Ct. at 958. Instead, Justice Alito found the appropriate inquiry to be “whether respondent’s reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.” *Id.* Justice Alito stated that the majority’s reasoning “disregard[ed] what is really important (the *use* of a GPS for the purpose of long-term tracking)” and “will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.” *Id.* at 962 (emphasis in original).

From the above precedent, we glean two broad principles regarding the Fourth Amendment analysis of surveillance technology. First, where surveillance technology is used without a warrant to obtain information about the contents of a home, not otherwise discernable without physical intrusion, there has been an unlawful search. *See Kyllo*, 533 U.S. at 34-35. Second, where the government has engaged in surveillance using “electronic signals without trespass[,]” the intrusion will “*remain* subject to *Katz* analysis.” *Jones*, 132 S. Ct. at 953 (emphasis in original). The Supreme Court has recognized, however, that cell phones present novel privacy concerns.

In *Riley, supra*, the Supreme Court made clear that a search of the information contained in a cell phone is subject to the warrant requirement regardless of its location. 134 S. Ct. at 2489-91. The Court held that even during a search incident to arrest, the government must first obtain a warrant before searching the digital contents of a cell phone found on the person being arrested. *Id.* at 2485-86.

Chief Justice Roberts described the modern cell phone as much more than a phone:

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person. The term “cell phone” is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag

behind them a trunk of the sort held to require a search warrant in *Chadwick, supra*, rather than a container the size of the cigarette package in *Robinson*.

*Id.* at 2489.

The State argues that its use of the Hailstorm here should be analogized to *Knotts*, 460 U.S. 276, wherein the Supreme Court upheld law enforcement officers' use of a radio transmitter to track the movements of a container, by automobile, to a defendant's home. In *Knotts*, the Court noted that "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways." *Id.* at 281. The Court concluded that:

A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

*Id.* at 281-82. Here, the State argues that because Andrews's cell phone was "constantly emitting 'pings' giving its location to the nearest cell tower, . . . there can be no reasonable expectation of privacy in [that] information" under *Knotts*.

The State's reliance on *Knotts*, however, is misplaced. In *Karo*, the Supreme Court clarified that in *Knotts* the electronic device "told the authorities nothing about the interior of Knotts' cabin." 468 U.S. at 715. Rather, the information obtained in *Knotts* was "voluntarily conveyed to anyone who wanted to look[.]" *id.* (quoting *Knotts*, 460 U.S. at 281), and the subsequent search warrant was also supported by "intermittent visual surveillance" of the cabin, *Knotts*, 460 U.S. at 279. As noted in *Kyllo*, the Supreme Court



has long recognized that “[v]isual surveillance [i]s unquestionably lawful because ‘the eye cannot by the laws of England be guilty of a trespass.’” 533 U.S. at 31-32 (quoting *Boyd v. United States*, 116 U.S. 616, 628 (1886)).

Here, there was no visual surveillance. The mere fact that police *could* have located Andrews within the residence by following him as he travelled over public thoroughfares does not change the fact that the police did not know where he was, so they could not follow him. Unlike *Knotts*, the information obtained in this case did reveal at least one critical detail about the residence; i.e., that its contents included Andrews’s cell phone, and therefore, most likely Andrews himself. Further, “pings” from Andrews’s cell phone to the nearest tower were not available “to anyone who wanted to look.” We find the surreptitious conversion of a cell phone into a tracking device and the electronic interception of location data from that cell phone markedly distinct from the combined use of visual surveillance and a “beeper to signal the presence of [the defendant’s] automobile to the police receiver” to track a vehicle over public roads. *See Knotts*, 460 U.S. at 282. Put simply, the information obtained by police in this case was not readily available and in the public view as it was in *Knotts*.

Cell site simulators, such as Hailstorm, can locate and track the movements of a cell phone and its user across both public and private spaces. Unchecked, the use of this technology would allow the government to discover the private and personal habits of any user. As Justice Sotomayor predicted in her concurring opinion in *Jones, supra*, we are compelled to ask “whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will,

their political and religious beliefs, sexual habits, and so on.” 132 S. Ct. at 956 (Sotomayor, J., concurring). We conclude that they do not.

We agree with the United States Court of Appeals for the Fourth Circuit in *United States v. Graham*, in declaring, “[w]e cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person.” 796 F.3d 332, 355 (4th Cir.), *reh’g en banc granted*, 624 F. App’x 75 (4th Cir. 2015).<sup>16</sup> Federal courts reviewing pen register & trace applications have similarly recognized a reasonable expectation of privacy in cell site location information. *See, e.g., In re the Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006) (“[D]etailed location information, such as triangulation and GPS data, ... unquestionably implicate Fourth Amendment privacy rights.”); *In re*

---

<sup>16</sup> The recent cell phone encryption battle between Apple and the United States Government illustrates how fervently people care about protecting their personal location information. In 2011, consumers learned that their iPhones stored months of data regarding Wi-Fi hotspots and cell towers around their location in a format that was not encrypted. The ensuing barrage of complaints caused Apple to revise its operating system to protect consumers’ location information. Apple, Inc. Press Release, Apple Q&A on Location Data (April 27, 2011) (available at <https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html>) [<https://perma.cc/PJ5V-KHGE>]. Apple refused to comply with a court order to create software to disable certain security protections of an iPhone. *See* Testimony of Bruce Sewell, *Encryption Tighrope: Balancing American’s Security and Privacy*, Hearing before the House Comm. on the Judiciary, 114th Cong. (March 1, 2016); Timothy B. Lee, *Apple’s Battle with the FBI over iPhone Security, Explained*, Vox (Feb. 17, 2016), <http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino> [<http://perma.cc/4MFA-JZ4D>].

*Application of the United States for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed)*, 402 F. Supp. 2d 597, 604–05 (D. Md. 2005) (recognizing that monitoring of cell phone location information is likely to violate a reasonable expectation of privacy)). We also accept the circuit court’s finding in this case that “no one expects that their phone information is being sent directly to the police department on their apparatus.”<sup>17</sup> Recognizing that the Fourth Amendment protects people and not simply areas, *Katz*, 389 U.S. at 353, we conclude that people have a reasonable expectation of privacy in real-time cell phone location information.

Moreover, because the use of the cell site simulator in this case revealed the location of the phone and Andrews inside a residence, we are presented with the additional concern that an electronic device not in general public use has been used to obtain information about the contents of a home, not otherwise discernable without physical intrusion. *See Kyllo*, 533 U.S. at 34-35. Under the applicable precedent, this is undoubtedly an intrusion that rises to the level of a Fourth Amendment “search.” *See id.* Indeed, “the Fourth Amendment draws a firm line at the entrance to the house[.]” *Id.* at 40 (citation and internal quotation marks omitted). Although we recognize that the use of a cell site simulator to track a phone will not always result in locating the phone within a residence, we agree with the Fourth Circuit’s observation that “the government cannot know in advance of obtaining

---

<sup>17</sup> As the Supreme Court stated in *Katz*, “[t]o read the Constitution more narrowly is to ignore the vital role that the ... telephone has come to play in private communication.” 389 U.S. at 352.

this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces." *Graham*, 796 F.3d at 350 (citation omitted). The United States District Court for the District of Maryland articulated the same concern when addressing the government's use of a particular cell phone as a tracking device to aid in execution of an arrest warrant. The district court stated:

Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation. Indeed, this is ostensibly the very characteristic that makes obtaining location data a desirable method of locating the subject of an arrest warrant. This also means, however, that **there is no way to know before receipt of location data whether the phone is physically located in a constitutionally-protected place. In other words, it is impossible for law enforcement agents to determine prior to obtaining real-time location data whether doing so infringes upon the subject's reasonable expectation of privacy and therefore constitutes a Fourth Amendment search.**

*In re Application of United States for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 540 (D. Md. 2011) (emphasis added).

It would be impractical to fashion a rule prohibiting a warrantless search only retrospectively based on the fact that the search resulted in locating the cell phone inside a home or some other constitutionally protected area. *See, e.g., Kyllo*, 533 U.S. at 38-39 (declining to adopt a Fourth Amendment standard that would only bar the use of thermal imaging to discern "intimate details" in the home because "no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." (emphasis in original)); *cf. Karo*, 468 U.S. at 718 ("We are also unpersuaded by the argument that a warrant should not be required because of the difficulty in satisfying the particularity

requirement of the Fourth Amendment.”). Such a rule would provide neither guidance nor deterrence, and would do nothing to thwart unconstitutional intrusions. *Cf. In re the Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F. Supp. 2d 294, 323 (E.D.N.Y.2005) (“Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking . . . which routinely require probable cause.” (Internal quotations and citations omitted)).

We determine that cell phone users have an objectively reasonable expectation that their cell phones will not be used as real-time tracking devices through the direct and active interference of law enforcement. We hold, therefore, that the use of a cell site simulator, such as Hailstorm, by the government, requires a search warrant based on probable cause and describing with particularity the object and manner of the search, unless an established exception to the warrant requirement applies.

We turn to consider whether such an exception applies in this case.

### **c. The Third Party Doctrine**

The State maintains that the “Third Party Doctrine” exception to the warrant requirement applied to the BPD’s use of Hailstorm to track down Andrews’s cell phone. The doctrine—providing that an individual forfeits his or her expectation of privacy in information that is turned over to a third party—finds its strongest expression in *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979).

In *Smith v. Maryland*, the Supreme Court was presented with the issues of whether the warrantless installation and use of a pen register to collect the telephone numbers dialed from a telephone at the petitioner’s home constituted a “search” within the meaning of the Fourth Amendment. 442 U.S. at 736-37. The Court described the function of pen registers, stating that they “disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purpose of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.” *Id.* at 741 (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977)). Accordingly, the Court narrowed the issue before it, stating:

Given a pen register’s limited capabilities, therefore, petitioner’s argument that its installation and use constituted a “search” necessarily rests upon a claim that he had a “legitimate expectation of privacy” regarding the numbers he dialed on his phone.

*Id.* at 742. In *United States v. Miller*, the Supreme Court held that no reasonable expectation of privacy existed once the owner of financial checks turned financial instruments over to a bank and “exposed [them] to [bank] employees in the ordinary course of business.” 425 U.S. at 442.

The State argues that the cell site simulator used in this case merely “detects the signal emitted by the cell phone, just as a regular cell tower would[,]” and, therefore, “the police used data that Andrews voluntarily shared with third parties—specifically his cell phone provider—to locate his phone.” The State maintains that, under *Smith* no Fourth Amendment “search” occurred because Andrews had no reasonable expectation of privacy in information he voluntarily transmitted to a third party. The State contends that, by

carrying and using a cell phone that regularly communicates with nearby cell towers, Andrews assumed the risk that the information transmitted to the cell towers would be revealed to the police.

According to Andrews, the third-party doctrine of *Smith v. Maryland*, is inapplicable because “a cell phone user takes no conscious, voluntary action to constantly share location information with a third party.” Andrews maintains that the Supreme Court in *Smith* reached its conclusion using a specific line of reasoning, recognizing that “telephone subscribers ‘realize’ that they send dialed numbers to the telephone company” and by virtue of those numbers appearing on their monthly bills “subscribers ‘realize’ that the dialed numbers are recorded by the telephone company.” Andrews contends that the same cannot be said in the instant case. As Andrews points out, the Court in *Smith* focused on the actual knowledge attributed to telephone users and stated:

All telephone users realize that they must “convey” phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

*Id.* at 742. In that context, the court determined that because the “petitioner voluntarily conveyed to [the telephone company] information that it had facilities for recording and that it was free to record[,] . . . petitioner assumed the risk that the information would be divulged to police.” *Id.* at 745.

Although the Supreme Court’s decision in *Smith* has been applied broadly, *see, e.g., United States v. Bynum*, 604 F.3d 161, 162-64 (4th Cir. 2010) (upholding the government’s

use of a subpoena to obtain a website user’s name, email address, telephone number, and physical address—all information that the user entered on the website when he opened his account—from a website operator), it remains that a party must **voluntarily convey** information to a third-party, before there is no longer a reasonable expectation of privacy in that information. *Cf. Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (“This approach [in *Smith*] is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.” (citation omitted)). Recently, in *United States v. Graham, supra*, the Fourth Circuit addressed the application of the third-party doctrine to CSLI and stated:

[The precedents] simply hold that a person can claim no legitimate expectation of privacy in information she voluntarily conveys to a third party. It is that voluntary conveyance—not the mere fact that the information winds up in the third party’s records—that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone user does not “convey” CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement.

796 F.3d at 354 (footnote omitted).

We agree, once again, with the *Graham* court and join in the view shared by other courts that, “[t]he fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by ‘choosing’ to carry a cell phone must be rejected.” *Graham*, 796 F.3d at 355-56 (quoting *In re United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809



F. Supp. 2d 113, 127 (E.D.N.Y. 2011)). Cell phone users do not actively submit their location information to their service provider.

In the present case, there was no affirmative act like “dialing.” This is made abundantly clear by Det. Haley’s testimony stating that “if they’re on the phone, then they’re already connected to . . . the [] network[, a]nd we’re not going to be able to pull them off of that until . . . they hang up the call.” Det. Haley’s testimony reveals that, in the event that an individual is actively using the cell phone to knowingly transmit signals to nearby cell towers, the cell site simulator will not be able to access the phone.

The pin-point location information that led to finding Andrews was obtained directly by law enforcement officers and not through a third-party. It is not the case that Andrews’s cell phone transmitted information to the service provider that was then recorded and shared with law enforcement. Thus, it cannot be said that Andrews “assumed the risk” that the information obtained through the use of the Hailstorm device would be shared by the service provider as in *Smith*. The function of the Hailstorm device foreclosed that possibility. When asked “how do you get information about where the phone is on the [Hailstorm] machine,” Det. Haley responded: “[W]hen [Hailstorm] captures that identifier that you put into the machine or the equipment, it then tells you . . . where the signal’s coming from[.]” Under the facts of this case, the ultimate location data relied on by the police was never transmitted to a third party voluntarily by Andrews. Because there was no third-party element to the use of the Hailstorm by the BPD to locate Andrews, *Smith* is inapposite. We conclude the Third Party Doctrine does not apply in this case.

## II.

### Standing

One of the State's primary arguments on appeal is that Andrews lacks standing to challenge the search of 5032 Clifton Avenue. The State argues that once it challenged Andrews's standing to protest the search of 5032 Clifton Avenue, the burden was on Andrews to put on evidence during the suppression hearing to establish Andrews's "basis for claiming he had a reasonable expectation of privacy in the contents of someone else's home." The State posits the suppression court erred in "finding that there was no need to prove standing."

Certainly, "[t]he burden is on the defendant to show standing; it is not on the State to show non-standing." *State v. Savage*, 170 Md. App. 149, 177 (2006). In *Savage*, however, this Court clarified that standing "[i]s exclusively a threshold question of applicability, concerned only with the coverage by the Fourth Amendment of the defendant who seeks to raise a Fourth Amendment challenge." *Id.* at 174. Thus, the burden on a proponent of a motion to suppress is to establish "*that his own Fourth Amendment rights were violated by the challenged search or seizure.*" *Id.* at 175 (emphasis in *Savage*) (quoting *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978)).

Andrews points out that the State "failed to respond in any meaningful way" to his motion to suppress, and did not raise the issue of standing to challenge the search of 5032 Clifton Avenue until well into the June 4, 2015 suppression hearing. Andrews asserts that it was the State's suggestion that the parties stipulate that the issues before the court be decided based on the transcripts, the arrest warrant, the pen register\trap & trace

application, and the search warrant. Andrews contends the State did not raise the standing issue until after the fact-finding portion of the hearing had concluded. At that time, the court requested that Andrews address the issue, and defense counsel made a proffer that Andrews was an overnight guest at 5032 Clifton Avenue and offered to put him on the stand to provide supporting testimony.<sup>18</sup> Andrews argues that the State waived any argument regarding standing, pointing to the State's delay, its failure to challenge his proffer, and its concession that its trial theory was the fact "that [Andrews] has some interest [in 5032 Clifton Avenue] and that is why the gun from this crime, the murder weapon, was there with him."

We need not pursue the nuances of the parties' "standing" argument as they have framed the issue. We have already determined that Andrews had a reasonable expectation of privacy in his aggregate and real-time location information (CLSI) contained in his cell phone. *See Rakas*, 439 U.S. at 139-140 (stating that "the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing[.]" and

---

<sup>18</sup> It is plain that an overnight guest has a legitimate expectation of privacy in his host's home and "may claim the protection of the Fourth Amendment." *Carter*, *supra*, 525 U.S. at 90; *Savage*, 170 Md. App. at 188-89. As Andrews points out, defense counsel made a proffer that Andrews was an overnight guest and offered to put testimony to that effect on the record. The State has not seriously challenged Andrews's connection to the residence, but seeks merely to assert that his unopposed proffer was not sufficient to rebut their late challenge. We observe that—after the State sought to rely on earlier transcripts to provide necessary testimony, failed to challenge standing during the evidentiary portion of the suppression hearing, and left uncontroverted Andrews's proffer that he was an overnight guest—Andrews's proffer under the circumstances may have been sufficient to counter the State's standing argument.

“[t]hat inquiry in turn requires a determination of whether the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect.”). The search warrant search for 5032 Clifton Avenue was based solely on constitutionally tainted information. As the suppression court explained, “I reviewed the warrant and it literally says the Defendant was in there so now we need a warrant. And information generated from the use of the Hailstorm [is to] be suppressed, that’s all that it is.” Because the Fourth Amendment violation of Andrews’s privacy in his real-time CSLI provided the only nexus to 5032 Clifton Avenue, Andrews was entitled to challenge that search. *See Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963) (stating that, in determining whether evidence is fruit of the poisonous tree, “the more apt question in such a case is whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.” (citation and internal quotation marks omitted)). For the foregoing reasons, Andrews had standing to challenge the “search” of 5032 Clifton Avenue.

### **III.**

#### **The Warrant Requirement**

Having determined that the government’s use of a cell site simulator to obtain location information directly from an individual’s cell phone is a “search” under the Fourth Amendment, and, therefore, requires a warrant based on probable cause, we now examine the state’s reliance on the pen register\trap & trace order issued by the circuit court. First, we examine whether the Maryland pen register statute authorized the use of a cell site

simulator. Second, we examine whether the putative pen register\trap & trace order in this case operated as the equivalent of a warrant as the State contends.

**a. The Maryland Pen Register Statute Does Not Authorize the Use of Cell Site Simulators Such as Hailstorm**

The function of the Hailstorm device, as illuminated by testimony before the suppression court, places it outside the statutory framework of the Maryland pen register statute. The statute authorizes the use of the following surveillance methods defined in CJP §10-4B-0.1:

**Pen register**

(c)(1) “Pen register” means a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.

(2) “Pen register” does not include any device or process used:

- (i) 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 the provider or any device used by a provider or customer of a wire communication service for cost accounting or other similar purposes in the ordinary course of its business; or
- (ii) To obtain the content of a communication.

**Trap and trace device**

(d)(1) “Trap and trace device” means a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.

(2) “Trap and trace device” does not include a device or process used to obtain the content of a communication.

**Wire communication, electronic communication, and electronic communication service**

(e) “Wire communication”, “electronic communication”, and “electronic communication service” have the meanings stated in § 10-401 of this title.

The statute specifies that any order issued must identify, if known, “the person to whom is leased or in whose name is listed the **telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.**” CJP § 10-4B-04(b)(1) (emphasis added).

Construing the plain language of CJP § 10-4B-01, we determine that it does not, on its face, apply to the use of cell site simulators. A “pen register” is “a device or process that records . . . signaling information transmitted by an instrument . . . **from which a wire or electronic communication is transmitted.**” CJP § 10-4B-01(c)(1) (emphasis added). As discussed above, the Hailstorm device does not passively intercept an electronic communication that has been transmitted. Rather, it initiates contact with a cell phone and traces the signal received in response. A “trap and trace device” is a “device or process that captures the **incoming electronic or other impulses** that identify the originating number or other dialing, routing, addressing, and **signaling information reasonably likely to identify the source of a wire or electronic communication.**” CJP § 10-4B-01(d)(1) (emphasis added). The function of the Hailstorm device—to shower an electronic barrage of signals into a target area to actively engage the target cell phone—goes well beyond the bounds of the pen register statute which by its terms is limited to authorizing devices that record or identify the source of a communication or capture an originating number.

The Maryland pen register statute has been examined in only one reported opinion by a Maryland appellate court.<sup>19</sup> *See Chan v. State*, 78 Md. App. 287, 293 (1989)

---

<sup>19</sup> In the federal district court in *United States v. Wilford*, a defendant more recently argued that cell phone pingging was not authorized by Maryland’s pen register statute. 961

(upholding the use of a trap and trace device pursuant to a court order to obtain data from over 5,000 calls over an eighty-day period). In *Chan*, although this Court determined that the newly enacted Maryland pen register statute was not applicable because it did not take effect until July 1, 1988, it stated that the new statute “unquestionably cover[ed]” the “trap and trace” of incoming calls and observed:

In response to the Electronic Communications Privacy Act of 1986 passed by the Federal Congress, the Maryland General Assembly moved for the first time to regulate “pen registers” and “trap and trace” devices by Chapter 607 of the Acts of 1988. The new regulation is not part of the “Wiretapping and Electronic Surveillance” subtitle but is a separate subtitle of its own, 4B, dealing with the distinct subject matter of “Pen Registers and Trap and Trace Devices.” **Its provisions and its wording are virtually verbatim with those of its Federal counterpart.**

*Id.* at 308 (emphasis added).

In 2001, Congress amended the definition of the term “pen register” in the federal counterpart as part of the USA PATRIOT Act. *See* PL 107–56, October 26, 2001, 115 Stat 272. Subsequently, in 2002, the Maryland pen register statute was also amended to the current versions, reproduced above. 2002 Md. Laws, ch. 100 (H.B. 1036). Notably, since

---

F. Supp. 2d 740, 768 (D. Md. 2013), *on reconsideration in part* (Nov. 27, 2013). In that case, the defendant maintained that the statutory language “is limited to providing law enforcement numbers that dialed into the target phone and numbers dialed out,” but does “not contemplate” the use of a cell phone as a “physical locator/tracking device.” *Id.* at 769. The district court noted that “[n]o judicial decision offers any guidance as to the scope of the Maryland statute with respect to ping[ing].” *Id.* However, rather than address whether the collection of CSLI was authorized by the pen register statute, the district court accepted that contention *arguendo* and, instead, based its holding on the unavailability of suppression as a remedy for violation of the statute. *Id.* at 770.

*Chan* was decided in 1989, the wording of the Maryland statute remains virtually verbatim with its federal counterpart. *See* 18 U.S.C. § 3127; 18 U.S.C. § 2510.

Looking then, at the federal statutory scheme, we note that the federal Communications Assistance for Law Enforcement Act (“CALEA”), which delineates a telecommunications carrier’s duty to cooperate in the interception of communications for law enforcement purposes, provides that “with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), **such call-identifying information shall not include any information that may disclose the physical location of the subscriber** (except to the extent that the location may be determined from the telephone number).” 47 U.S.C. § 1002 (2015) (emphasis added). Thus, federal law specifies that the federal equivalent to the Maryland pen register statute does not authorize location information. Rather, the federal scheme allows the government to use a mobile tracking device through warrant or other order as contemplated in 18 U.S.C. § 3117 and Federal Rule of Criminal Procedure 41.

Although there are no reported opinions that address whether the collection of real-time cell site location information (CSLI) is authorized under the Maryland’s pen register statute, numerous federal courts construing the virtually identical federal statutes have found no statutory authorization for obtaining such information without demonstrating probable cause. In 2005, the United States District Court for the Southern District of Texas held that the government must demonstrate probable cause and obtain a search warrant to obtain real-time CSLI. *In re Application for Pen Register & Trap/Trace Device with Cell*



*Site Location Auth.*, 396 F. Supp. 2d 747, 759 (S.D. Tex. 2005). Construing the federal statutes, the district court stated:

Tracking device information such as cell site data is plainly not a form of electronic communication at all.

\* \* \*

This type of surveillance is unquestionably available upon a traditional probable cause showing under Rule 41 [for a mobile tracking device]. On the other hand, permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected.

*Id.* at 759, 765. See also *In re Application of the United States for an Order Authorizing Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2006) (holding that the government was not entitled to real-time CSLI by statute and thus, was required to make a “showing that there exists probable cause to believe that the data sought will yield evidence of a crime.”). Directly addressing the use of a cell site simulator (such as Stingray or Hailstorm) to obtain real-time CSLI for tracking purposes, the District Court for the Southern District of Texas determined that, rather than merely capturing signaling information as contemplated in the federal pen register statute, the use of a cell site simulator constituted a mobile tracking device. *In re the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012).

We acknowledge that law enforcement has long relied on pen register\trap & trace orders for valid and vital investigative purposes. They will continue to do so. The pen register statute, however, is limited by its terms and is not intended to apply to other, newer

technologies. Thus we hold that a pen register\trap & trace order is not sufficient to authorize use of the Hailstorm.<sup>20</sup>

### **Criminal Procedure § 1-203.1**

Although at the time Andrews was arrested Maryland did not have a corollary to the provision in Federal Rule of Criminal Procedure 41 that specifically authorizes issuance of a warrant for a mobile tracking device, Maryland has since enacted a statute authorizing law enforcement to obtain real-time CSLI, effective October 1, 2014. Maryland Code (2001, 2008 Repl. Vol., 2014 Supp.) Criminal Procedure Article (“CP”) § 1-203.1. The statute provides that a court may issue an order allowing an officer to obtain real-time location information from an electronic device based on probable cause that:

- (i) a misdemeanor or felony has been, is being, or will be committed by the owner or user of the electronic device or by the individual about whom location information is being sought; and
- (ii) the location information being sought:

- 1. is evidence of, or will lead to evidence of, the misdemeanor or felony being investigated; or

---

<sup>20</sup> Federal law enforcement agencies have recognized that they need to obtain warrants rather than rely on less rigorous legal authorizations before utilizing cell site simulators. On September 3, 2015, the United States Justice Department of Justice announced a new policy setting forth required practices with respect to the treatment of information collected through the use of cell site simulators and stated:

While the department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, **law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator.**

*Justice News, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, DOJ 15-1084 (2015) (emphasis added).

2. will lead to the apprehension of an individual for whom an arrest warrant has been previously issued.

CP § 1-203.1(b)(1). The Fiscal and Policy Note prepared by the Department of Legislative Services for the General Assembly concerning this statute when it was first proposed, recognized that law enforcement officers were using the Maryland pen register statute to obtain cell phone-related information. It explained that the proposed statute would specifically authorize the capture of CSLI in accord with several recent federal court decisions finding that probable cause was needed to obtain such information. Fiscal and Policy Note (Revised), Senate Bill 698, Criminal Procedure – Electronic Device Location Information – Order (2014). The fiscal and policy note also contemplated the use of cell site simulators and stated:

While cell phone records are usually obtained from a cell phone provider, technology is making it possible for law enforcement to bypass these companies altogether. Certain devices allow law enforcement to obtain location data by imitating a cell phone tower, getting a phone to connect with it, and measuring signals from the phone to pinpoint its location. The device, which is being used by the Federal Bureau of Investigation, the military, and local law enforcement, is known by several trade names, including StingRay, KingFish, and LoggerHead.

Notably, CP § 1-203.1 contains safeguards and limitations not found in the Maryland pen register statute, including a thirty-day durational limit on the collection of location information unless an extension is sought on continuing probable cause, and a provision requiring notice to the user or owner of the monitored device within 10 days absent a showing of good cause to delay. CP § 1-203.1(c) & (d).

The parties have briefed extensively their view of the meaning and application of CP 1-203.1. Other than to provide context for the history of the Maryland pen register

statute and our conclusion that it was not intended to cover cell site simulators, we do not address the application of CP 1-203.1 and decline to opine as to whether an order under CP 1-203.1 will suffice to satisfy the requirements of a warrant based on probable cause.

In sum, we conclude that the purpose of Maryland's pen register statute is to capture information resulting from two-way, electronic or wire communications. Nothing in the plain language of CJP § 10-4B-01 *et seq.* suggests that it was ever intended to allow surveillance technology that can exploit the manner in which a cell phone transmits data to convert it into a mobile tracking device. Accordingly, an order issued pursuant to CJP § 10-4B-04 cannot authorize the use of a cell site simulator, such as Hailstorm. Because there was no statutory authorization for the BPD's use of the Hailstorm cell site simulator, we hold that the BPD should have sought a warrant or a specialized order upon a particularized showing of probable cause, and based on sufficient information about the technology involved to permit the court to contour reasonable limitations on the scope and manner of the BPD's use of the device.<sup>21</sup> *See, e.g., In re Application of the United States for an Order Authorizing Installation & Use of a Pen Register*, 415 F. Supp. 2d at 219.

**b. The Order Obtained by the State Was Not Equivalent to a Warrant**

The State insists that its use of the Hailstorm device to track Andrews's cell phone was authorized by the court order. In the absence of a specific statute that would have

---

<sup>21</sup> To the extent that the State makes a limited argument that there is no suppression remedy available for violation of the sections 10-4B-01 *et seq.*, we respond simply that the circuit court found, and we agree, that the use of the cell site simulator was a Fourth Amendment violation and, thereby, the exclusionary rule applies. The fact that there may have been a contemporaneous violation of sections 10-4B-01 *et seq.* does not limit the available remedy.

authorized the use of a cell site simulator at the time Andrews was arrested, the State presses that “the police erred on the side of caution and obtained a court order specifically authorizing the use of a cellular tracking device to find Andrews’s phone[,]” pursuant to the “nearest analog”—the Maryland pen register statute. The State acknowledges that the court order described in the Maryland pen register statute does not use the words “warrant” or “probable cause.” Nevertheless, the State argues that, in this case, the BPD’s application and the resulting order “went far beyond the requirements of the statute.”

The State points out that the BPD application was for an order allowing the police to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register\Trap & Trace and Cellular Tracking Device [. . .] and shall initiate a signal to determine the location of the subject’s mobile device on the service provider’s network or with such other reference points as may be reasonabl[y] available . . .

The State also notes that the resultant order states that probable cause exists to authorize the use of a “Cellular Tracking Device.” Thus, the State contends that because the pen register\trap & trace order stated that it was based upon a finding of probable cause, it was, therefore, “the functional equivalent of a warrant.”

Andrews emphasizes that the order may issue on just a showing “that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.” CJP § 10-4B-04(a)(1). In addition to the fact that a pen register\trap & trace order does not contemplate the use of a cell site simulator, Andrews points out that it also does not satisfy the requirements that a warrant based on probable cause be attached to a specific suspected crime, be confined in scope, or describe with

particularity the place to be searched or the person to be seized. Andrews contends that “[t]he moment BPD conducted surveillance with something other than a pen register, it exceeded the purview of the pen register order.” Further, Andrews contends that BPD’s application “For an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace,” was intentionally captioned to ensure that the circuit court scrutinized it according to the statutory pen register factors. Andrews argues that BPD’s “disingenuous efforts” hid from the circuit court “the scope, intensity, [and] nature of the search,” and prevented the court from conducting a proper probable cause analysis.

We begin with our appraisal that an order issued under the pen register statute is not the equivalent of a warrant based on probable cause—a fact the State implicitly concedes in its argument that it “went beyond the requirement of the statute.” The applicable requirements of the statute are contained first in § 10-4B-03:

(b) *Contents.* — An application under subsection (a) of this section shall include:

- (1) The identity of the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
- (2) A statement under oath by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Additionally, 10-4B-04(a) states that an order may issue if the court finds the information likely to be obtained by the device is relevant to an ongoing criminal investigation, and the order must:

- (3) Specify the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace

device is to be attached or applied, and, in the case of a trap and trace device, the geographic limits of the trap and trace order;  
(4) Contain a description of the offense to which the information likely to be obtained by the pen register or trap and trace device relates[.]

CJP § 10-4B-04(b)(3) & (4). Plainly, this limited showing falls short of the particularity required for the issuance of a search warrant. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983) (“The task of the issuing magistrate is simply to make a practical, common-sense decision whether . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.”); *Nero v. State*, 144 Md. App. 333, 345-46 (2002) (“General warrants, of course, are prohibited by the Fourth Amendment. . . . [T]he problem [posed by the general warrant] is not that of intrusion per se, but of a general, exploratory rummaging in a person’s belongings. . . . [The Fourth Amendment addresses the problem] by requiring a ‘particular description’ of the things to be seized.” (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976))).

Moving to the State’s argument that the order was sufficient because it went beyond the requirements of the statute, we start by rejecting the State’s contention that the words “probable cause” contained in the pen register application and order converted the overreaching order into a warrant. The “probable cause” articulated in the resulting order is merely that “**information likely to be obtained . . . is relevant to an ongoing criminal investigation.**” (Emphasis in original). Certainly, while this reflects the standard required for issuance of an order under CJP § 10-4B-04, it falls far short of the particularity required to support a search warrant. *See Gates*, 462 U.S. at 238; *Nero*, 144 Md. App. at 345-46.

In the information “offered in support of probable cause” the application states:

Your Applicant hereby certifies that the information likely to be obtained concerning [Andrews's] location will be obtained by learning the numbers, locations and subscribers of the telephone number(s) being dialed or pulsed from or to the aforesaid telephone and that such information is relevant to the ongoing criminal investigation.

Plainly, the State's use of the Hailstorm device extended far beyond this certification as to how information concerning Andrews's location would be obtained.

Here, the State inserted language into its application and proposed order attempting to, without being specific, obtain court authorization for more than a pen register\trap & trace order. Although the application does request authorization to use a "Cellular Tracking Device," it fails to name or describe any cell site simulator. In fact, there is absolutely nothing in the application or order that identifies the Hailstorm device, or provides even a rudimentary description of cell site simulator technology. The application also failed to identify any geographical limitation to the BPD's use of the undisclosed surveillance technology, and did not explain what was to be done with the information collected. Nor did the application disclose the possibility that the technology employed may capture the cell phone information (unique serial numbers) of innocent third parties in range of the target area. Finally, we are troubled that the application for a pen register\trap & trace order did not fully apprise the circuit court judge from whom it was sought of the information that it would yield. Based on the application that he received, the circuit judge was entitled to expect that the results would be a list of telephone numbers that Andrews called and that called Andrews—not a real-time fix on his location.

We determine that the pen register\trap & trace order in this case failed to meet the requirements of a warrant. To allow the government to collect real-time location



information on an unknown number of private cell phones, without any geographic boundaries, without any reporting requirements or requirements that any unrelated data be deleted, and without a showing of probable cause that contraband or evidence of a particular crime will be found through the particular manner in which the search is conducted would certainly run afoul of the Fourth Amendment. As stated in our holding above, unless a valid exception to the warrant requirement applies,<sup>22</sup> the government may not use a cell phone simulator without a warrant or, alternatively, a specialized order that requires a particularized showing of probable cause, based on sufficient information about the technology involved to allow a court to contour reasonable limitations on the scope and manner of the search, and that provides adequate protections in case any third-party cell phone information might be unintentionally intercepted. To hold otherwise would be to

---

<sup>22</sup> One of the exceptions more commonly relied upon applies when ‘the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.’” *Kentucky v. King*, 563 U.S. 452, 460 (2011) (some internal quotation marks omitted) (quoting *Mincey v. Arizona*, 437 U.S. 385, 394 (1978)). Maryland has recognized that “[e]xigent circumstances exist when a substantial risk of harm to the law enforcement officials involved, to the law enforcement process itself, or to others would arise if the police were to delay until a warrant could be issued.” *Williams v. State*, 372 Md. 386, 402 (2002) (citations omitted). It remains the State’s burden to establish exigent circumstances sufficient to justify a warrantless search. *Wengert v. State*, 364 Md. 76, 85 (2001) (citations omitted). We note that the Supreme Court in *Riley, supra*, rejected the argument that officer safety, in that case, presented an exigent circumstance that justified officer’s accessing content on a cell phone seized in a search incident to arrest. The Court observed that “[t]o the extent dangers to arresting officers may be implicated in a particular way in a particular case, they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances.” 134 S. Ct. at 2486.

abandon the Fourth Amendment by assuming, without any foundation, that the citizens of Maryland have forfeited their reasonable expectation of privacy in their personal location.

#### IV.

##### **The Exclusionary Rule**

###### **a. The Search Warrant Does Not Survive Removal of the Constitutionally Tainted Information.**

The State contends that the search warrant that was obtained for 5032 Clifton Avenue was valid because probable cause existed once “Andrews was found in the home.” According to the State, Andrews was arrested pursuant to a valid arrest warrant and the police had “the consent of the apparent owner of the home to enter the home to take Andrews into custody.” Thus, the State argues, “[n]othing about the way in which Andrews was located negated the probable cause to believe that there could be evidence of the crimes at that address.”

In riposte, Andrews avers that without the location data provided by the cell site simulator, “the BPD possessed no nexus between the criminal activity at hand and 5032 Clifton Avenue.” Andrews asserts that, “[b]ecause the search warrant relied entirely on that nexus, it withers as fruit of the poisonous tree.”

First, we note that where entry into a protected space “was demanded under color of office” and “granted in submission to authority,” that submission does not equate to a waiver of a constitutional right. *Johnson, supra*, 333 U.S. at 13 (citing *Amos v. United States*, 255 U.S. 313 (1921)). Thus, the existence of an arrest warrant and the consent of

the owner of the residence do not, in themselves, diminish Andrews's protection under the Fourth Amendment. Nor do they render the later-acquired search warrant unassailable.

Second, the courts of Maryland have recognized that where a search warrant relies on information obtained in violation of the constitution, the question is "whether 'after the constitutionally tainted information is excised from the warrant, the remaining information is sufficient to support a finding of probable cause.'" *Redmond v. State*, 213 Md. App. 163, 191-92 (2013) (quoting *Williams v. State*, 372 Md. 386, 419 (2002)). See also *Karo*, 468 U.S. at 720-21 (stating that in determining whether evidence seized pursuant to a contested warrant remains admissible, one of the pertinent questions is whether "the warrant affidavit, after striking the [constitutionally tainted] facts . . . contained sufficient untainted information to furnish probable cause for the issuance of the search warrant.") Here, there can be no doubt that the only information linking Andrews and 5023 Clifton Avenue was the fruit of the Fourth Amendment violation. The State presents no credible argument that evidence of Andrew's presence in the home was obtained by independent lawful means.

In *Redmond v. State*, the BPD were investigating an armed robbery in which a cell phone was stolen. 213 Md. App. at 169. During their investigation, detectives contacted the victim's mobile service provider and, "by triangulating the signal from cell phone towers in the area, determined that the stolen cell phone was in the proximity of 3303 Round Road." *Id.* at 169. Thereafter, detectives began moving from house to house in the area, speaking to residents using a ruse that they were "looking for a pedophile named 'Leroy Smalls.'" *Id.* at 170. After obtaining consent to enter the appellant's residence

under those false pretenses, one of the detectives surreptitiously dialed the number of the stolen cell phone, heard it ringing upstairs, and then walked through the entire house conducting a “protective sweep” including opening closet doors and checking under beds. *Id.* at 171. Officers then sought a search warrant for the home on the basis of what they had discovered in the home. *Id.* at 171-72.

After a careful analysis, we determined that “[b]y dialing the number of the stolen cell phone and walking upstairs to locate it, the police exceeded the scope of any consent that was given to their presence inside 3303 Round Road.” *Id.* at 189-90. Applying the exclusionary rule, we noted that “all the information . . . attested to in applying for the search warrant (and on which the search warrant was granted) . . . was discovered during the initial illegal entry.” *Id.* at 192. We determined that the search warrant was not issued based on an independent lawful source and the unlawfully obtained evidence should be suppressed.<sup>23</sup> *Id.* And, we soundly rejected the argument that evidence in a warrant

---

<sup>23</sup> Although the warrant application in *Redmond* mentioned reliance on “sophisticated mobile and/or portable surveillance equipment” to locate the stolen cell phone, in that case we observed that:

Detective Jendrek did not testify that the ATT used *any* “sophisticated mobile and/or portable surveillance equipment” while in the 3300 block of Round Road. Rather, his testimony was that the ATT detectives confirmed the precise location of the cell phone by use of ordinary police investigatory tactics: speaking to the occupants of two houses, dialing the number of the stolen cell phone, listening for it to ring, and, ultimately, physically observing the stolen cell phone lying on a dresser.

Thus, to the extent that the averments in the search warrant application represent that the ATT detectives used “sophisticated” means to locate the

application was obtained by independent lawful means “(1) where the officer’s decision to seek the warrant was prompted by what they had seen during the initial entry; and (2) where information obtained during that entry was presented to the [judge] and affected his [or her] decision to issue the warrant.” *Id.* at 191 (internal quotation marks omitted) (alterations in *Redmond*) (quoting *Kamara v. State*, 205 Md. App. 607, 627-28 (2012)). *See also Murray v. United States*, 487 U.S. 533, 534 (1988) (“The ultimate question is whether the search pursuant to warrant was in fact a genuinely independent source of the information and tangible evidence at issue. This would not have been the case if the agents’ decision to seek the warrant was prompted by what they had seen during the initial entry or if information obtained during that entry was presented to the Magistrate and affected his decision to issue the warrant.”).

As in *Redmond*, here, the evidence that forms the only basis for probable cause in the State’s search warrant application—that Andrews was at 5032 Clifton Avenue—was that obtained through an unlawful search—in this case, the BPD’s use of the Hailstorm device. We agree with the circuit court’s determination that there was no independent lawful source to establish a nexus between Andrews and the residence. *Cf. Agurs v. State*, 415 Md. 62, 84 (2010) (stating that “police should have been aware that there must be a

---

stolen cell phone while at the scene on the afternoon of March 2, 2010, they are simply inaccurate.

213 Md. App. at 193. The defendant in *Redmond* did not challenge the use of any such device or the use of cell tower information. Accordingly, in *Redmond* we did not address the use of sophisticated mobile surveillance systems, as we must in the matter *sub judice*.

nexus between criminal activity and the place to be searched.”). Accordingly, once the constitutional taint is removed from the search warrant in this case, what remains is insufficient to establish probable cause for a search of 5032 Clifton Avenue and, as discussed further *infra*, the evidence seized in that search withers as the fruit of the poisoned tree. *Franks v. Delaware*, 438 U.S. 154, 156 (1978) (stating that if “the affidavit’s remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.”). Therefore, we affirm the suppression court’s exclusion of all evidence found at 5032 Clifton Avenue.

**b. The State Cannot Rely on the Good Faith Exception**

Finally, the State argues that BPD’s relied in good faith on the search warrant issued for 5032 Clifton Avenue after locating Andrews inside that address. The State asserts that police officers relied on, first, the pen register\trap & trace order, and, second, on the later issued search warrant for the premises. The State maintains that “[t]his is good faith squared[,]” and there is “simply no officer misconduct to deter in this case.” Thus, the State contends that the exclusionary rule should not apply in this case.

Andrews contends that without the location information provided by the cell site simulator the BPD possessed no nexus between him and 5032 Clifton Avenue, and, “[b]ecause the search warrant relied entirely on that nexus, it withers as the fruit of the poisonous tree.” Andrews asserts that where the information relied on to obtain a warrant is the product of a Fourth amendment violation, the fruit of the poisonous tree doctrine

trumps the good faith exception. Moreover, Andrews argues that good faith cannot apply where “law enforcement officers, from the outset, dealt dishonestly with the judiciary.”

In *United States v. Leon*, the Supreme Court held that, where officers have acted in good faith pursuant to a warrant that was later discovered to be invalid, exclusion is not warranted to deter police over-reach or misconduct. 468 U.S. 897, 924 (1984). The Supreme Court cautioned, however, that

[t]he good-faith exception for searches conducted pursuant to warrants is not intended to signal our unwillingness strictly to enforce the requirements of the Fourth Amendment, and we do not believe that it will have this effect. As we have already suggested, the good-faith exception, turning as it does on objective reasonableness, should not be difficult to apply in practice. When officers have acted pursuant to a warrant, the prosecution should ordinarily be able to establish objective good faith without a substantial expenditure of judicial time.

In *Fitzgerald v. State*, this Court aptly summarized the “good faith” exception:

Because the only purpose of the Exclusionary Rule of *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961), is to deter unreasonable police behavior, *Leon* and [*Massachusetts v. Sheppard*, 468 U.S. 981 (1984)] held that a mistake made by a judge in issuing a warrant should not be attributed to the police officer who executes it. Because the officer has been reasonable in relying on the judge’s legal expertise, it would serve no deterrent purpose to exclude otherwise competent, material, and trustworthy evidence. See *Connelly v. State*, 322 Md. 719, 720–21, 589 A.2d 958 (1991).

153 Md. App. 601, 655-56 (2003) *aff’d*, 384 Md. 484 (2004). However, this Court observed that in *Karo, supra*, the Supreme Court instructed that, if the information obtained through a Fourth Amendment violation “proved critical to establishing probable cause for the issuance of the warrant,” it would invalidate the subsequent search warrant for the house. *Id.* at 656 (citing *Karo, supra*, 468 U.S. at 719). Accordingly, “the conclusion may readily be drawn that in the case of an antecedent Fourth Amendment violation which

contributes to a warrant application, the ‘fruit of the poisoned tree’ doctrine ‘trumps’ the officer’s ‘good faith’ reliance under *Leon* and *Sheppard*.” *Id.*

Here, as we noted above, the BPD submitted an overreaching pen register\trap & trace application that failed to clearly articulate the intended use, i.e., to track Andrews’s cell phone using an active cell site simulator. The ensuing order did not support the use of the Hailstorm device, nor did it, in any way, serve as a de facto warrant for the use of the Hailstorm device. As the State’s May 15, 2015 supplemental disclosure made clear, “WATF did not have the Clifton Ave address as a possible location until ATT provided that information.” Only after receiving that information through the use of the Hailstorm device and arresting Andrews at the premises did the same BPD officers who submitted the pen register\trap & trace application then apply for a search warrant.

As Andrews points out, without the antecedent Fourth Amendment violation the nexus between the residence to be searched and the alleged criminal activity could not have been established. *Cf. Agurs*, 415 Md. at 84 (stating that “police should have been aware that there must be a nexus between criminal activity and the place to be searched.”). In the present case, the antecedent Fourth Amendment violation was the only basis upon which the search warrant application stood, and the fruit of the poisoned tree doctrine does, indeed, trump alleged good faith reliance on the part of BPD. *See Fitzgerald*, 153 Md. App. at 656.

The Supreme Court in *Leon*, was clear that “the officer’s reliance on the magistrate’s probable-cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable.” 468 U.S. at 922. *See, e.g., Spence v. State*, 444 Md. 1, 12-13



(2015) (wherein the police officer, in searching a cell phone and reading text messages during a search incident to arrest, was acting in good faith reliance on then-controlling authority in Maryland); *Agurs*, 415 Md. at 83 (concluding that the good faith exception did not apply where “no reasonably well-trained police officer could have relied on the warrant that authorized the search of Agurs’ home.”). We cannot say the BPD officers in this case reasonably relied on the warrant obtained through their own misleading order application and unconstitutionally intrusive conduct. To do so would allow law enforcement to insulate its own errors merely by presenting limited information to a magistrate, obtaining a warrant post-intrusion, and then re-entering the place to be searched. The good faith exception to the exclusionary rule seeks to avoid “[p]enalizing the officer for the magistrate’s error, rather than his own.” *Leon*, 468 U.S at 921. That is, however, not that case here. *See id.* at 919 (“The deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right. By refusing to admit evidence gained as a result of such conduct, the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of an accused.” (quoting *United States v. Peltier*, 442 U.S. 531, 539 (1975))).

It is for all of these reasons that we hold that the evidence obtained in the search of 5032 Clifton Avenue is inadmissible as fruit of the poisoned tree and was properly excluded by the suppression court.

**JUDGMENTS OF THE CIRCUIT  
COURT FOR BALTIMORE CITY  
AFFIRMED.**

**COSTS TO BE PAID BY MAYOR AND  
CITY COUNCIL OF BALTIMORE.**

**From:** (b)(6); (b)(7)(C)  
**Sent:** 28 Aug 2018 20:51:00 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** (b) (7)(E) PPT  
**Attachments:** Cell-site Simulator PP (2nd).ppt, GPS Maritime - Final to (b)(6); (b)(7)(C) docx, GPS Hypotheticals.docx

(b)(7)(E)

Start at slide 137.

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

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (office)  
202-500-(b)(6) (mobile)

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

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~



# U.S. Immigration and Customs Enforcement

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

Associate Legal Advisor

Homeland Security Investigations Law Division

Criminal Law Section

Office of the Principal Legal Advisor

August 2016

- OPLA
  - CLS
  - HSI Embed Program
- Introduction to Cell-Site Simulators
- Reintroduction to Fourth Amendment Search and Seizure
  - The Pen Register Statute and the Electronic Communications Privacy Act of 1986
- Cell-Site Simulator Policy



## Overview: OPLA

- ICE Office of the Principal Legal Advisor
  - Headquarters
    - Overview of Divisions
      - Homeland Security Investigations Law Division
        - Criminal Law Section
- Offices of the Chief Counsel
  - HSI Embedded Attorney



## What are Cell-Site Simulators?

- Purpose?

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

- [Redacted]

- How do they work?

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

- [Redacted]



# ICE

## Use of Cell-Site Simulators

ICE must use cell-site simulators in a manner consistent with the protections of the U.S. Constitution, specifically the Fourth Amendment, and applicable statutory authorities, notably the Pen Register Statute.



U.S. Immigration  
and Customs  
Enforcement



# ICE

## Fourth Amendment and How it Protects

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.

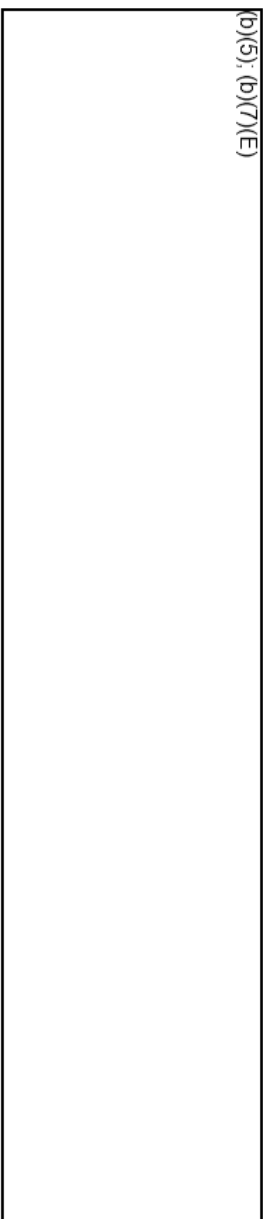


U.S. Immigration  
and Customs  
Enforcement

# ICE

## Fourth Amendment: Exclusionary Rule

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

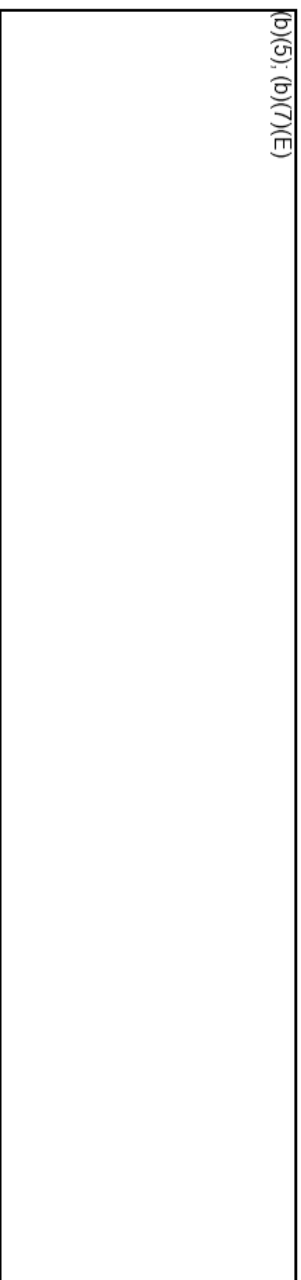


U.S. Immigration  
and Customs  
Enforcement

# ICE

## Fourth Amendment Exclusionary Rule: Exception

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



U.S. Immigration  
and Customs  
Enforcement

## Searches

- Government participation
- Intrusion (physical, visual, auditory)
- Reasonable Expectation of Privacy (“REP”)
  - Subjective expectation of privacy
  - Objectively reasonable



# ICE

# No REFP

- Open fields
- Open view
- Overheard conversations
- Abandoned Property
- Trash
- Odors
- Items previously and lawfully searched
- Movement of vehicles and containers in public



U.S. Immigration  
and Customs  
Enforcement

## *U.S. v. Jones*

- Warrantless Installation of GPS Tracker
  - Intent to obtain information + Trespass
  - Short duration monitoring permissible
- 48-hour rule (DOJ policy)
- Inapplicable situations
  - Exceptions to warrant requirement
  - Commercial vehicles, aircraft, vessels
  - Border searches
    - Per se reasonable
    - Extended border search
- Extraterritorial application



## General Rule - Warrants

- Warrantless searches & seizures generally are presumed to be unreasonable unless a reasonable exception applies
- Requirements:
  - Probable Cause
  - Particularity



# ICE

## Warrants & Electronic Devices

- Scope
- Particularity
- Retention
- Time limits



U.S. Immigration  
and Customs  
Enforcement



# IOIE

## Exceptions to Warrants But PC Still Needed

- Arrest in a Public Place
- Plain View
  - Lawful presence/access
  - Probable cause to seize is immediately apparent
- Mobile Conveyances
- **Exigent Circumstances**



U.S. Immigration  
and Customs  
Enforcement

# ICE

## Exceptions – Warrant & PC

- Protective Sweep
- Stop/Frisk
- Inventory
- Regulatory
- Administrative
- Search Incident to Arrest
- Consent
- Border Search



U.S. Immigration  
and Customs  
Enforcement

## The Pen Register Statute and ECPA

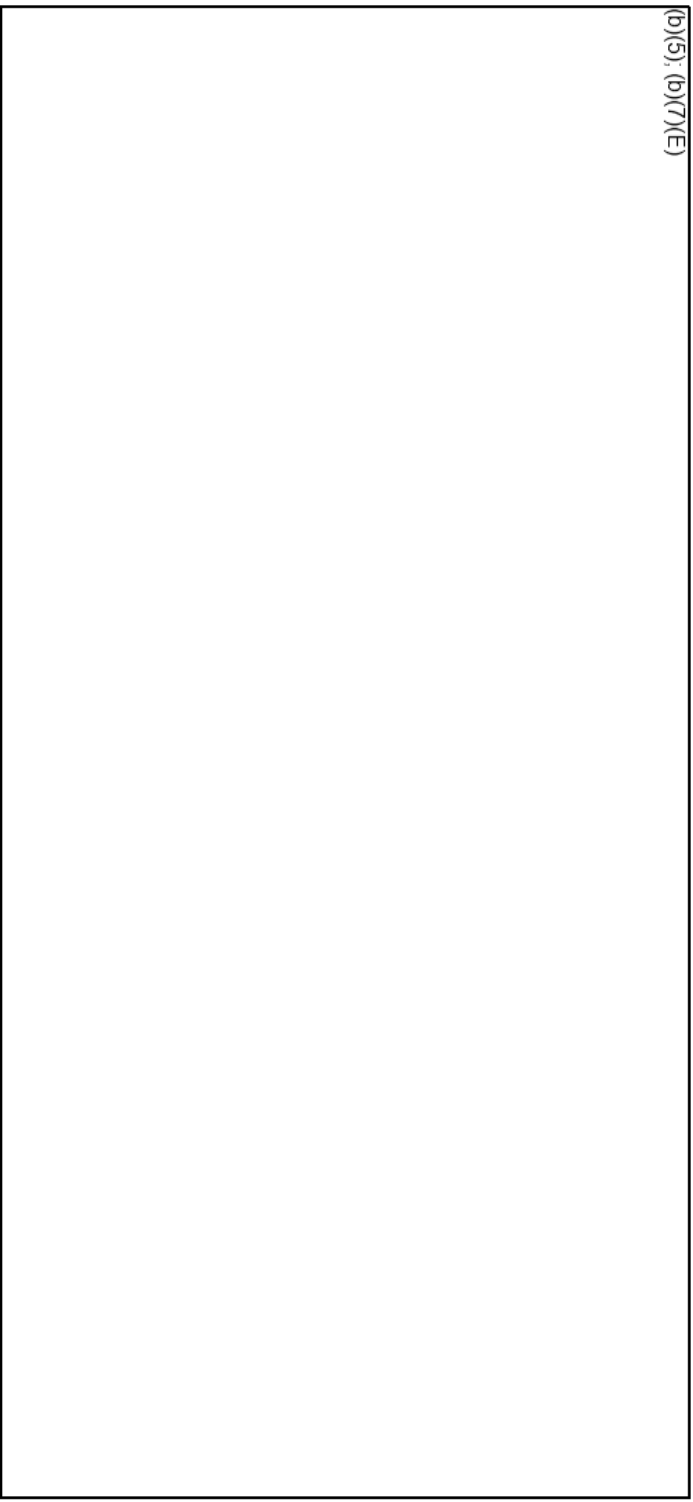
- The Pen Register Statute is a component of the Electronic Communications Privacy Act of 1986 (“ECPA”), which is also comprised of the Stored Communications Act and amendments to the Wiretap Act.
  - § ECPA Controls the collection and disclosure of content and non-content information related to electronic communications, as well as content that has been stored remotely.
    - w Title I of ECPA – Wiretap Act
    - w Title II of ECPA – Stored Communications Act
    - w **Title III of ECPA – Pen register and trap and trace devices**
- As noted above, a cell-site simulator must be configured as a pen register.



# ICE

## Pen Register and Trap and Trace Devices

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



U.S. Immigration  
and Customs  
Enforcement

# ICE

## Cell-Site Simulator Policy

Must obtain a search warrant supported by **probable cause** and issued pursuant to rule 41 of the Federal Rules of Criminal Procedure, **unless** there is an exigent circumstance under the Fourth Amendment or an exceptional circumstance.



U.S. Immigration  
and Customs  
Enforcement

# ICE

## 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.



U.S. Immigration  
and Customs  
Enforcement

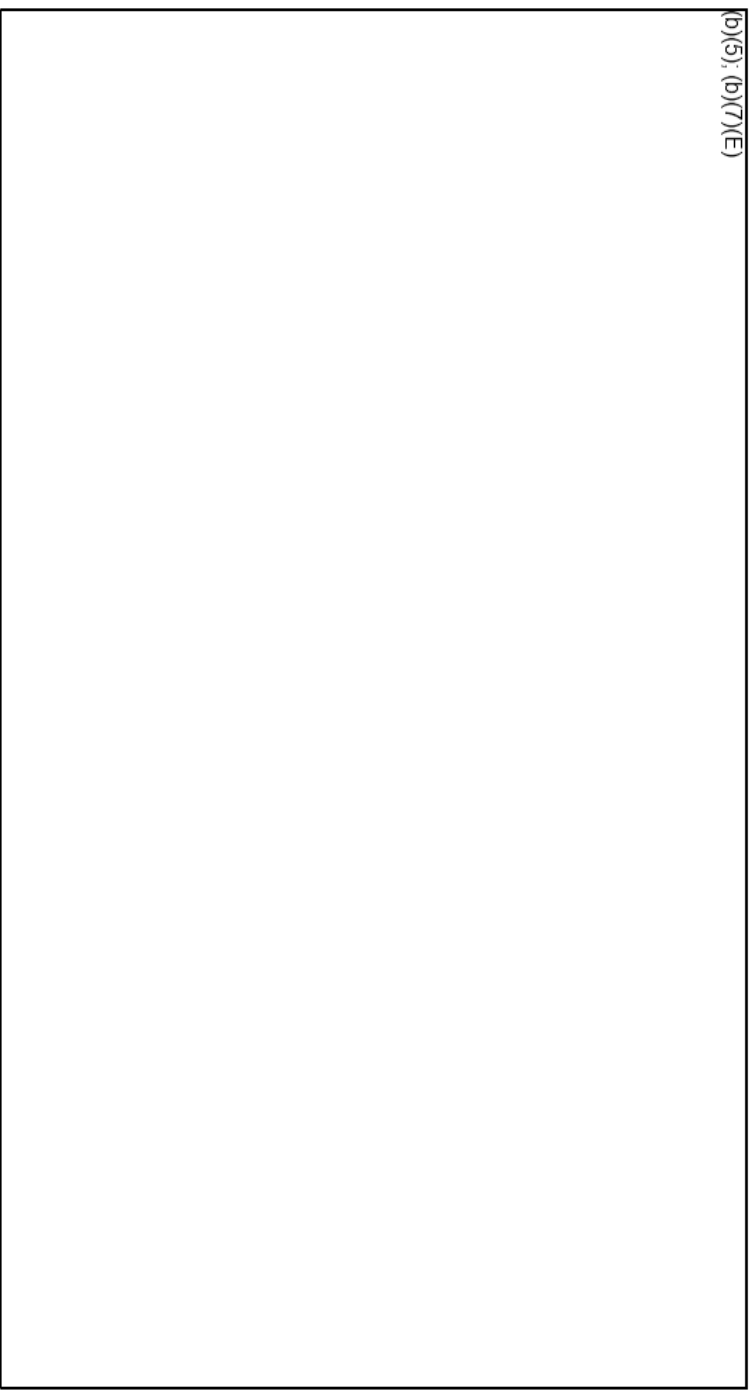
2020-ICLI-00013 802

# ICE

## Cell-Site Simulator Policy

**Exigent Circumstances (cont.)**

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



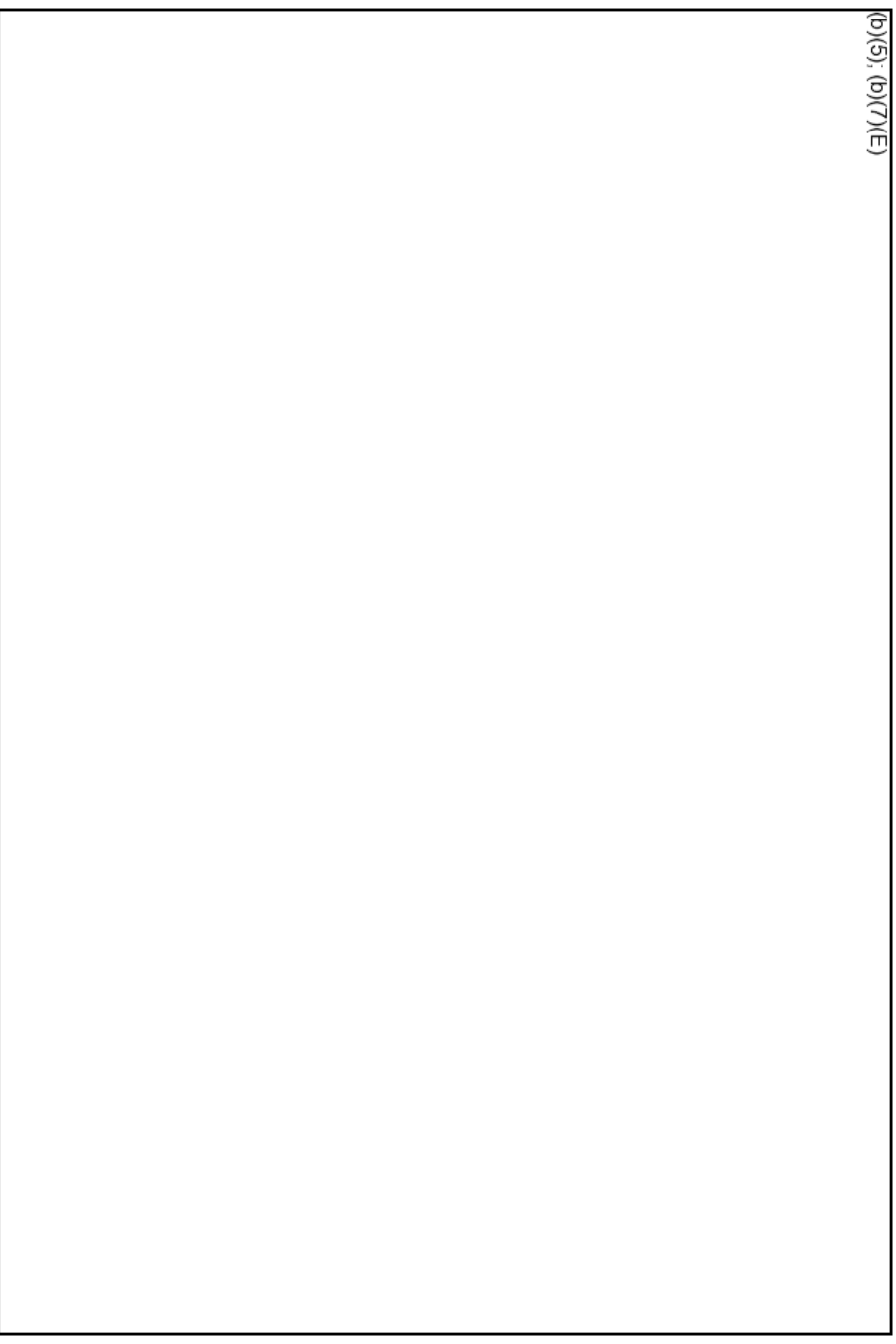
U.S. Immigration  
and Customs  
Enforcement

# ICE

## Cell-Site Simulator Policy

**Exigent Circumstances (cont.)**

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



U.S. Immigration  
and Customs  
Enforcement

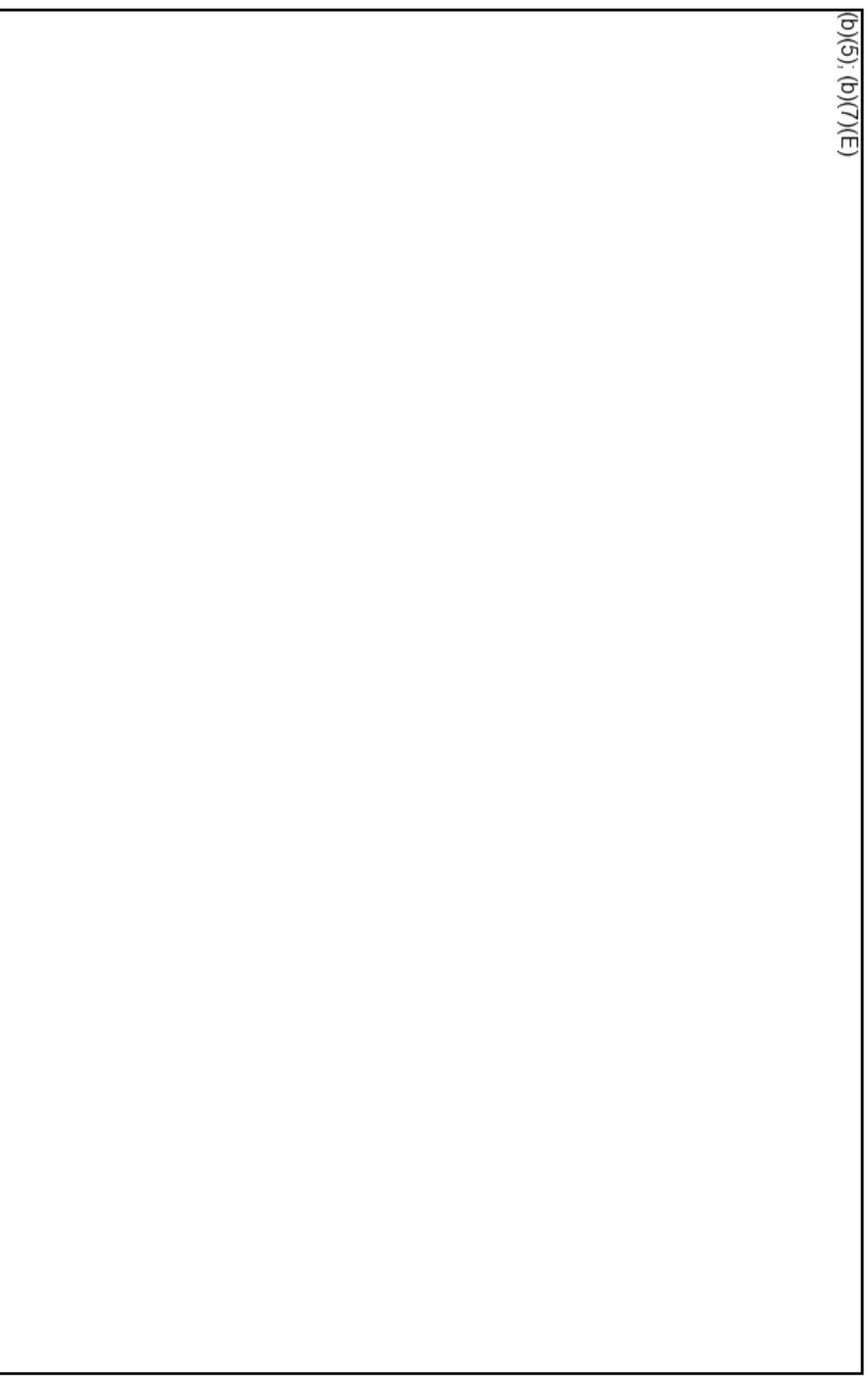


# ICE

## Cell-Site Simulator Policy

### Exceptional Circumstances

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



U.S. Immigration  
and Customs  
Enforcement

# ICE

## Cell-Site Simulator Review

**Always need a warrant with requisite probable cause!**

- § Unless an **exigent** circumstance exists; or
- § Unless an **exceptional** circumstance exists.



U.S. Immigration  
and Customs  
Enforcement

# ICE

## Applications for Use of Cell-Site Simulators

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

[Redacted content]



U.S. Immigration  
and Customs  
Enforcement

# ICE

## Information to be included in Application

- Application or supporting affidavit for use of cell-site simulator should:

§ (b)(5); (b)(7)(E)

§

§

§



U.S. Immigration  
and Customs  
Enforcement

# ICIE

## Data Collection and Disposal

- Data collected through the use of a cell cite simulator must be handled in the same manner, consistent with applicable existing laws and requirements, including duty to preserve exculpatory evidence.

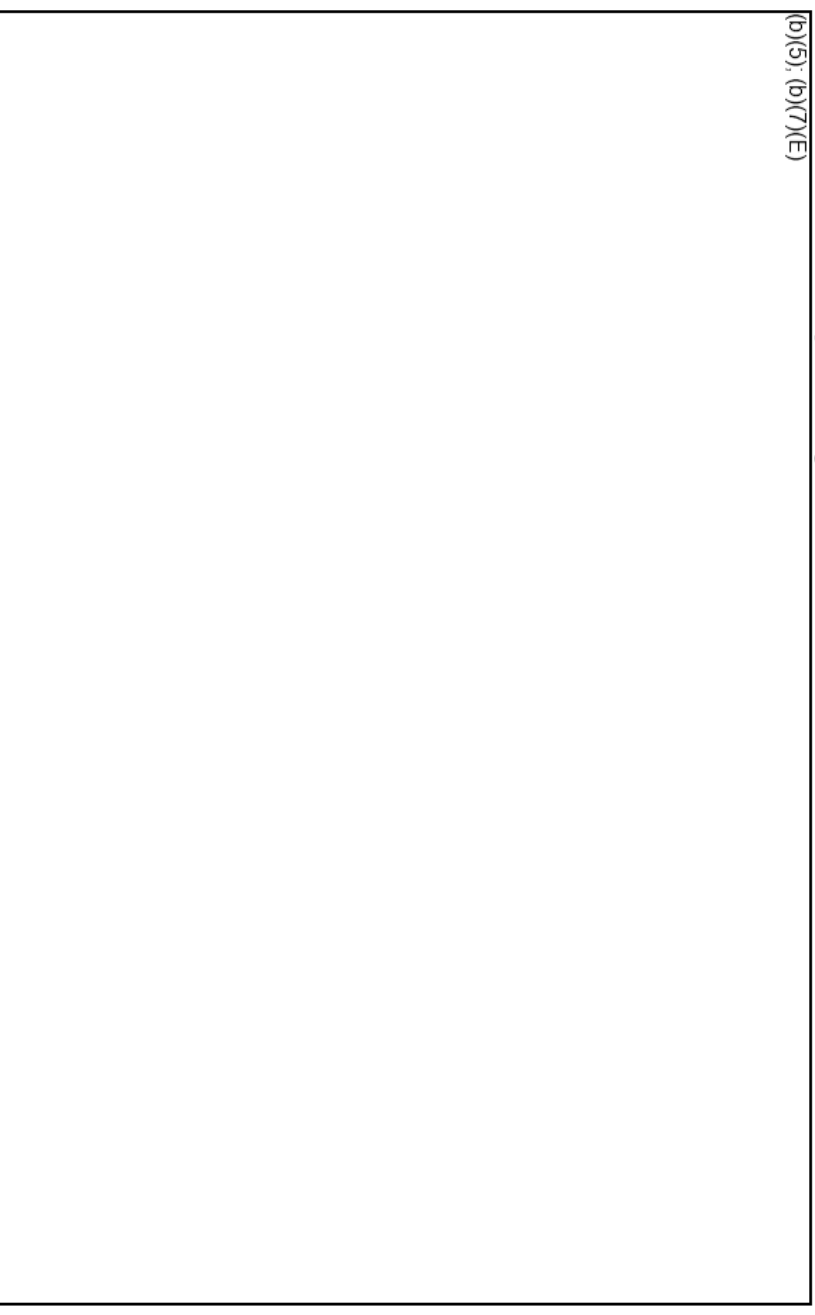
§ (b)(5); (b)(7)(E)

§

§

§

§



U.S. Immigration  
and Customs  
Enforcement

## Additional Notes

- State and Local Partners  

(b)(5); (b)(7)(E)
- Improper Use of Cell-Site Simulators
- This policy is guidance and 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.



# ICE

## Quiz

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

[Redacted content]



U.S. Immigration  
and Customs  
Enforcement

# Questions?

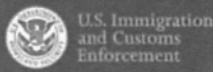
**[OPLA-CLS@ice.dhs.gov](mailto:OPLA-CLS@ice.dhs.gov)**



# ICE

## Electronic Communications Privacy Act

- **Title I of ECPA** – Wiretap Act
- **Title II of ECPA** – Stored Communications Act
- **Title III of ECPA** – Pen register and trap and trace devices



ECPA is made up of three titles. We will discuss these in more detail in the next. CALIFORNIA RECENTLY PASSED ITS OWN VERSION THAT HAS SOME UNIQUE DIFFERENCES. WE'VE ASKED (b)(6); (b)(7)(C) TO DISCUSS THESE AFTER WE FINISH ADDRESSING CURRENT FEDERAL LAW.

Title I - prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence. 18 U.S.C. § 2515.

Title II – Stored Communications Act protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses. 18 U.S.C. §§ 2701-12.

Title III - Addresses pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap

and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated). No actual communications are intercepted by a pen register or trap and trace. The authorization order can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applicant's agency.

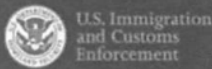
The Communications Assistance to Law Enforcement Act (CALEA) amended ECPA in 2004. CALEA sets out obligations of telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. The FBI is responsible for implementing CALEA.

- Note – there is some discussion of amending CALEA to address recent cell phone encryption concerns.

# ICE

## Title III – Pen Register and Trap and Trace Devices

- Obtain the pen register records from the appropriate phone company to identify which numbers are being called by the target telephone, how often they are called, and for what duration.
- Under the USA Patriot Act, the legal threshold for obtaining these records was lowered to a demonstration that the records are relevant to an ongoing criminal investigation.



This is found in USA Patriot Act sections 214-216.

Pen register = device or process that records or decodes dialing, routing, addressing or signaling information transmitted by a communication instrument or facility; does not include content, which is governed by Title III. 18 USC 3127(3)

Trap and trace device = device or process that captures the incoming electronic impulses, which identify the source of the communication (originating number or other dialing, routing, addressing or signaling information); does not include content, which is governed by Title III. 18 USC 3127(4).

ICE requests installation or use of pen registers or trap and trace devices through a court order; the standard for obtaining the order is that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency. 18 USC 3122.

# ICE

## Cell Phone Location Data

- Historical Cell-Site Information
- Prospective Cell Phone Location Information
  - Cell-Site
  - E911
- Stingray/Trigger Fish Devices/  
International Mobile Subscriber Identity  
(IMSI) Catchers



U.S. Immigration  
and Customs  
Enforcement

- Historical Cell-Site Location Information
  - 18 USC 1703(d) orders generally can be used to obtain cell-site records, however there is much litigation surrounding this (especially bulk historical data collection in light of *Jones*).
  - The Fourth Circuit now joins the Fifth, Sixth, and Eleventh Circuits in holding that no Fourth Amendment protection exists for cell site records under the third party doctrine.

### ***U.S. v. Graham*, No. 12-4659 (4th Cir. May 31, 2016) (en banc)**

The Fourth Circuit issued an en banc decision on the U.S. government's petition, finding that no warrant is required for law enforcement to obtain historical cell-site location information (CSLI) from carriers. This decision eliminates the circuit split created in the initial Fourth Circuit panel decision. *U.S. v. Graham*, 796 F.3d 332 (4th Cir. 2015). In the panel decision, the Fourth Circuit held that the government had violated defendants' rights when it obtained historical CSLI for an extended period of time without a warrant. The panel cited to the Justice Sotomayor concurrence in *U.S. v. Jones* for the conclusion that long-term location information disclosed in cell phone records can reveal a significant

comprehensive view of an individual's daily life. 132 S.Ct. 945, 955 (2012). Although the court refused to declare a bright line rule for what is too long a time period, it determined that the 14 days of CSLI in this case was too long. The court nevertheless determined that the government acted in good faith in obtaining the historical CSLI without a warrant and affirmed the convictions of Defendants Aaron Graham and Eric Jordan arising from their participation in a series of armed robberies.

The en banc opinion disagreed with the 2015 panel decision, concluding that the government's acquisition of historical CSLI from defendants' cell phone provider did not violate the Fourth Amendment.

Supreme Court precedent mandates this conclusion. For the Court has long held that an individual enjoys no Fourth Amendment protection "in information he voluntarily turns over to [a] third part[y]." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). This rule -- the third-party doctrine -- applies even when "the information is revealed" to a third party, as it assertedly was here, "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976). All of our sister circuits to have considered the question have held, as we do today, that the government does not violate the Fourth Amendment when it obtains historical CSLI from a service provider without a warrant. In addition to disregarding precedent, Defendants' contrary arguments misunderstand the nature of CSLI, improperly attempt to redefine the third-party doctrine, and blur the critical distinction between content and non-content information.

The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case.

Although the en banc opinion acknowledges the defendants' analogy to government location tracking, it determines that "it is premature to equate CSLI with the surveillance information obtained in...*Jones*" because CSLI can only determine a four-square-mile area within which a person used his or her cell phone, and CSLI does not allow the government to "place an individual" at home or other private locations. (n. 3)

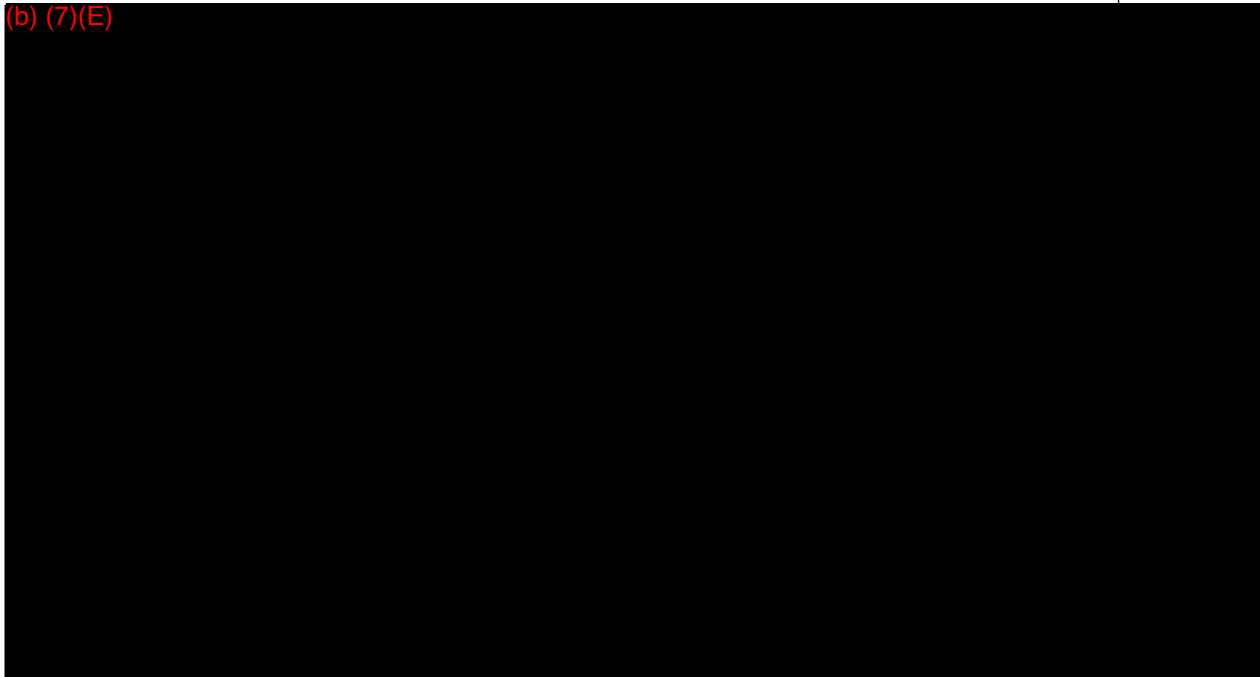
- Prospective Cell Phone Location Information
  - Prospective cell-site information identifies the tower (and in most cases the sector of the cell tower) used to route communications to or from the target phone. Taken together with the location of the relevant cell towers, these

records permit investigators to determine the general area in which the target phone is located at the time that a communication occurs.

- DOJ believes that prospective cell-site information can be properly obtained with a hybrid order, which is based on the combined authority of Section 2703(d) of the Stored Communications Act and the Pen/Trap Statute. Some judges, however, have refused to sign hybrid orders for prospective cell-site information and have required the use of a search warrant.
- E911 data provides more precise information, in the form of geographic coordinates, about the location of a target phone. Significantly, while all providers can supply prospective cell-phone location information, some providers (e.g. Verizon) lack the ability to produce prospective E911 location information to law enforcement even when served with a search warrant.
- DOJ recommends that law enforcement always utilize a search warrant when seeking to compel a provider to produce E911 location information.

•Stingray/Trigger Fish/IMSI Catchers

(b) (7)(E)



# 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)

# 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)

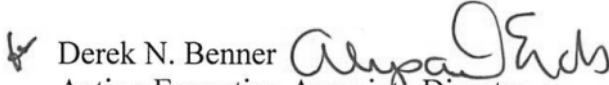




U.S. Immigration  
and Customs  
Enforcement

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:

(b)(7)(E)

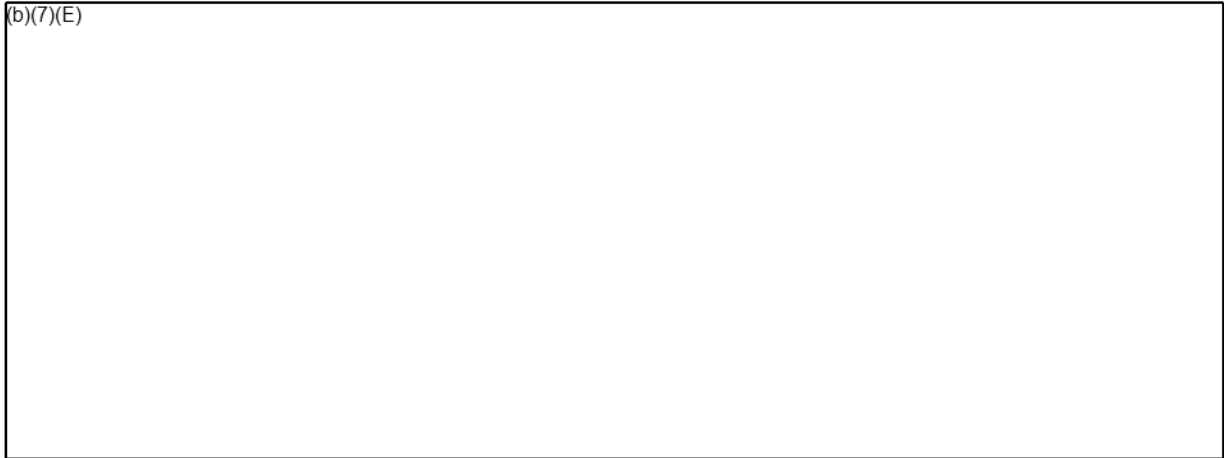
Background:

(b)(7)(E)

Management Controls and Accountability

(b)(7)(E)

(b)(7)(E)

A large rectangular area of the page is redacted, indicated by a black border. The text "(b)(7)(E)" is written in the top-left corner of this area.

Legal Process and Court Orders

(b)(7)(E)

A very large rectangular area of the page is redacted, indicated by a black border. The text "(b)(7)(E)" is written in the top-left corner of this area.

(b)(7)(E)



(b)(7)(E)



~~LAW ENFORCEMENT SENSITIVE~~

Applications for Use of Cell-Site Simulators

(b)(7)(E)



(b)(7)(E)



~~LAW ENFORCEMENT SENSITIVE~~

Data Collection, Recordkeeping, and Disposal

(b)(7)(E)



State and Local Partners

(b)(7)(E)



Coordination and Ongoing Management

(b)(7)(E)

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.

(b)(7)(E)



# HSI

## POLICY GUIDANCE REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY

2020-ICLL\_00013 828





# Basic Uses

(b)(7)(E)

[Redacted content]

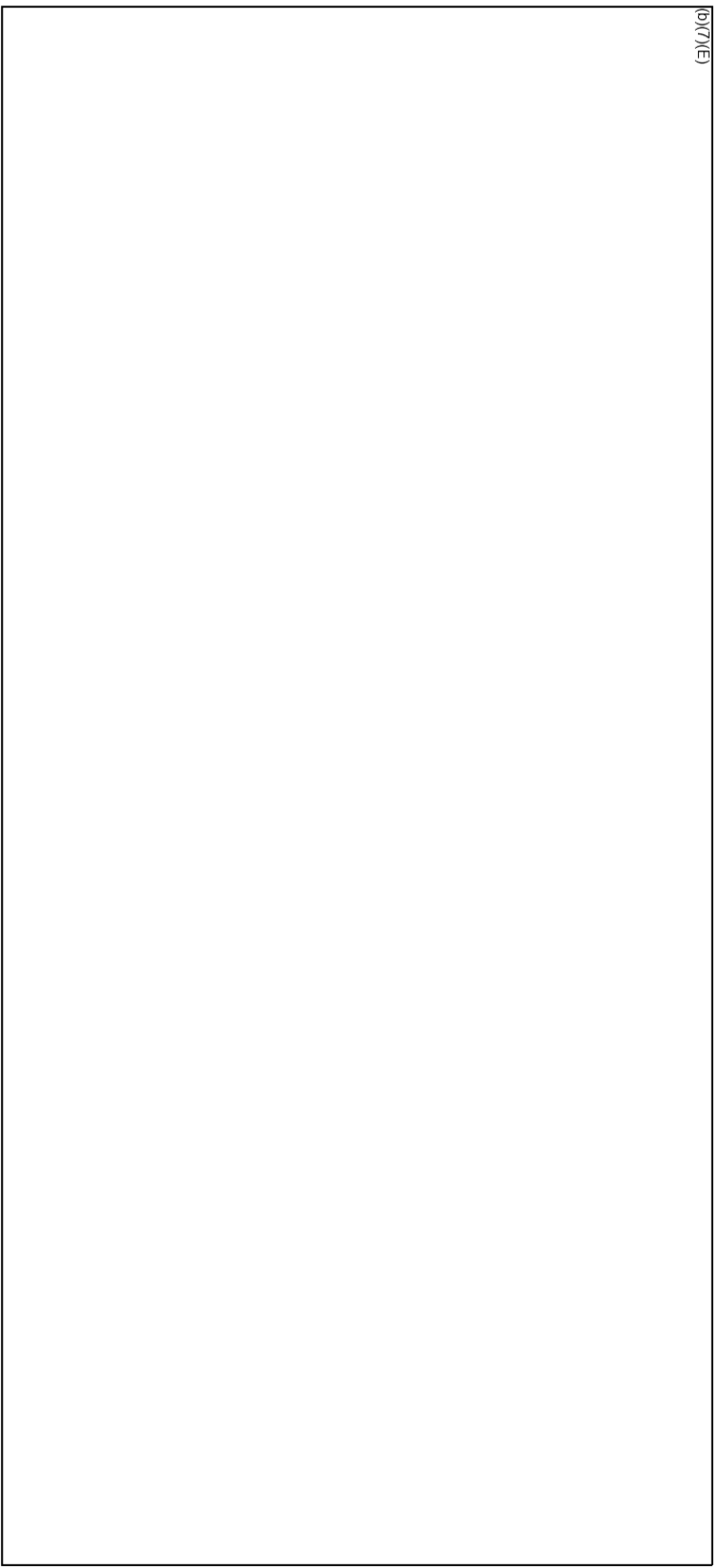
12/3/2019

2020-ICLI 00013 829



# How They Function

(b)(7)(E)



12/3/2019

2020-ICLI 00013 830



# How They Function

(b)(7)(E)

[Redacted content]

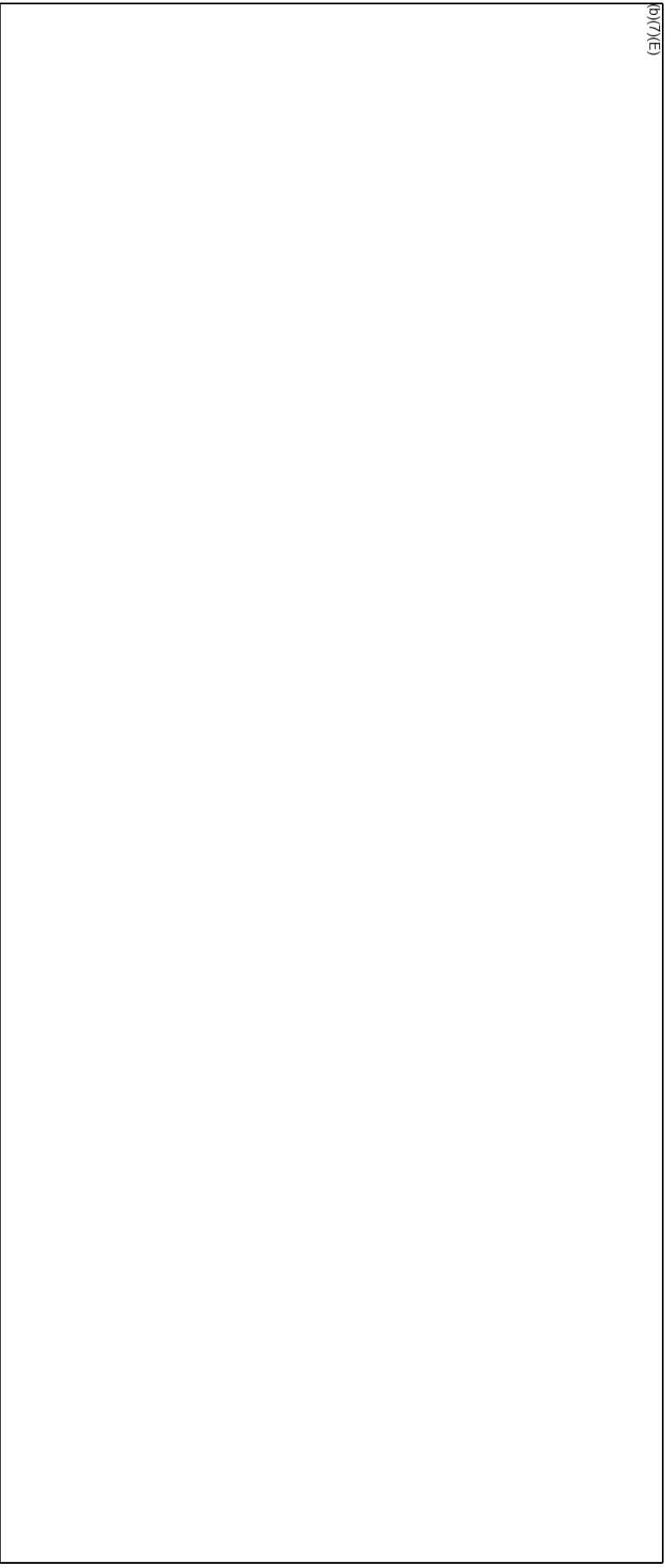
12/3/2019

2020-ICLI 00013 831



# How They Function

(b)(7)(E)



12/3/2019

2020-ICLI 00013 832

5





# HSI Cell-Site Simulators Obtain....

(b)(7)(E)

[Redacted content]

12/3/2019

2020-ICLI 00013 833



# HSI Cell-Site Simulators DO NOT....

(b)(7)(E)

12/3/2019

2020-ICLI 00013 834



# PEN Register Configuration

(b)(7)(E)

[Redacted content]

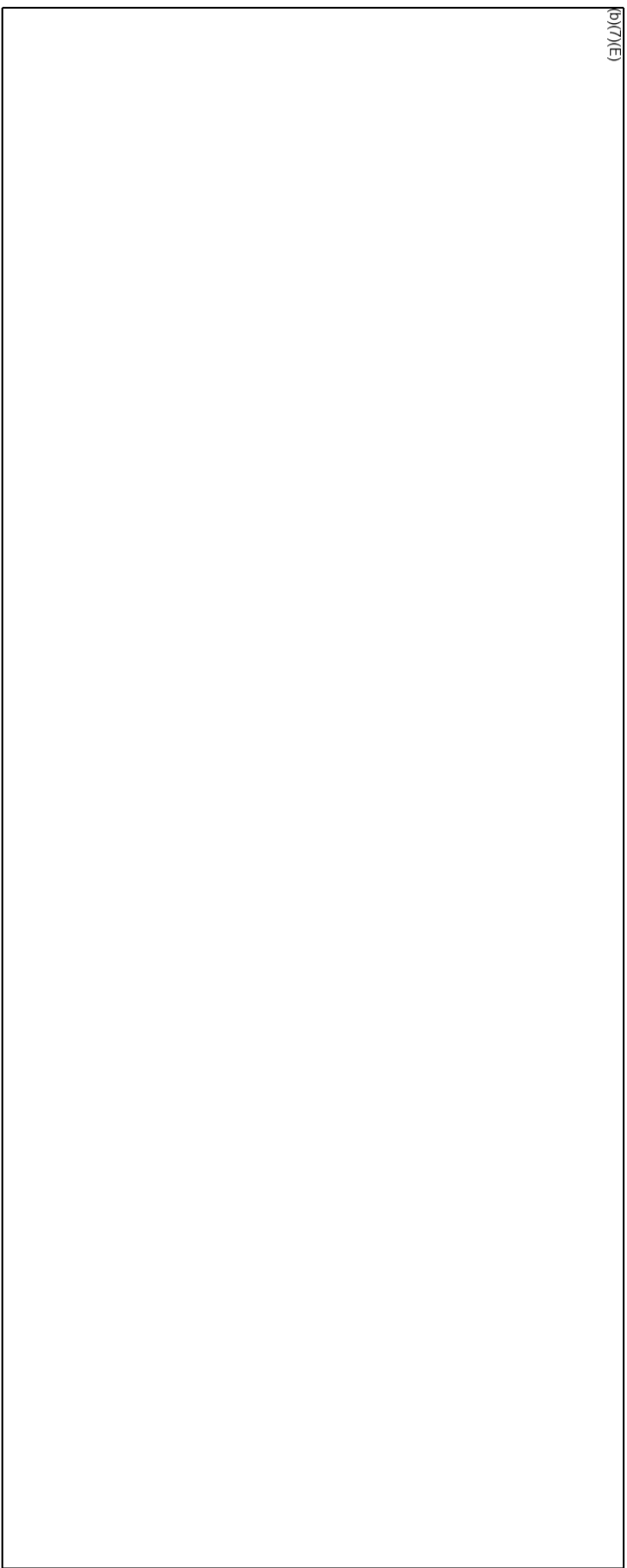
12/3/2019

2020-ICLI 00013 835



# Management and Accountability

(b)(7)(E)



12/3/2019

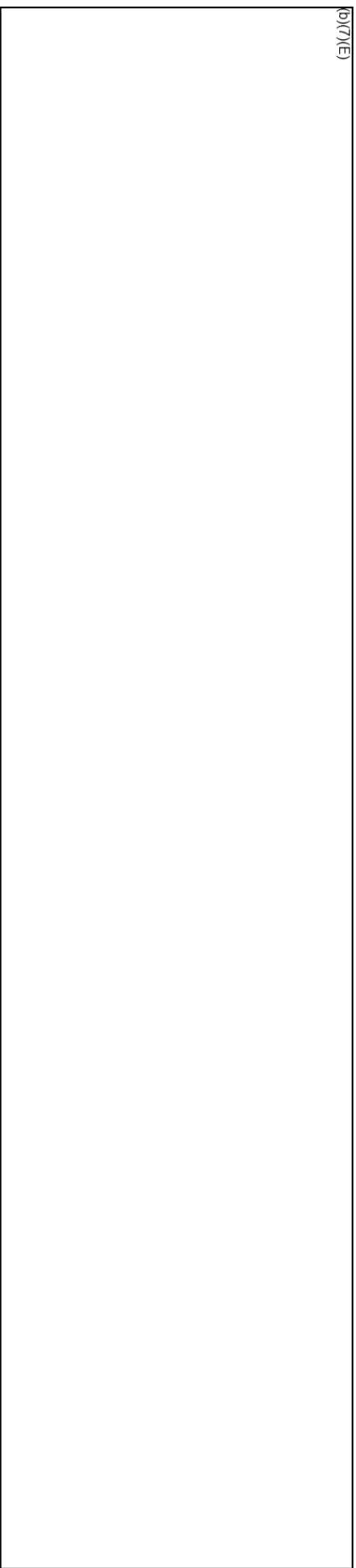
2020-ICLI 00013 836





# Legal Process

(b)(7)(E)



12/3/2019

2020-ICLI 00013 837

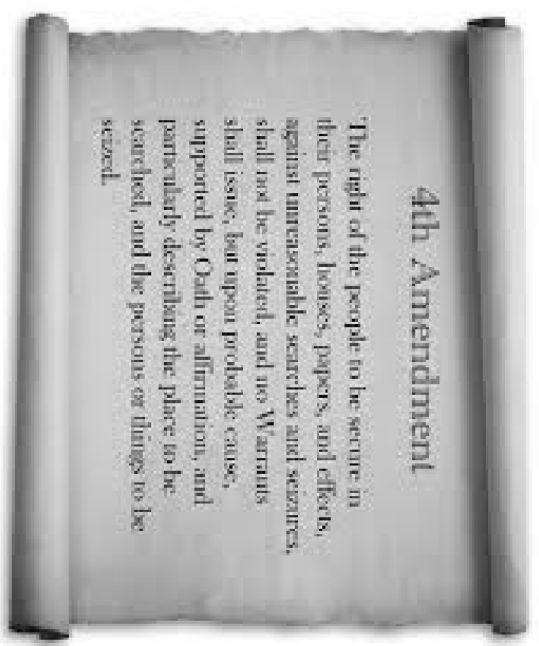
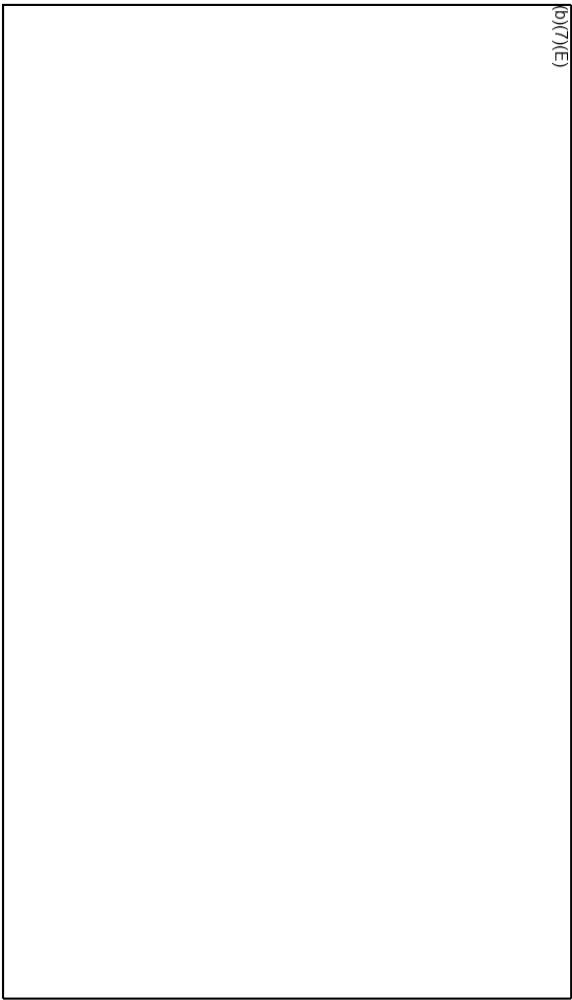
10





# Legal Process

(b)(7)(E)



12/3/2019

2020-ICLI 00013 838

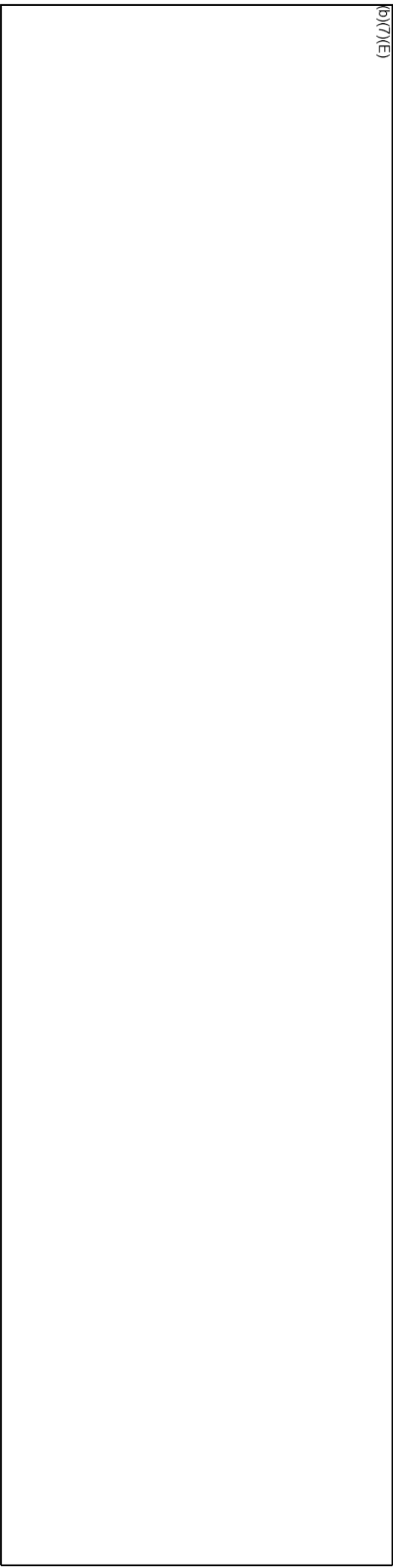
11





# Legal Process

(b)(7)(E)



12/3/2019

2020-ICLI 00013 839

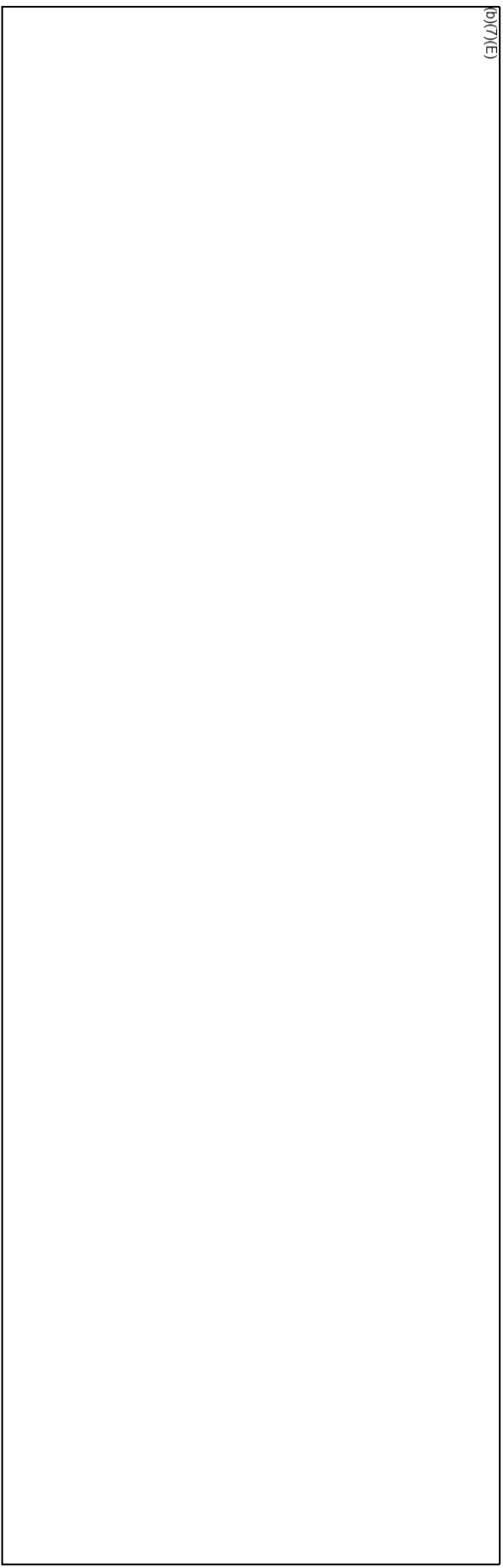
12





# Exigent Circumstances under the Fourth Amendment

[b](7)(E)



12/3/2019

2020-ICLI 00013 840

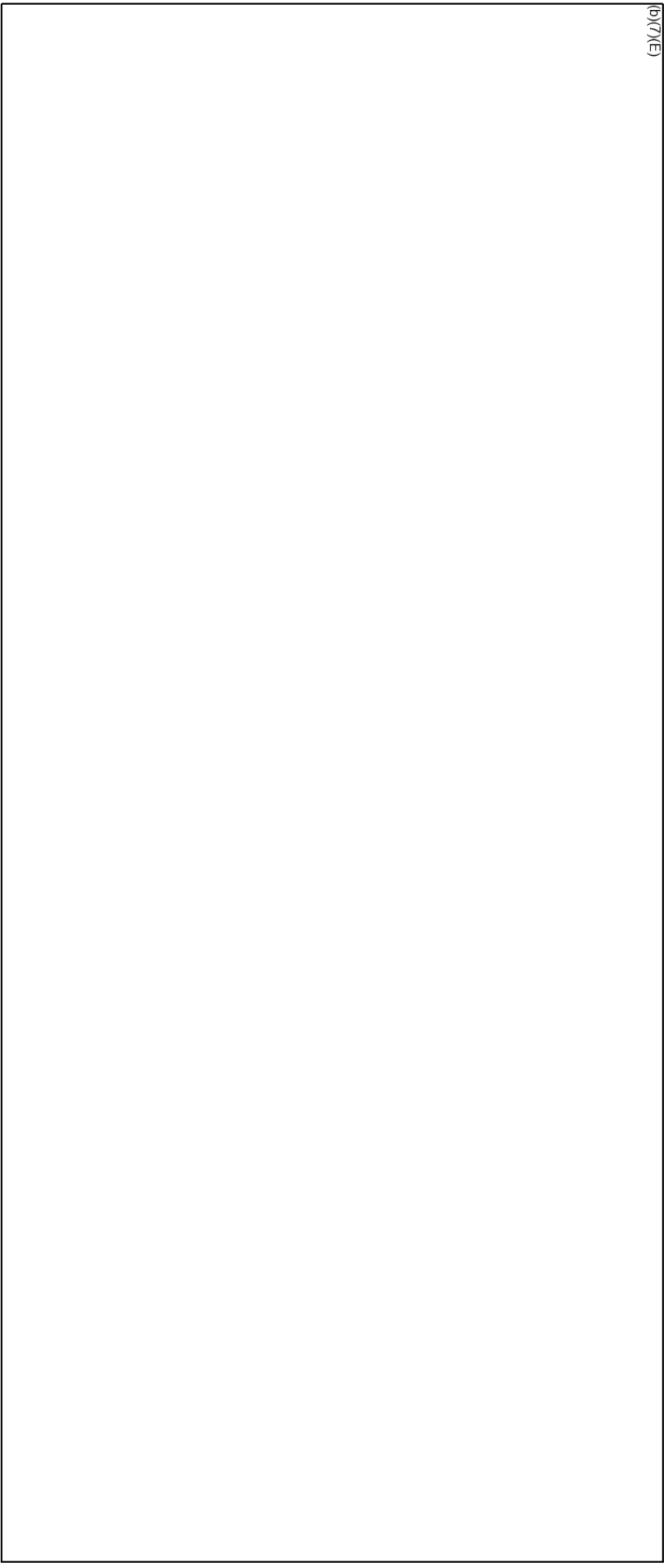
13





# Exigent Circumstances under the Fourth Amendment

(b)(7)(E)



12/3/2019

2020-ICLI 00013 841

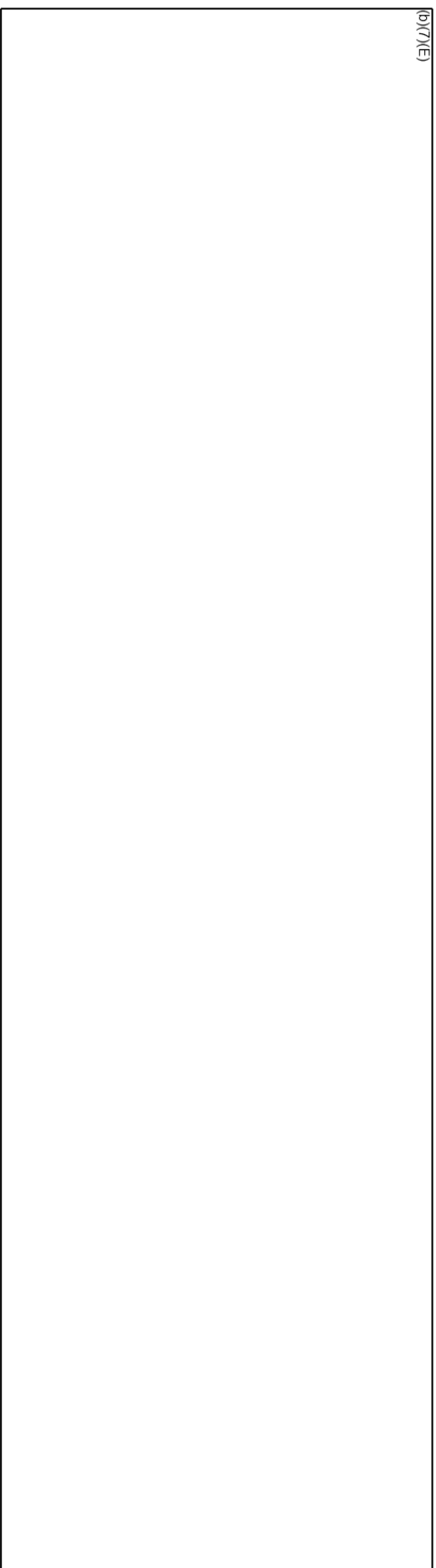
14





# Applications for Use of Cell-Site Simulators

(b)(7)(E)



12/3/2019

2020-ICLI 00013 842



# Applications for Use of Cell-Site Simulators

(b) (7)(E)

[Redacted Content]

12/3/2019

2020-ICLI 00013 843

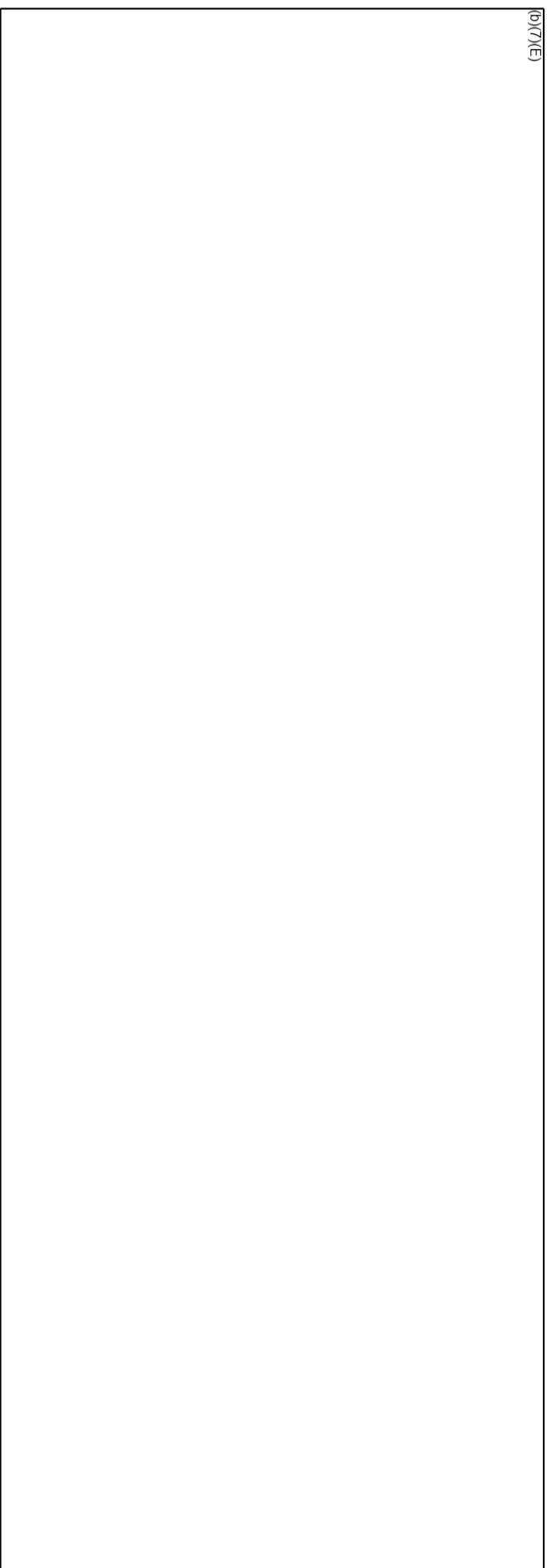
16





# Applications for Use of Cell-Site Simulators

(b)(7)(E)



12/3/2019

2020-ICLI 00013 844

17

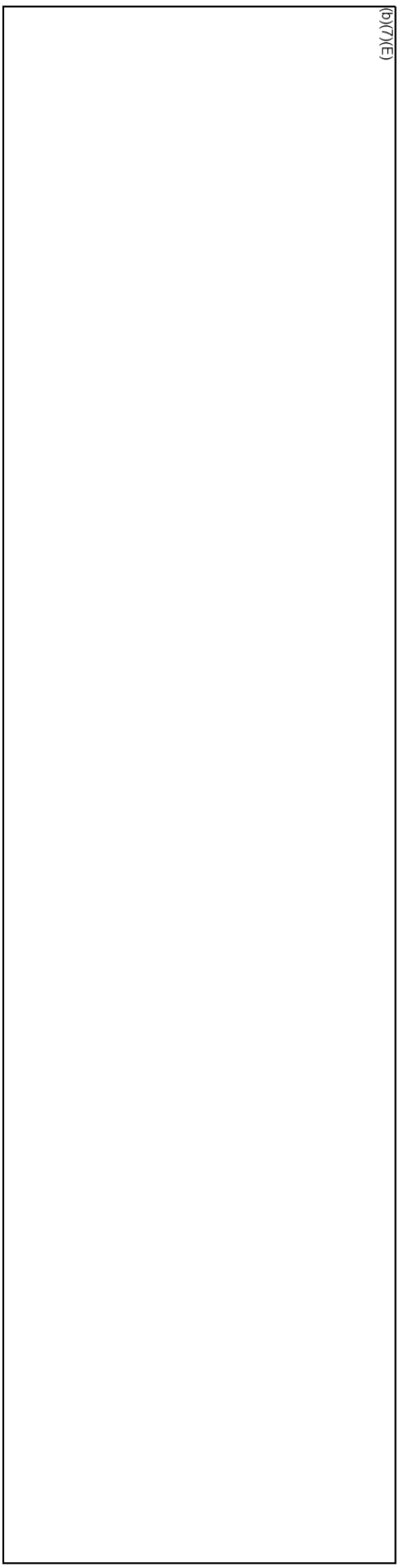






# Applications for Use of Cell-Site Simulators

(b)(7)(E)



12/3/2019

2020-ICLI 00013 845

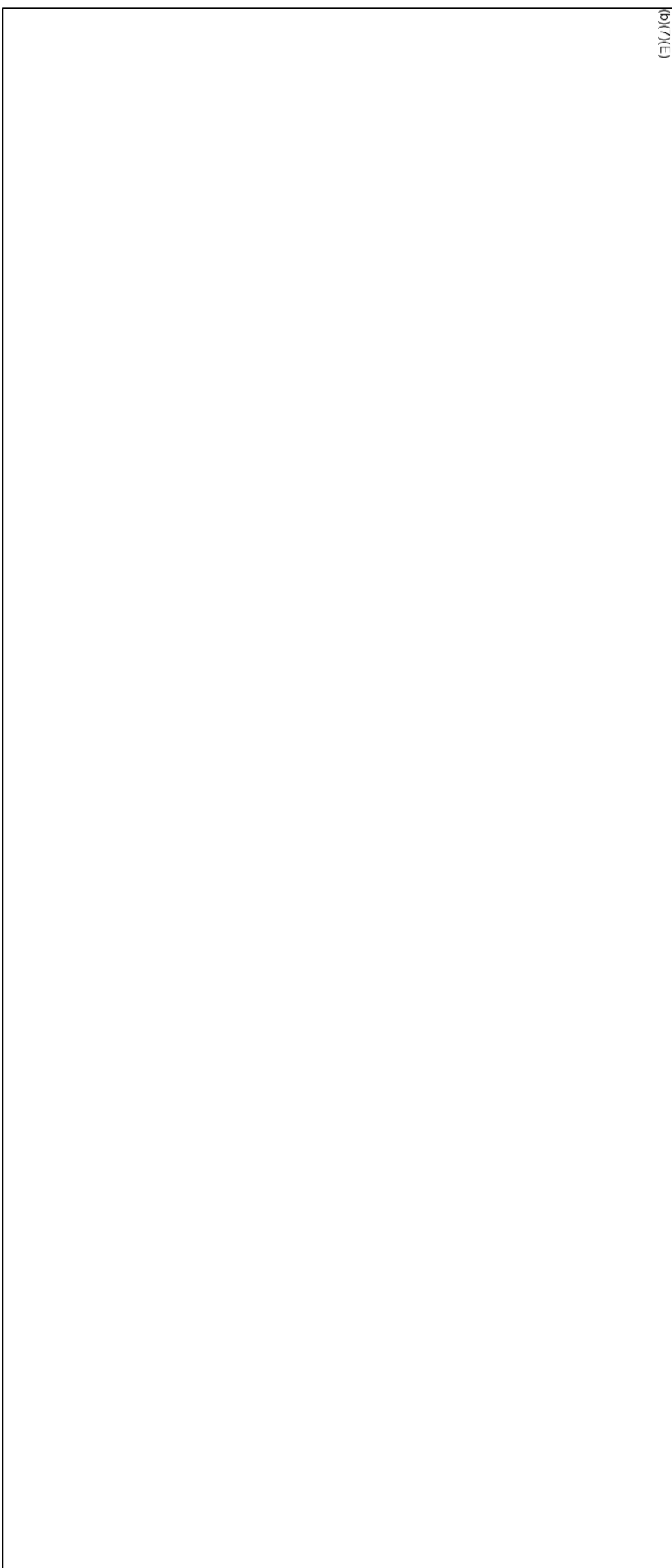
18





# Data Collection & Disposal

(b)(7)(E)



12/3/2019

2020-ICLI 00013 846

19



# Auditing

(b)(7)(E)

[Redacted content]

12/3/2019

2020-ICLI 00013 847

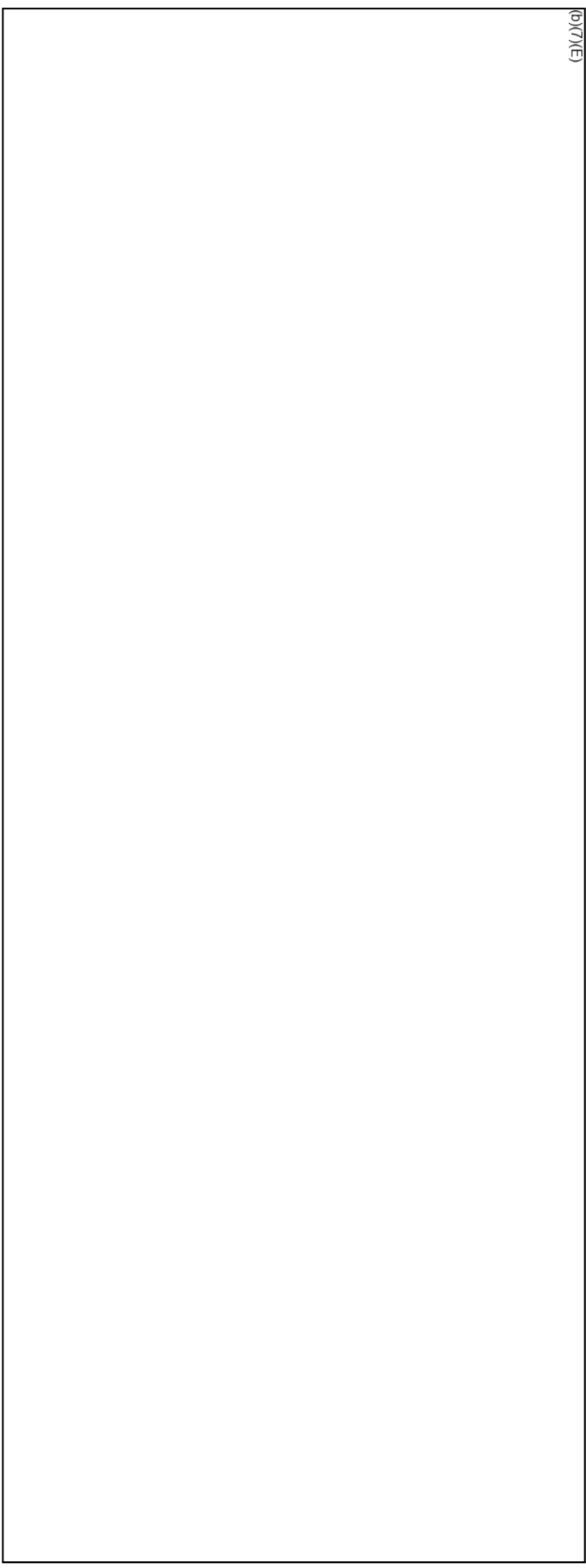
20





# Auditing

(b)(7)(E)



12/3/2019

2020-ICLI 00013 848

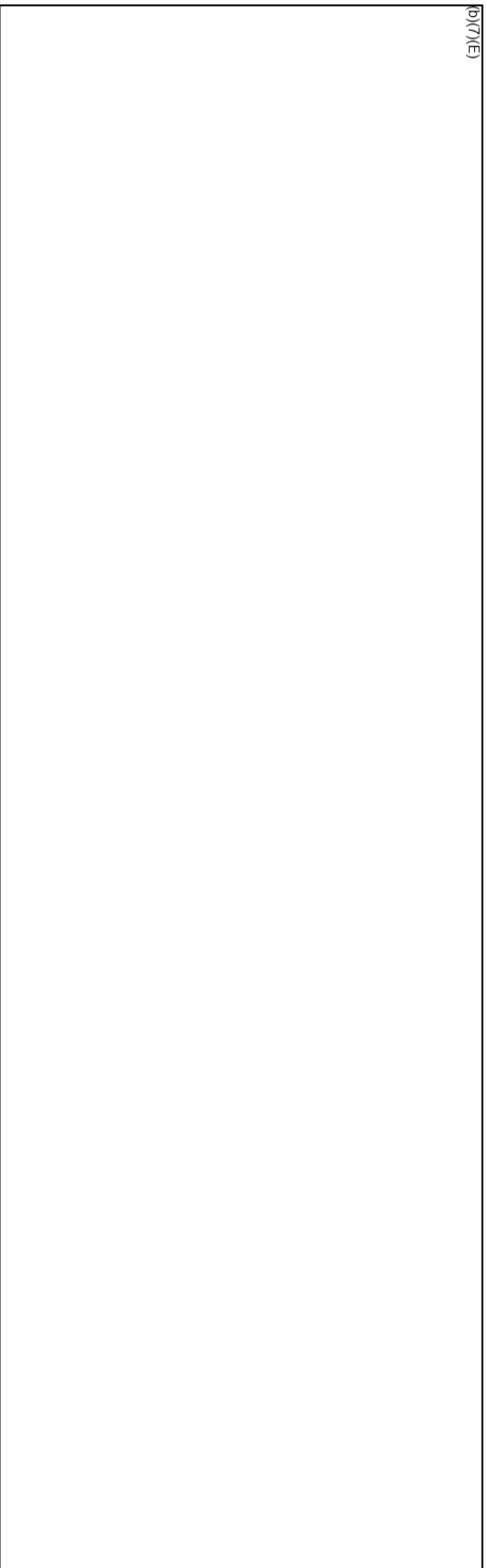
21





# State and Local Partners

(b)(7)(E)



12/3/2019

2020-ICLI 00013 849

22





# Training and Coordination

(b)(7)(E)



12/3/2019

2020-ICLI 00013 850

23





# 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)

# 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)

# 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)

# 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)

# 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)

# 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)

# 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)

# 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)



# 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)

# Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

March 7, 2019

March 1, -March 7, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

March 15, -March 21, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April

4, 2019

March 29, -April 4, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

April 12, -April 17, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

April 26, -May 2, 2019

Target Located

Arrests

(b)(7)(E)

# Technical Operations CSS Weekly Report

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

May 3, -May 9, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

May 16, -May 23, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June

6, 2019

May 31, -June 6, 2019

Target Located

Arrests

(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)



# Technical Operations CSS Weekly Report

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

June 13, -June 20, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

June 27, -July 5, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

July 12, -July 18, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

July 26, -August 1, 2019

Target Located

Arrests

(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)



# Technical Operations CSS Weekly Report

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

August 8, -August 15, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

August 28, 2019

August 23, -August 28, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

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

September 6, -September 12, 2019

Target Located

Arrests

(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)

# Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

September 26, 2019

September 21, -September 26, 2019

Target Located

Arrests

(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)



# Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

October 4, 2019

October 4, -October 7, 2019

Target Located

Arrests

(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)

# 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)

# 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)

# 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)

# 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)

# 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)

# 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)



# 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)

**From:**

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

**Sent:**

2 Apr 2013 11:47:54 -0400

**To:**

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

**Cc:**

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

**Subject:**

RE: Stingray/Portable Cell Tower Technology

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

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

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

Regards

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

*Unit Chief  
Technical Operations  
Homeland Security Investigations  
Immigration & Customs Enforcement  
Department of Homeland Security  
Desk: (703) 551-(b)(6);  
Cell: (571) 245-(b)(7)(C)*  
(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Tuesday, April 02, 2013 10:54 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: Stingray/Portable Cell Tower Technology

Thanks (b)(6). If I could get a briefing sometime in the next couple of weeks on this, I would appreciate it. Happy to head down to TechOps if that's easier. Just let me know.

(b)(6):

Privacy Officer  
Assistant Director for Privacy & Records  
U.S. Immigration & Customs Enforcement  
Direct: (202) 732-(b)(6);  
Main: (202) 732-(b)(7)(C)

Questions? Please visit the Privacy & Records Office website at <http://intranet.ice.dhs.gov/sites/ooop/>.

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, April 01, 2013 5:57 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: Stingray/Portable Cell Tower Technology

(b)(6);

I have copied in TechOps Unit Chief (b)(6); (b)(7)(C) as the Stingray program for HSI is under his shop with devices dispersed throughout the US (b)(6); can provide you with a briefing and information on the HSI program managed by TechOps.

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

Thanks

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

Deputy Assistant Director  
Law Enforcement Support & Information Management (LESIM)  
Homeland Security Investigations (HSI)  
Immigration and Customs Enforcement (ICE)  
Department of Homeland Security (DHS)  
(202) 732-(b)(6);

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

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, April 01, 2013 5:42 PM

**To:** (b)(6); (b)(7)(C)

**Subject:** FW: Stingray/Portable Cell Tower Technology

**Importance:** High

Let's talk...

(b)(6);

Privacy Officer

Assistant Director for Privacy & Records

U.S. Immigration & Customs Enforcement

Direct: (202) 732-(b)(6);

Main: (202) 732-(b)(7)(C)

Questions? Please visit the Privacy & Records Office website at <http://intranet.ice.dhs.gov/sites/ooop/>.

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, April 01, 2013 2:42 PM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** Stingray/Portable Cell Tower Technology

**Importance:** High

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

(b)(5); (b)(7)(E)

- 1) **Slate: FBI Files Unlock History Behind Clandestine Cellphone Tracking Tool**  
[http://www.slate.com/blogs/future\\_tense/2013/02/15/stingray\\_imsi\\_catcher\\_fbi\\_files\\_unlock\\_history\\_behind\\_cellphone\\_tracking.html](http://www.slate.com/blogs/future_tense/2013/02/15/stingray_imsi_catcher_fbi_files_unlock_history_behind_cellphone_tracking.html)
- 2) **Wall Street Journal: 'Stingray' Phone Tracker Fuels Constitutional Clash**  
<http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html>
- 3) **The Washington Post: Little-known surveillance tool raises concerns by judges, privacy activists**  
[http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f\\_story.html](http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html)

(b)(5); (b)(7)(E)

I'm out on Tuesday, April 2, 2013, but am free this afternoon and much of the remainder of this week if you need to chat.

Best wishes,

(b)(6);  
(b)(7)(C)

(b)(6); (b)(7)(C)

**M.S., J.D., CIPP/US/G**  
**Directorate Privacy Officer | Science & Technology Directorate | Department of Homeland Security**  
**202-254-(b)(6) Office | 202-527-(b)(6) Blackberry (b)(6); (b)(7)(C) @hq.dhs.gov**

**From:** (b)(6); (b)(7)(C)  
**To:**  
**Cc:**  
**Subject:** HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment  
**Date:** Monday, January 12, 2015 1:23:29 PM

---

(b)(6);  
(b)(7)(C)

(b)(6);  
(b)(7)(C) advised you were requesting HSI policy information. See below HSI policy for the use of Use of Over-The-Air Wireless (Cellular) Tracking Equipment. HSI HB14-04 Technical Operations Handbook dated 07/21/2014.

### 16.1 Use of Over-The-Air Wireless (Cellular) Tracking Equipment

(b)(5); (b)(7)(E)

Please let me know if you require additional information.

(b)(6); (b)(7)(C)

Section Chief  
Investigative Intercept Section  
Technical Operations  
ICE-Homeland Security Investigations  
U.S. Department of Homeland Security  
Lorton, VA  
703-551-(b)(6); Desk  
703-599-(b)(7)(C) Cell

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** 12 Jan 2015 14:23:31 -0500  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

(b)(5); (b)(7)(E)

(b)(6); (b)(7)(C) (CTR)  
AGS, Inc.  
Privacy Compliance Specialist  
In support of the ICE Privacy Office  
U.S. Immigration and Customs Enforcement

Direct: 202-732-(b)(6);  
Main: 202-732-(b)(7)(C)

For help with privacy questions, please visit the ICE Intranet at

<https://insight.ice.dhs.gov/mgt/oop/>

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, January 12, 2015 2:21 PM  
**To:** (b)(6); (b)(7)(C) (CTR); (b)(6); (b)(7)(C)  
**Subject:** RE: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

Get the language from them on this too: are required to submit reports in accordance with Section 19.4 of this Handbook

(b)(6);  
Privacy Officer  
Assistant Director for Privacy & Records  
U.S. Immigration & Customs Enforcement  
Direct: (202) 732-(b)(6);  
Main: (202) 732-(b)(7)(C)

Questions? Please visit the Privacy & Records Office website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.

---

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** Monday, January 12, 2015 1:35 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

FYI

(b)(6); (b)(7)(C) (CTR)  
AGS, Inc.  
Privacy Compliance Specialist  
In support of the ICE Privacy Office  
U.S. Immigration and Customs Enforcement  
  
Direct: 202-732-(b)(6);  
Main: 202-732-(b)(7)(C)

For help with privacy questions, please visit the ICE Intranet at <https://insight.ice.dhs.gov/mgt/oop/>

---

**From:** (b)(6);  
**Sent:** Monday, January 12, 2015 1:23 PM  
**To:** (b)(6); (b)(7)(C) (CTR)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

(b)(6); (b)(7)(C)



(b)(6); (b)(7)(C) advised you were requesting HSI policy information. See below HSI policy for the use of Use of Over-The-Air Wireless (Cellular) Tracking Equipment. HSI HB14-04 Technical Operations Handbook dated 07/21/2014.

(b)(5); (b)(7)(E)

Please let me know if you require additional information.

(b)(6); (b)(7)(C)

Section Chief  
Investigative Intercept Section  
Technical Operations  
ICE-Homeland Security Investigations  
U.S. Department of Homeland Security  
Lorton, VA  
703-551-(b)(6) Desk  
703-599-(b)(7) Cell

~~Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.~~

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** 31 Jan 2019 17:32:00 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Surveillance Technologies PIA  
**Attachments:** HSI Surveillance Technologies PIA TechOps Draft (01 31 19).docx

H(b)(6);

Attached please find a draft of the Surveillance Technologies PIA for your review.

Please let me know if I can provide any additional information.

Best,

(b)(6);  
(b)(7)(C)

(b)(6);  
(b)(7)(C)

Supporting the Office of Information Governance & Privacy  
U.S. Immigration and Customs Enforcement

(b)(6); @associates.ice.dhs.gov

(Mobile) (b)(6); (b)(7)(C)



Privacy Impact Assessment  
for the

# Homeland Security Investigation (HSI) Surveillance Technologies

**DHS/ICE/PIA-048**

**January 31, 2019**

**Contact Point**

**Derek N. Benner**

**Executive Associate Director**

**Homeland Security Investigations**

**U.S. Immigration and Customs Enforcement**

**(202) 732-(b)(6);  
(b)(7)(C)**

**Reviewing Official**

**Philip S. Kaplan**

**Chief Privacy Officer**

**Department of Homeland Security**

**(202)343-(b)(6);  
(b)(7)(C)**

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)





(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)





(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)





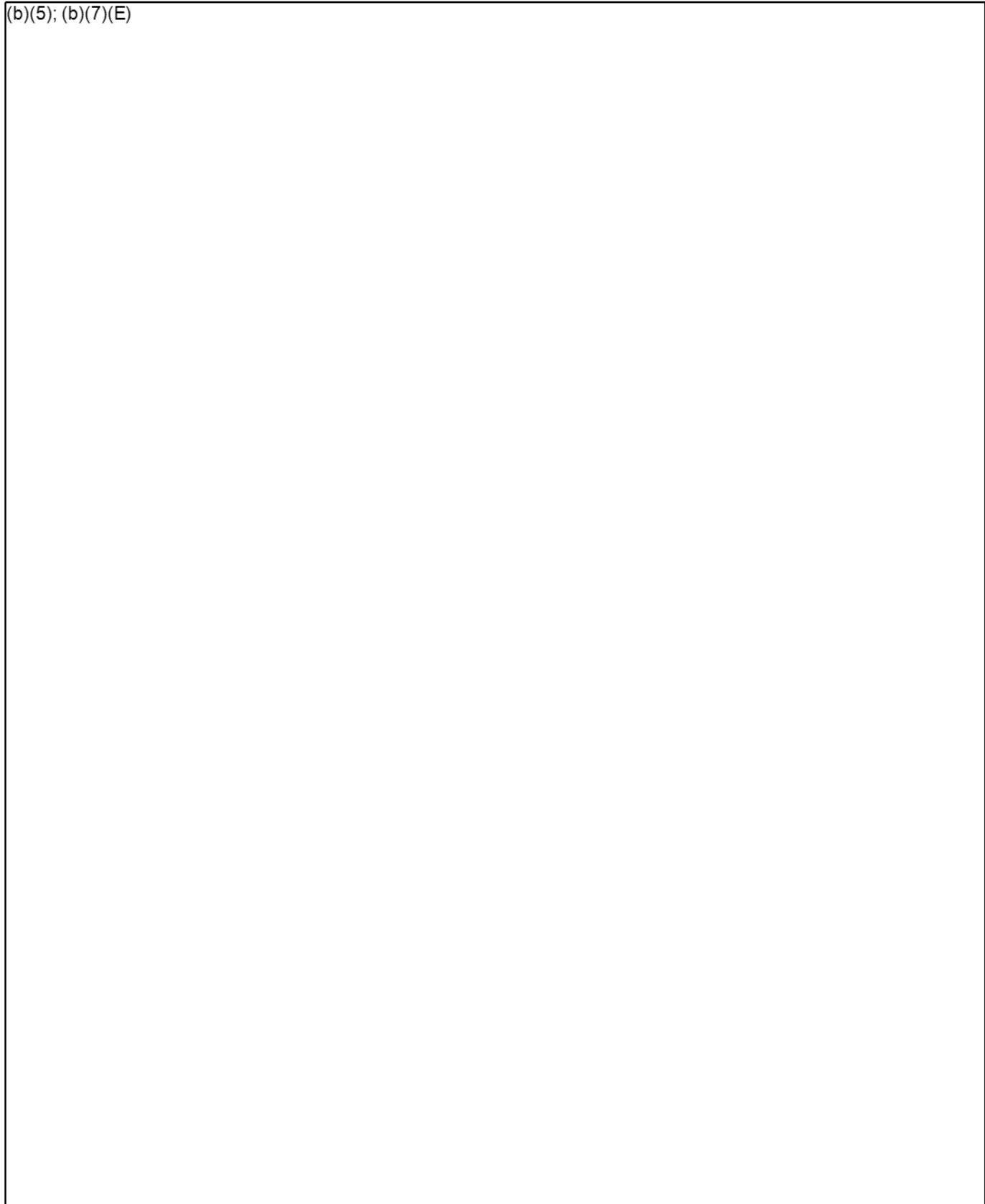
(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)





(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

## Responsible Officials

Program Manager:

## Approval Signature Page

---

Philip S. Kaplan  
Chief Privacy Officer  
Department of Homeland Security



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)





# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)





# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



# Homeland Security

The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

(b)(5); (b)(7)(E)



**U.S. Immigration  
and Customs  
Enforcement**

February 16, 2017

MEMORANDUM FOR     Derek Benner  
                                  Deputy Executive Associate Director  
                                  Homeland Security Investigations

FROM:                     Lyn Rahilly  
                                  Assistant Director

SUBJECT:                 Comments on HSI Policy Use of Cell-Site Simulator Technology

Thank you for the opportunity to review this draft policy. As use of this technology has been the focus of much attention in the media and from Congress, I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

Training Requirements

I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

I also recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



Recordkeeping

I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

When responding to a letter on cell-site simulators from several (b)(7)(E)  
DHS provided information about how the surveillance outcomes are documented within HSI.  
The DHS response is below:

*Q. How long is the collected information retained? How is this information disposed of, and what timeframe is your agency using to dispose of information collected by such devices?*

(b)(5); (b)(7)(E)

See (b)(7)(E) final, p.9.

Assuming it is still accurate, I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

cc: Scott Lanum, Assistant Director, ODCR  
Debbie Seguin, Assistant Director, Policy

<sup>1</sup> This recommendation (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** 8 Nov 2018 14:15:30 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C) (CTR)  
**Subject:** RE: ICE HSI Cell Site Simulator Log PTA

Thanks (b)(6);

I will work with (b)(6); to update the (b)(7)(E) to include the information regarding the Cell Site Simulators. We are currently waiting for an updated Draft from the Program Office.

Thanks,  
(b)(6);

---

**From:** (b)(6);  
**Sent:** Thursday, November 8, 2018 8:41 AM  
**To:** (b)(6); (b)(7)(C) @ice.dhs.gov > (b)(6); (b)(7)(C) (CTR)  
<(b)(6); (b)(7)(C) @associates.ice.dhs.gov >  
**Cc:** (b)(6); (b)(7)(C) @ice.dhs.gov >; (b)(6); (b)(7)(C) (CTR)  
(b)(6); @associates.ice.dhs.gov >  
**Subject:** RE: ICE HSI Cell Site Simulator Log PTA

Thanks (b)(6);  
(b)(7)(C)

If possible I would rather keep everything in one PTA than to write separate ones.

(b)(6) - would you be able to work with (b)(6); to update the (b)(7)(E) to include information regarding Cell Site Simulators?

Regarding PIA coverage, I know that (b)(6); is currently working on updating the (b)(7)(E) PIA, so this might be something we need to address. I've also copied (b)(6); since he'll be writing a PIA on (b)(7)(E) (b)(7)(E) generally, which might be a better fit.

Let's get the bulk of the PTA done first, and then we can determine where PIA coverage should fall.

(b)(6); (b)(7)(C)  
Deputy Privacy Officer  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Desk: 202-732-(b)(6);  
Mobile: 202-70-(b)(6);  
Main: 202-732-(b)(6);

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx>

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, November 8, 2018 8:35 AM

To: (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6); (b)(7)(C) (CTR)  
(b)(6); (b)(7)(C) @associates.ice.dhs.gov>

**Subject:** FW: ICE HSI Cell Site Simulator Log PTA

**Importance:** High

H (b)(6);

I received the email below (and a screen shot attached) from the PM, (b)(6); for the Cell Site Simulator Log – he says that their program was told by someone here in ICE Privacy that because this is just the log of what action was taken (in a SharePoint site) ICE Privacy was going to include this log where the Cell Site Simulator is discussed in the existing (b)(7)(E) and a new PTA for the log is not needed.

From the shared drive, I see the (b)(7)(E) is currently under review for renewal by (b)(6); copied here.

(b)(5); (b)(6); (b)(7)(C)

---

**From:** (b)(6);

**Sent:** Wednesday, November 7, 2018 4:45 PM

**To:** (b)(6); (b)(7)(C) @ice.dhs.gov>

**Subject:** RE: ICE HSI Cell Site Simulator Log PTA

(b)(6);

I was under the impression that this was not required. My DA [redacted] spoke with someone in the privacy office several months ago and it was determined that we would either not need a PTA or it would be added under the [redacted]

Thanks,

[redacted]  
[redacted]  
Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-[redacted] Desk  
571-839-[redacted] Mobile  
[redacted]@ICE.DHS.GOV

Technical Support: ICE Service Desk: (888) 34-[redacted]  
VECADS Support: VECADS 24/7 Support Desk: (888) [redacted] or  
[redacted]@ice.dhs.gov  
CVN Support: Spectrum Support Desk: (703) 551-[redacted]@ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

**From:** [redacted]@ice.dhs.gov>  
**Date:** Wednesday, Nov 07, 2018, 16:12  
**To:** [redacted]@ice.dhs.gov>  
**Subject:** ICE HSI Cell Site Simulator Log PTA

Hi [redacted]  
I've recently joined ICE Privacy as a detailee from CBP Privacy to support them while they back-fill some of the vacancies left in their office. I know you were working with both [redacted] and [redacted] on this PTA, but neither are in this office at this time. I believe [redacted] has left, and [redacted] is out on training, returning in a month or so. I'm here until the end of the year, and was hoping to assist in closing out some of the backlog of PTAs. For this reason, [redacted], Acting Privacy Officer for [redacted] has assigned this PTA to me to see if we can move it up to DHS HQ Privacy (PRIV).

Attached is the latest email between you and [redacted] with the most recent version of the PTA. I'm not sure if you've had an opportunity to respond to [redacted] questions/comments, but before I dove too deep into this, I wanted to check with you to be sure we're working on the most recent version. Can

you please let me know where you are on this PTA, and send me the updated/edited version so I can review and assist you in getting this cleared through PRIV?

Thanks,

(b)(6);

(b)(6); (b)(7)(C)

Sr. Privacy Analyst (detailed to)  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement

202-394-(b)(6); Mobile

(b)(6); (b)(7)(C)@ice.dhs.gov

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx>

**From:** (b)(6); (b)(7)(C)  
**Sent:** 30 Dec 2014 15:43:05 -0500  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: PTA for Stingray

(b)(6);  
(b)(7)(C)

Understood and will do.

Please note that I have also copied (b)(6); and (b)(6); (b)(7)(C) on your email so that they are aware of this request.

Have a Happy New year!

**Regards.**

(b)(6); (b)(7)(C)

Section Chief  
Information Systems Security Office  
Law Enforcement Support & Information Sharing (LESIM)  
**ICE/Homeland Security Investigations (HSI)**  
Department of Homeland Security (DHS)  
Office: 202-732-(b)(6);  
Mobile: 202-421-(b)(7)(C)  
(b)(6); (b)(7)(C) @ice.dhs.gov

ISSO Support: [HSI-LESIM-ISSO@ice.dhs.gov](mailto:HSI-LESIM-ISSO@ice.dhs.gov)

~~Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, December 30, 2014 3:36 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** PTA for Stingray

Hi (b)(6);

We received a letter from the Senate inquiring on privacy compliance for HSI's Stingray surveillance technology. We worked on the response last week with an agent named (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) down in (b)(7)(E) who was very helpful. It's clear the Senators were very interested in whether my office had conducted a privacy review of this technology, and we have not as it is not required under the law or DHS policy. In light of their concerns, however, we promised to do one.

What I suggest is (b)(5)  
(b)(5); (b)(6); (b)(7)(C)

If you could have them send the PTA to my new deputy, (b)(6); (b)(7)(C) when it's done, that would be great.

(b)(6);  
**Privacy Officer**  
**Assistant Director for Privacy & Records**  
**U.S. Immigration & Customs Enforcement**  
Direct: (202) 732-(b)(6)  
Main: (202) 732-(b)(6);

Questions? Please visit the Privacy & Records Office website at <https://insight.ice.dhs.gov/mgt/ooop/Pages/index.aspx>.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** 17 Nov 2014 15:32:17 -0500  
**To:** (b)(6); (b)(7)(C)  
(ICE-HSI) (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: Stingrays Fox News

Many thanks!

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, November 17, 2014 3:32 PM  
**To:** Edge, Peter T (b)(6); (b)(7)(C) (ICE-HSI);  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** Re: Stingrays Fox News

I agree.

(b)(6); (b)(7)(C)  
Deputy Principal Legal Advisor  
(305) 970 (b)(6) (cell)  
(202) 732 (b)(6) (desk)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

-----  
Sent from my BlackBerry Wireless Handheld

---

**From:** Edge, Peter T  
**Sent:** Monday, November 17, 2014 03:27 PM  
**To:** (b)(6); (b)(7)(C) (ICE-HSI);  
(b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: Stingrays Fox News

(b)(5) is appropriate.



Peter T. Edge  
Executive Associate Director  
Homeland Security Investigations- ICE  
202-732-(b)(6) office

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, November 17, 2014 3:24:03 PM  
**To:** (b)(6); (b)(7)(C) Edge, Peter T.; (b)(6); (b)(7)(C) (ICE-HSI); (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** FW: Stingrays Fox News

Folks –

Fox News is asking us if we have a response to a FOIA'd document tweeted out by a senior ACLU member (see below) about the fact that ICE uses the "Harris Stingray II" system to listen in on phone conversations. The FOIA'd docs (which you'll have to look up on a non-work computer or mobile device since our system blocks the link below), is a redacted purchase order showing a contract from the ICE Office of Investigations dated Sept. 2010 for some of the related technology and devices. It looks like it was the ICE attaché office in Amman.

I've discussed with (b)(6) and our sense is (b)(5)

(b)(5)

HSI/OPLA/Privacy – do you feel differently?

Many thanks!

(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C) [mailto:(b)(6); (b)(7)(C)@FOXNEWS.COM]  
**Sent:** Monday, November 17, 2014 2:42 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Stingrays

Hey (b)(6),

Can you look at p. 44 (see link below) and comment on ICE using Harris Stingray II system similar system US Marshalls story from WSJ Friday to listen in to phone conversations?

Thank you,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

tweeted at 6:11 PM on Thu, Nov 13, 2014:

The US Marshals aren't the only feds with phone spying gear strapped to airplanes. ICE does it too. <https://t.co/u07ySUqsUz>  
(<https://twitter.com/csoghoian/status/533034551472586752?s=03>)

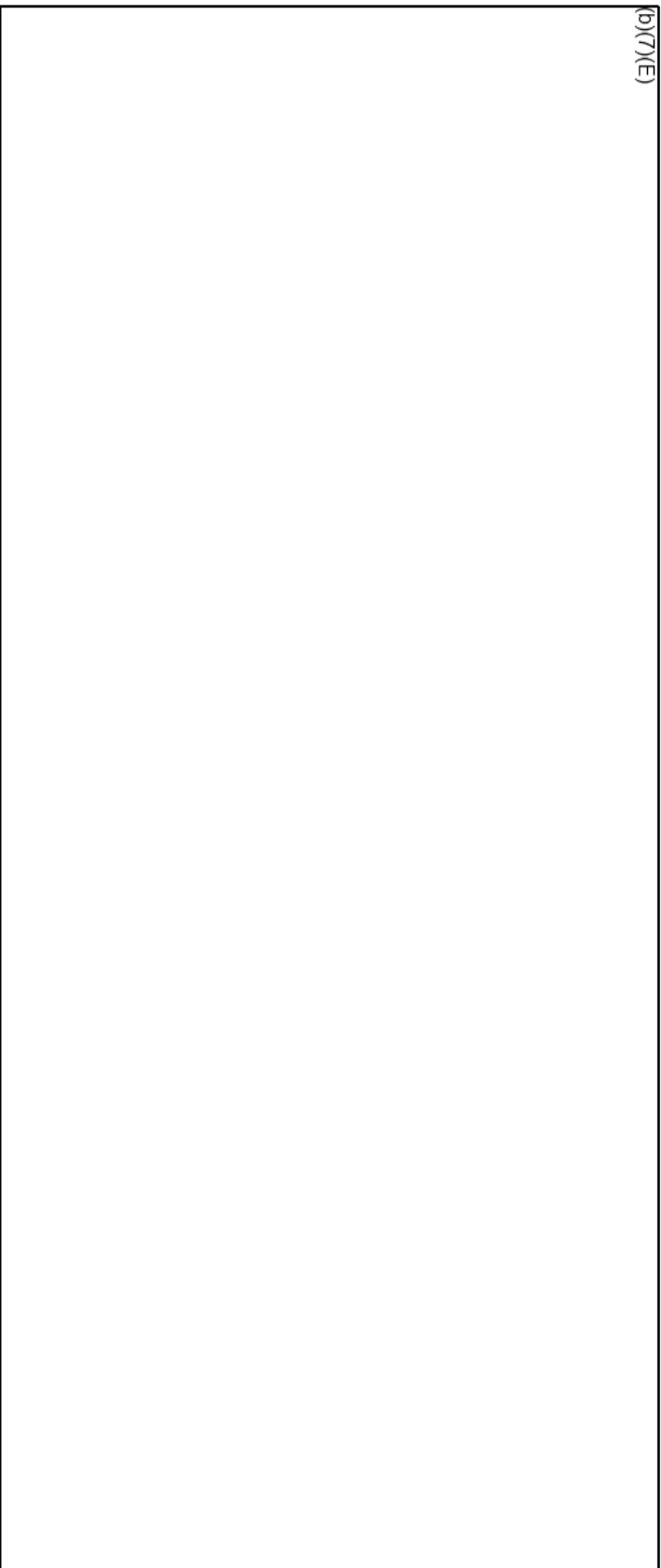
Stingray tracking system---

[http://en.wikipedia.org/wiki/Stingray\\_phone\\_tracker](http://en.wikipedia.org/wiki/Stingray_phone_tracker)

# Homeland Security Investigations (HSI)

## Basic Uses

(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

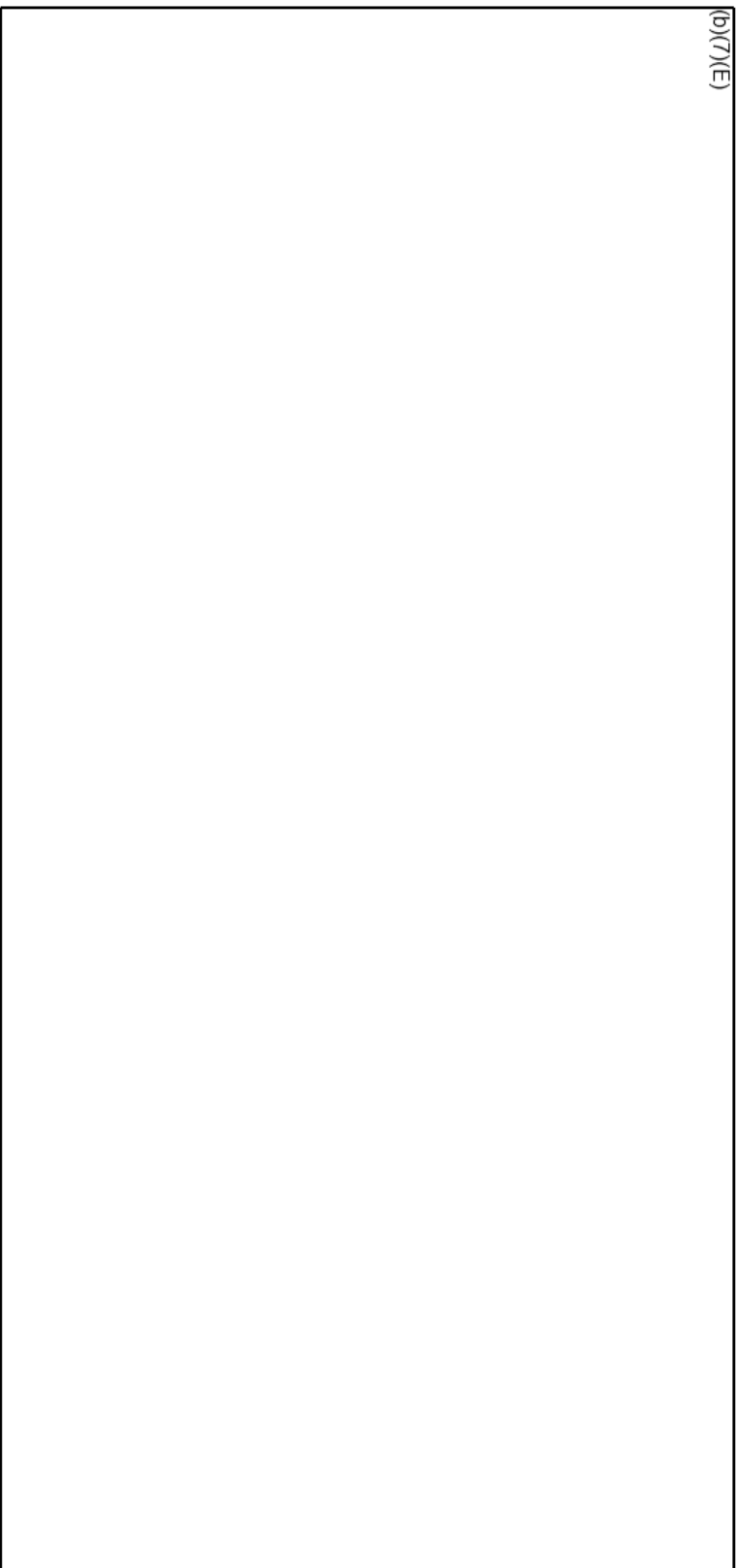
— ~~Law Enforcement Sensitive~~ —

# Homeland Security Investigations (HSI)

## How Cell-Site Simulators Function



(b)(7)(E)



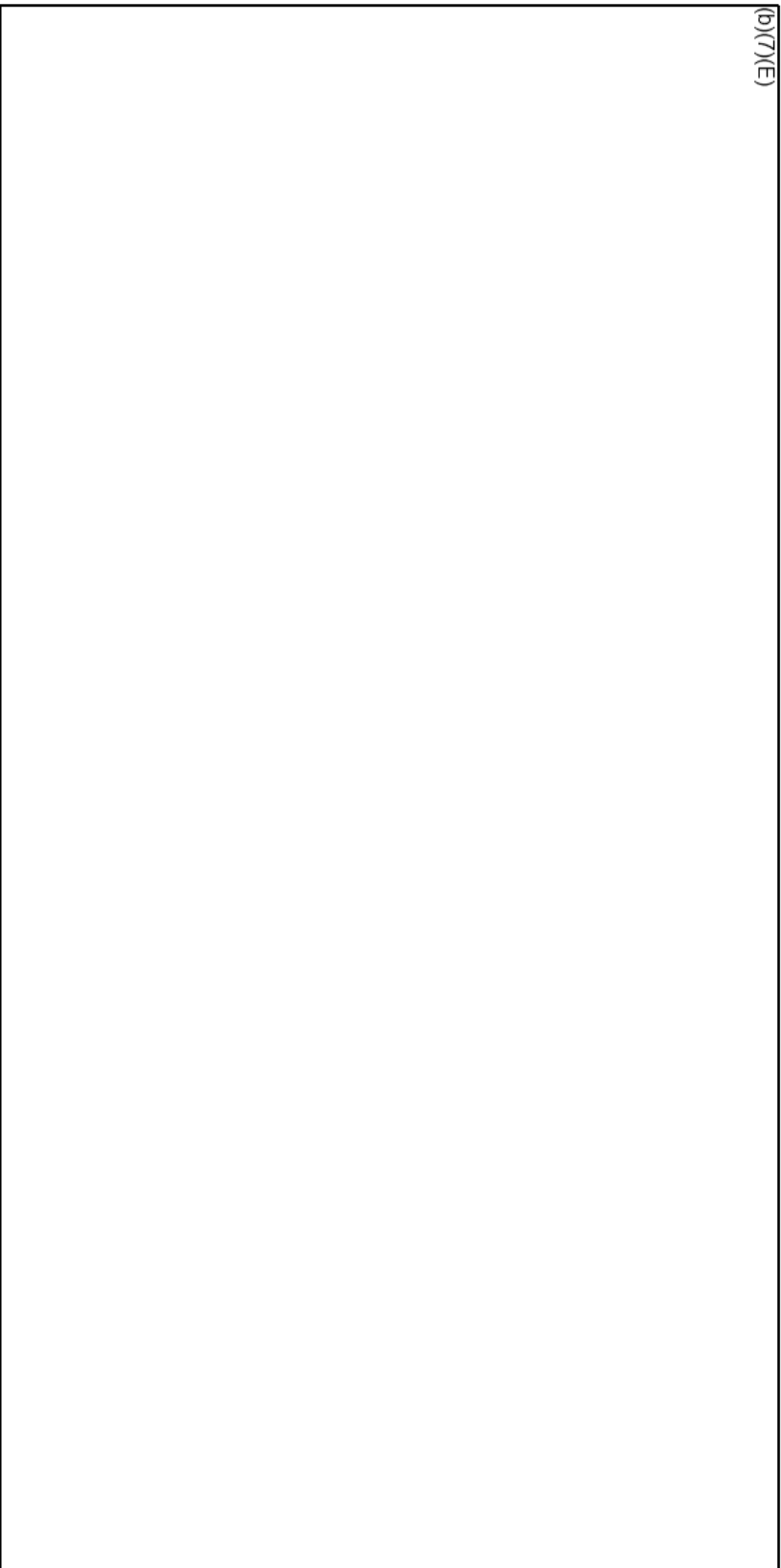
U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## How Cell-Site Simulators Function



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

~~Language for Confidential Source~~

## HSI Cell-Site Simulators Usage



HSI Cell-Site Simulators may obtain:

(b)(7)(E)

- [Redacted]
- [Redacted]
- [Redacted]



U.S. Immigration  
and Customs  
Enforcement

# HSI Cell-Site Simulators Usage



HSI Cell-Site Simulators Do Not:

(b)(7)(E)

- [Redacted]
- [Redacted]
- [Redacted]



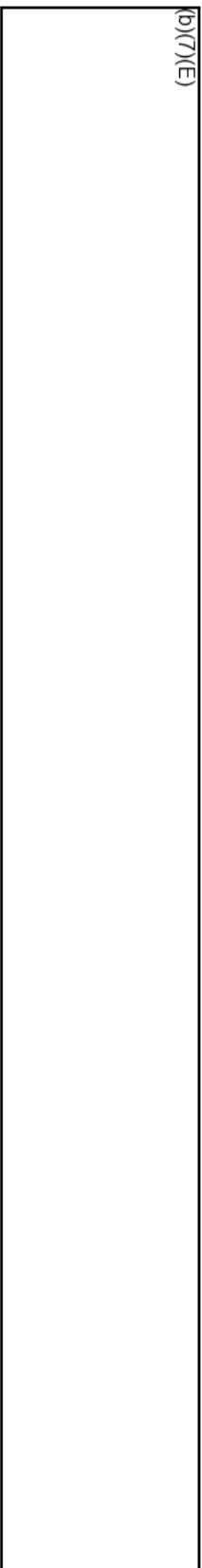
U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## HSI Cell-Site Simulators Usage



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

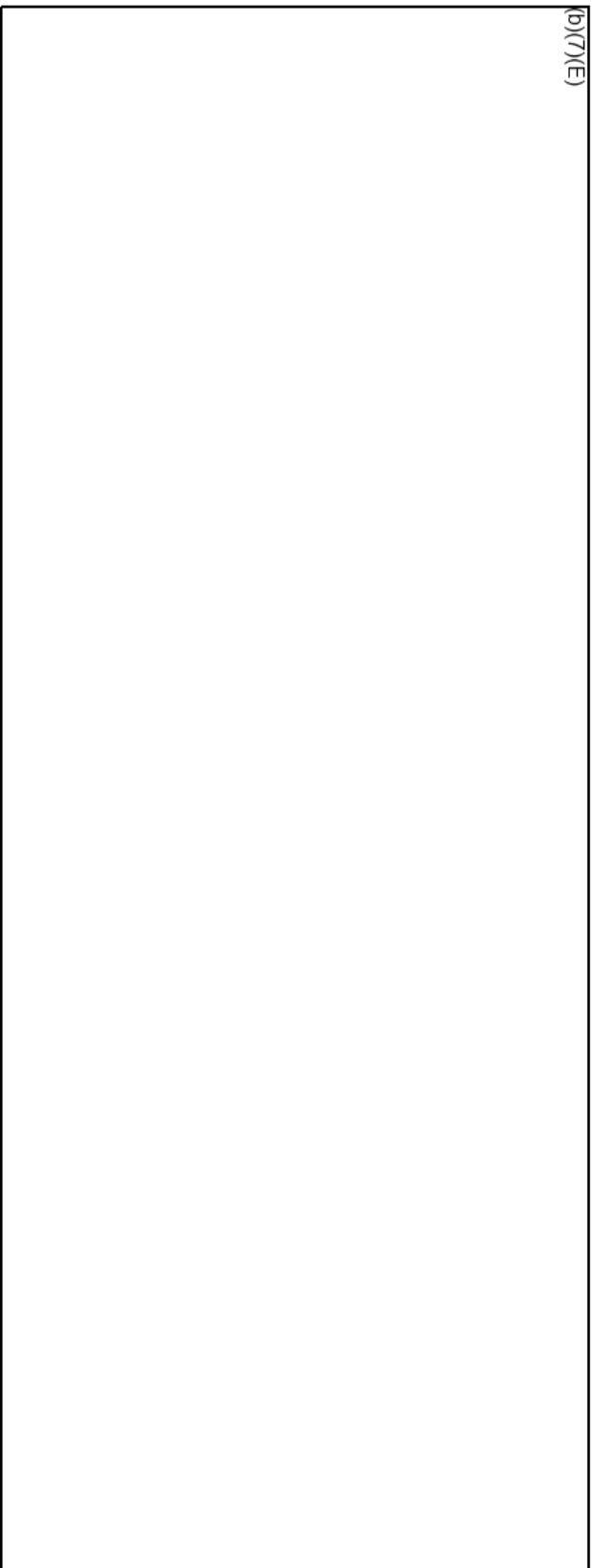


# Homeland Security Investigations (HSI)

## Management And Accountability



(b)(7)(E)



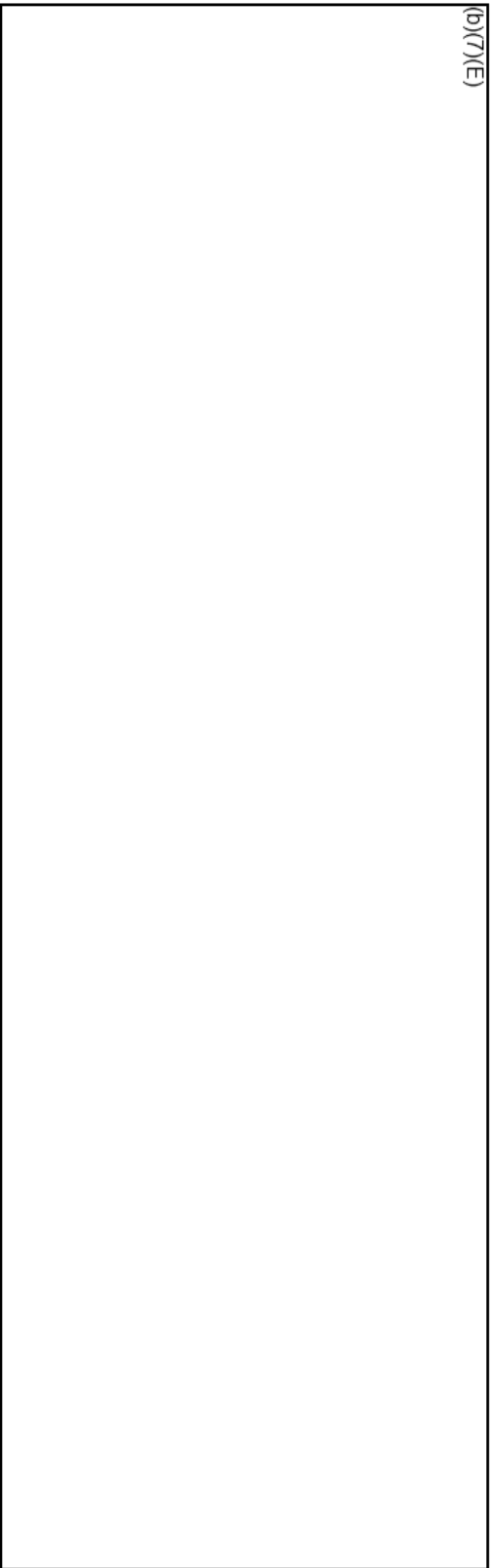
U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## Management And Accountability



(b)(7)(E)



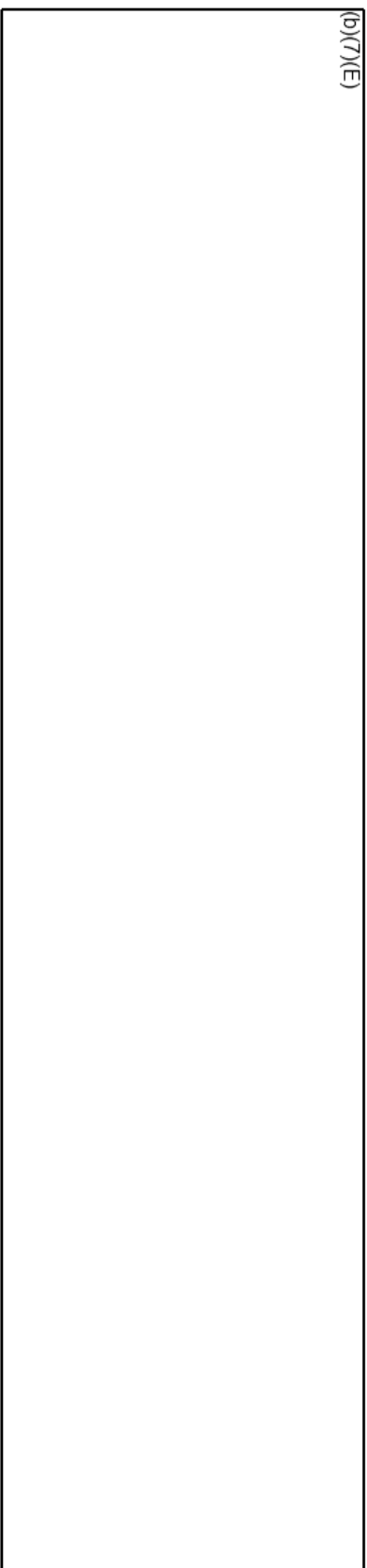
U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## Legal Process



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

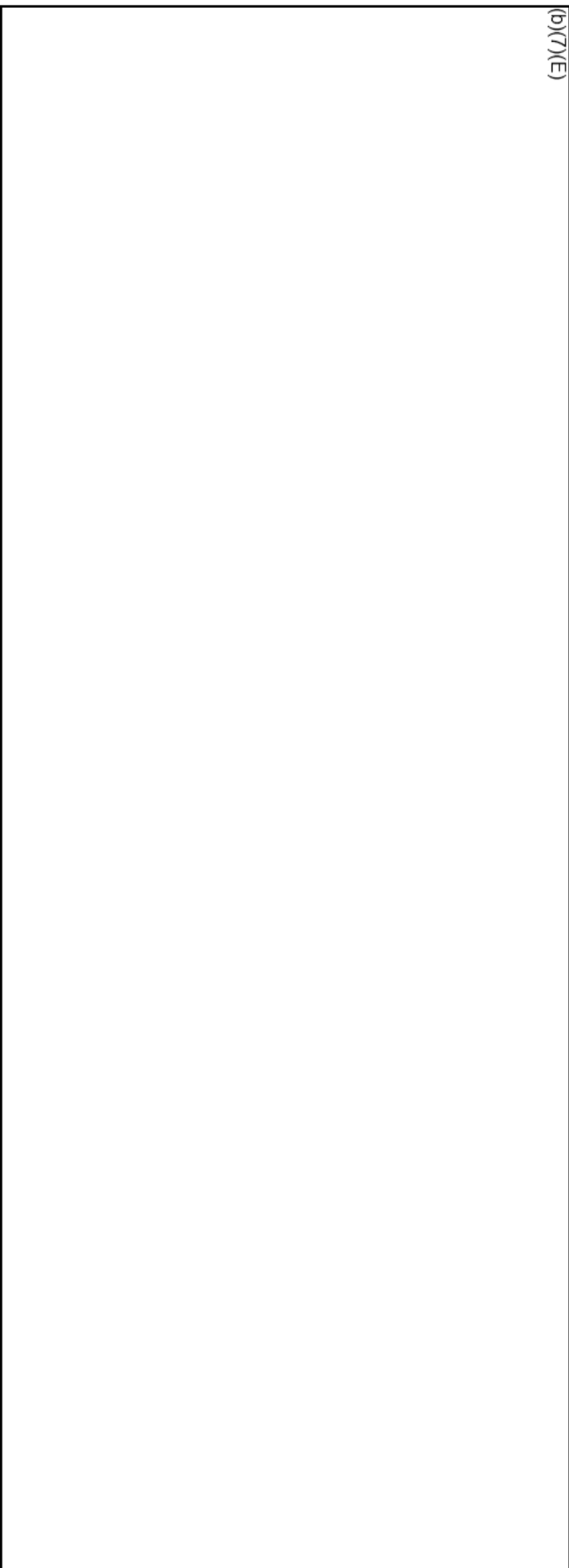
~~Law Enforcement Sensitive~~

# Homeland Security Investigations (HSI)

## Legal Process



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

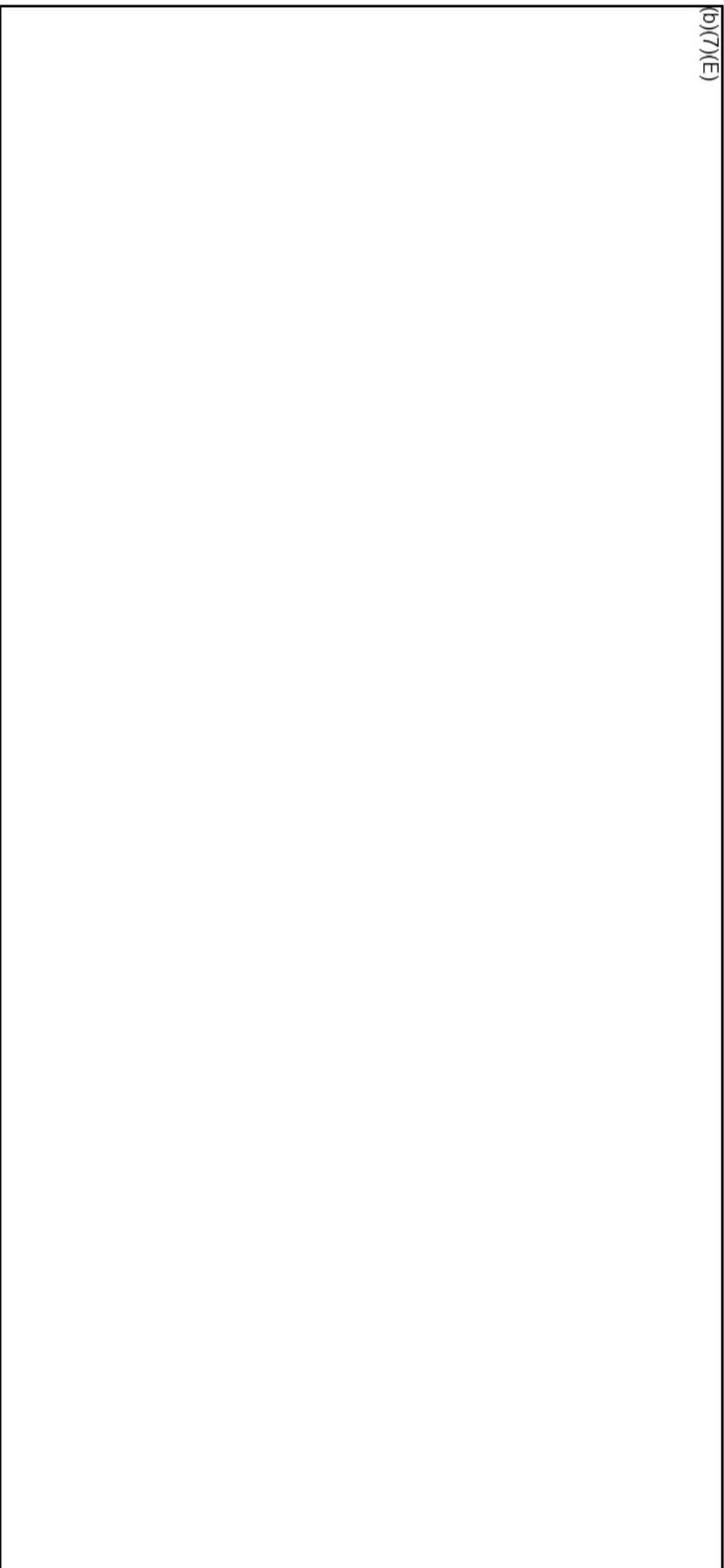
~~Law Enforcement Sensitive~~

# Homeland Security Investigations (HSI)



## Exigent Circumstances under the Fourth Amendment

(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## Exigent Circumstances under the Fourth Amendment



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

Language Operations Service

# Homeland Security Investigations (HSI)

## Exigent Circumstances under the Fourth Amendment



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

Language for Classified Sensitive

# Homeland Security Investigations (HSI)

## Applications for Use of Cell-Site Simulators



(b)(7)(E)

- 
- 
- 
- 



U.S. Immigration  
and Customs  
Enforcement



# Homeland Security Investigations (HSI)

## Applications for Use of Cell-Site Simulators



(b)(7)(E)

[Redacted content]



U.S. Immigration  
and Customs  
Enforcement

~~Law Enforcement Sensitive~~

# Homeland Security Investigations (HSI)

## Applications for Use of Cell-Site Simulators



(b)(7)(E)

[Redacted content]



U.S. Immigration  
and Customs  
Enforcement

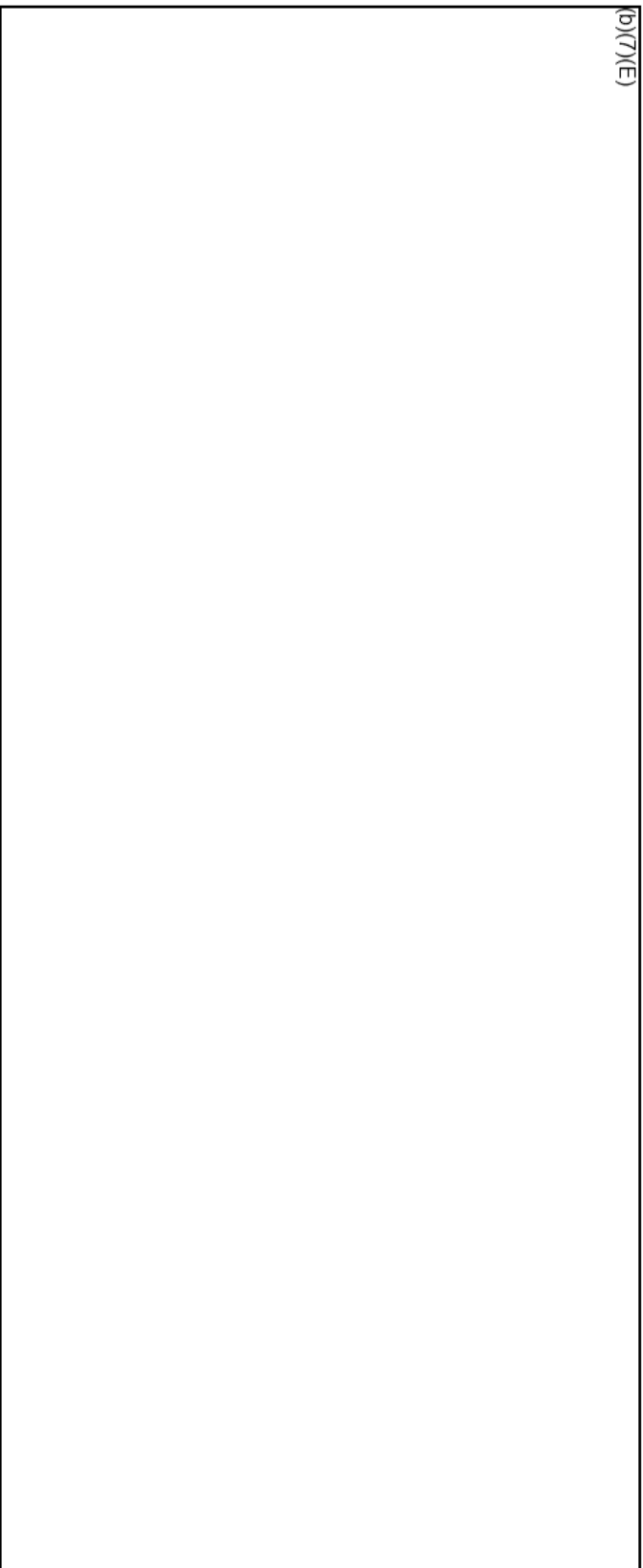
~~Law Enforcement Sensitive~~

# Homeland Security Investigations (HSI)

## Data Collection & Disposal



(b)(7)(E)



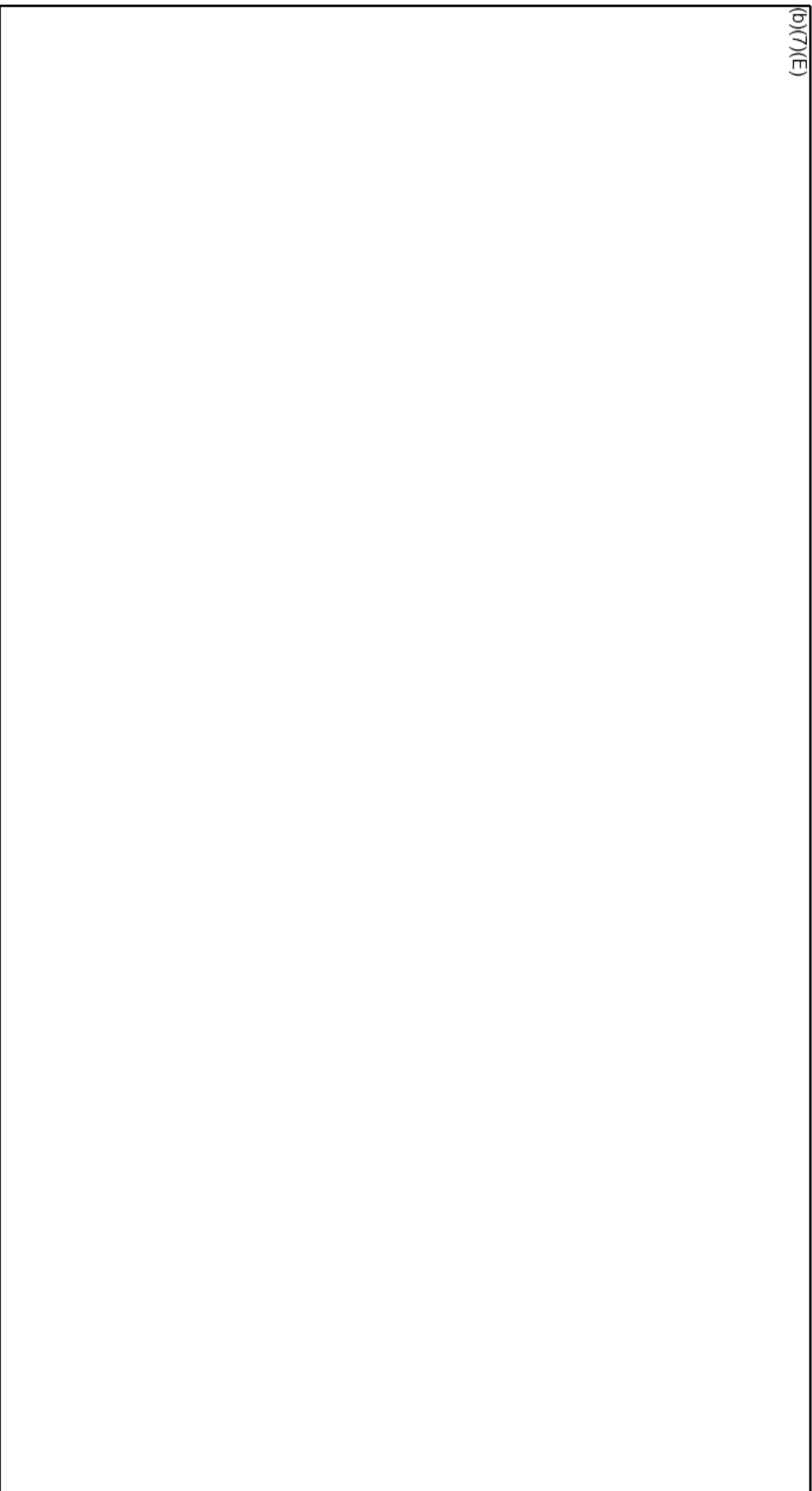
U.S. Immigration  
and Customs  
Enforcement

~~Law Enforcement Sensitive~~

# Homeland Security Investigations (HSI)

## Data Collection & Disposal

(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

Law Enforcement Sensitive

# Homeland Security Investigations (HSI)

## Training and Coordination

(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

— Law Enforcement Sensitive —

# Homeland Security Investigations (HSI)

## Improper Use of Cell-Site Simulators



Accountability is an essential element in maintaining the integrity of HSI. Activities involving the improper use of cell-site simulators, which are in contrast to the polices and procedures established by HSI in regard to these devices, as with other allegations of misconduct, will be reported to the ICE Office of Professional Responsibility or the Joint Intake Center.

U.S. Immigration  
and Customs  
Enforcement

Language Center



# Homeland Security Investigations (HSI)

## Frequently Asked Questions



(b)(7)(E)

Q:

A:

Q:

A:

[Redacted content]



U.S. Immigration  
and Customs  
Enforcement

~~For Official Use Only~~

# Homeland Security Investigations (HSI)

## Frequently Asked Questions



(b)(7)(E)

Q:

A:

Q:

A:



U.S. Immigration  
and Customs  
Enforcement



# Homeland Security Investigations (HSI)

## Frequently Asked Questions



(b)(7)(E)

Q:

A:

Q:

A:

[Redacted content]



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## Frequently Asked Questions



(b)(7)(E)

Q:

A:

Q:

A:

[Redacted content]



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)



For Questions Pertaining to the  
HSI Cell-Site Simulator Program,  
Please Contact:

Technical Operations Unit  
Cell-Site Simulator Program Manager

703-551- (b)(6); (b)(7)(C)



U.S. Immigration  
and Customs  
Enforcement



CNET News

## FBI prepares to defend 'Stingray' cell phone tracking

Privacy groups plan to tell a judge tomorrow that controversial cell phone tracking technology, used by federal police since at least the mid-1990s, violates Americans' Fourth Amendment rights.

by [Declan McCullagh](#) March 27, 2013 4:57 PM PDT



Follow [@declanm](#)

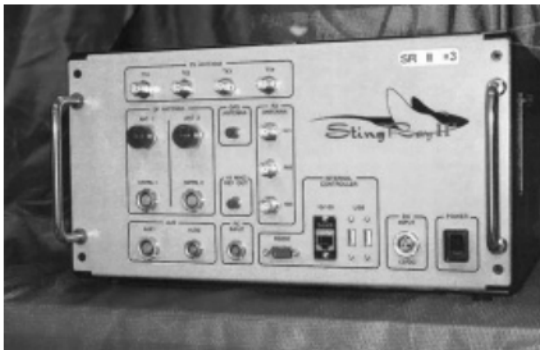


The FBI has used "stingray" cell-tracking technology since at least the mid-1990s. Now it's the focus of a constitutional challenge.

The Federal Bureau of Investigation's secretive "Stingray" surveillance technology that allows police to surreptitiously track the locations of cell phones and other mobile devices will itself go on trial in an Arizona courtroom tomorrow afternoon.

Attorneys representing the U.S. Department of Justice are expected to defend warrantless use of stingray devices, which trick mobile devices into connecting to them by impersonating legitimate cell towers. Prosecutors yesterday filed court documents saying stingrays were used in investigations in Arizona and Wisconsin going back to 2008.

In the legal skirmishing leading up to tomorrow's three-hour hearing, federal attorneys have told U.S. District Judge David Campbell that the defendant in this case, Daniel Rigmaiden, did not have reasonable "privacy expectations" in the whereabouts of his Verizon mobile broadband card and "thus the agents in this case were not required to obtain a warrant."



One of the so-called stingray cell phone tracking devices, which impersonates a cell tower.

Civil libertarians are hoping the Rigmaiden case will be the first in the nation to impose privacy limits on how police use stingrays, in much the same way that previous legal challenges have resulted in curbs on warrantless use of thermal imaging devices and GPS tracking of vehicles through physical bugs.

To the American Civil Liberties Union and the Electronic Frontier Foundation, it's a clear case of surveillance technology outpacing the law. They say that "the government's use of the stingray violated the Fourth Amendment." Because stingrays represent a dragnet surveillance technique, capturing not only the target's electronic identifier but that of anyone else in the vicinity, the technique amounts to precisely the type of general search warrant outlawed by the Fourth Amendment, they say.

Another objection they have lodged is that federal agents did ask a judge to permit them to obtain telephone records from Verizon -- but, crucially, did not divulge that a stingray device was going to be used against Rigmaiden.

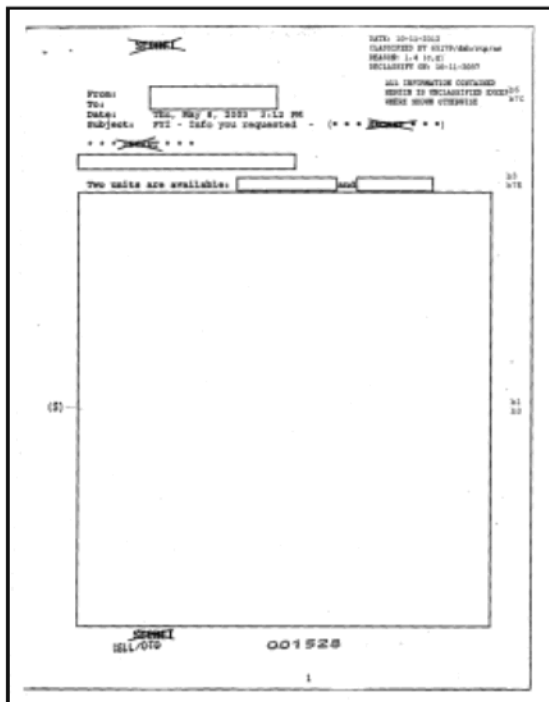
"Had the government candidly told the judge that it intended to use a stingray, he may have denied the application without prejudice to a subsequent application providing further details about the technology," the ACLU and EFF say. That's what happened last summer in Texas, when a federal magistrate judge rejected an effort by the Drug Enforcement Administration to deploy stingrays without obtaining a search warrant backed by probable cause.

Linda Lye, a staff attorney at the ACLU of Northern California who will be arguing in court in Arizona tomorrow, said this morning that there appears to be a pattern of concealment when police use stingray devices.

A newly disclosed email ([PDF](#)) from Miranda Kane, the head of the criminal division for the U.S. Attorney's office in the northern district of California, says (WIT refers to stingray devices):

It has recently come to my attention that many agents are still using WIT technology in the field although the pen register application does not make that explicit. While we continue work on a long term fix for this problem, it is important that we are consistent and forthright in our pen register requests to the magistrates...

Tomorrow's hearing in the case against Rigmaiden, who faces charges including conspiracy, wire fraud, mail fraud, and aggravated identity theft for allegedly filing more than 1,000 bogus tax returns, will center on his request to "suppress" data he contends the government acquired in violation of the Fourth Amendment. If he wins that argument, the so-called exclusionary rule would make evidence derived from unconstitutional surveillance inadmissible in court, but prosecutors could still win a conviction if the remainder of the evidence is sufficient.



The FBI has not disclosed details about its stingray devices. In response to an open records request from the Electronic Privacy Information Center, the bureau declassified this previously SECRET document but completely redacted it. [Click for larger image.](#)

(Credit: FBI)

The Justice Department has taken the unusual position of agreeing in January that the "the aircard location operation was a Fourth Amendment search and seizure." But, prosecutors say, they nevertheless intend to argue that the "defendant has no standing to complain" about any possible Fourth Amendment violations because, in part, he used a pseudonym to obtain the wireless device and rent the apartment: "Defendant's wide-ranging fraudulent and deceptive conduct should not merit an expectation of privacy that society is prepared to recognize as reasonable."

A ruling that the Fourth Amendment requires a warrant before deploying a stingray device would, if upheld on appeal, end the FBI's practice of attempting to obtain them using less privacy-protective procedures intended for recording what numbers were called on an analog telephone line. But it wouldn't halt the use of the devices: Agents could still deploy them using a warrant based on probable cause that a crime is being committed.

Stingrays aren't exactly new technology. A 1996 [Wired article](#) described how an FBI surveillance team from Quantico, Va., used one to track Kevin Mitnick: "It could also be used to page Mitnick's cell phone without ringing it, as long as he had the phone turned on but not in use. The phone would then act as a transmitter that they could home in on with a Triggerfish cellular radio direction-finding system that they were using."

Their use has spread far beyond the FBI and the military, which has long employed direction-finding gear. [LA Weekly reported](#) in January that the [First Amendment Coalition](#) obtained documents showing stingrays were used during routine "criminal investigations 21 times in a four-month period during 2012" by the Los Angeles Police Department. Those included burglary, drug, and murder investigations.


Last month, the Electronic Privacy Information Center obtained stingray documents ([PDF](#)) from the FBI describing procedures for the "loan" of stingray cell site simulators to state and local agencies. A 2009 [government procurement document](#) shows that the U.S. Secret Service paid Harris Corp., which makes stingray devices, over \$25,000 for training. (Harris secured [another](#) Secret Service contract last year.)

A trial in Rigmaiden's criminal case is scheduled to start in Phoenix on May 15.



## **Declan McCullagh**

[Declan McCullagh](#) is the chief political correspondent for CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.

 [Follow @declanm](#)

890 F.Supp.2d 747  
**(Cite as: 890 F.Supp.2d 747)**

**C**

United States District Court,  
 S.D. Texas,  
 Corpus Christi Division.

In the Matter of THE APPLICATION OF THE  
 UNITED STATES of America for AN ORDER  
 AUTHORIZING THE INSTALLATION AND USE  
 OF A PEN REGISTER AND TRAP AND TRACE  
 DEVICE.


C.A. No. C-12-534M.  
 June 2, 2012.

**Background:** Assistant United States Attorney applied for issuance of an order authorizing installation and use of pen register and trap and trace device to detect radio signals emitted from cellular telephones in vicinity of subject.

**Holding:** The District Court, Brian L. Owsley, United States Magistrate Judge, held that equipment required authorization pursuant to a warrant, rather than under pen register statute.

Denied.

West Headnotes

**[1] Telecommunications 372  1475**


372 Telecommunications

372X Interception or Disclosure of Electronic Communications; Electronic Surveillance

372X(B) Authorization by Courts or Public Officers

372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

The pen register and trap and trace device statute mandates that a court have a telephone number or some similar identifier before issuing an order authorizing such devices. 18 U.S.C.A. § 3123.

**[2] Telecommunications 372  1475**

372 Telecommunications

372X Interception or Disclosure of Electronic Communications; Electronic Surveillance

372X(B) Authorization by Courts or Public Officers

372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Equipment designed to capture cell phone numbers of phones within vicinity of subject of criminal investigation required authorization pursuant to a warrant, warranting denial of application pursuant to pen register statute; pen register applications required telephone number or some similar identifier and application did not explain the technology or process by which it would be used to gather subject's cell phone number. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 3123.

***\*748 OPINION DENYING THE APPLICATION FOR A PEN REGISTER AND TRAP AND TRACE DEVICE***

BRIAN L. OWSLEY, United States Magistrate Judge.

This matter comes before the Court pursuant to a written and sworn application pursuant to 18 U.S.C. §§ 3122(a)(1), 3127(5), and 2703(c)(1) by an Assistant United States Attorney who is an attorney for the government as defined by Rule 1(b)(1)(B) of the Federal Rules of Criminal Procedure and an accompanying affidavit of a special agent with the United States Drug Enforcement Agency.

**BACKGROUND**

In the application, the Assistant United States Attorney "certifies that the Drug Enforcement Administration (DEA) is conducting an ongoing criminal investigation regarding violations of federal criminal statutes." Specifically, the investigation focuses on a Subject alleged to be engaged in narcotics trafficking. The application details the investigation spanning several years of the Subject's alleged involvement and notes that at one point the Subject's cell phone number was known, but that the Subject apparently is no longer using that cell phone. Based on information provided by individuals cooperating with the investigation, it is believed that the Subject is using a new cellular telephone.



890 F.Supp.2d 747  
 (Cite as: 890 F.Supp.2d 747)

In the pending application, the Assistant United States Attorney “requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication.” The applicant further explains that “[b]y determining the identifying registration data at various locations in which the [Subject's] Telephone is reasonably believed to be operating, the telephone number corresponding to the [Subject's] Telephone can be identified.”

After reviewing the application, an *ex parte* hearing was conducted with the special agent leading the investigation. He indicated that this equipment designed to capture these cell phone numbers was known as a “**stingray**.” Moreover, the Assistant\*749 United States Attorney explained that the application was based on a standard application model and proposed order approved by the United States Department of Justice. During this hearing, a number of the decisions addressed below were discussed with the Assistant United States Attorney. He was not familiar with these cases, but indicated that he would be able to provide case law to support this application the next day.<sup>FNI</sup>

<sup>FNI</sup>. This memorandum was never provided to the Court.

The application has a number of shortcomings. It does not explain the technology, or the process by which the technology will be used to engage in the electronic surveillance to gather the Subject's cell phone number. For example, there was no discussion as to how many distinct surveillance sites they intend to use, or how long they intend to operate the **stingray** equipment to gather all telephone numbers in the immediate area. It was not explained how close they intend to be to the Subject before using the **stingray** equipment. They did not address what the government would do with the cell phone numbers and other information concerning seemingly innocent cell phone users whose information was recorded by the equipment.

While these various issues were discussed at the

hearing, the government did not have specific answers to these questions. Moreover, neither the special agent nor the Assistant United States Attorney appeared to understand the technology very well. At a minimum, they seemed to have some discomfort in trying to explain it.

#### ANALYSIS

Historically, a pen register was viewed as a device recording the outgoing numbers dialed from a specific telephone number. United States v. Giordano, 416 U.S. 505, 512 n. 2, 94 S.Ct. 1820, 40 L.Ed.2d 341 (1974) (noting that a pen register is “a device that records telephone numbers dialed from a particular phone” ) (emphasis added); United States v. New York Telephone Co., 434 U.S. 159, 161 n. 1, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977) (“A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.”).

In 2001, Congress amended the definition of the term “pen register” as part of the USA PATRIOT Act. See In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F.Supp.2d 448, 455 (S.D.N.Y.2006). In that statute, Congress redefined a “pen register” as

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 purposes in the ordinary course of its business.

18 U.S.C. § 3127(3); accord \*750In re United States, 622 F.Supp.2d 411, 414 (S.D.Tex.2007) . Additionally, a trap and trace device is defined as

890 F.Supp.2d 747

(Cite as: 890 F.Supp.2d 747)

a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

18 U.S.C. § 3127(4); accord *In re United States*, 622 F.Supp.2d at 414. Congress further mandated the information that a court needs to grant such an application based on what is required to be in the court order authorizing the pen register and trap and trace device

(b) Contents of order—an order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied,....

18 U.S.C. § 3123(b)(1) (emphasis added).

With the PATRIOT Act, the definition of a pen register was broadened. *In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F.Supp.2d at 455. Nonetheless, courts still have determined that pen register applications seek information about a particular telephone. See, e.g., *United States v. Jadowe*, 628 F.3d 1, 6 n. 4 (1st Cir.2010) (“A ‘pen register’ is a device used, inter alia, to record the dialing and other information transmitted by a targeted phone.”); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d 747, 752

(S.D.Tex.2005) (“A ‘pen register’ is a device that records the numbers dialed for outgoing calls made from the target phone.”); *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers*, 402 F.Supp.2d 597, 602 (D.Md.2005) (“pen register records telephone numbers dialed for outgoing calls from the target phone”); *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F.Supp.2d 435, 438 (S.D.N.Y.2005) (“Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a particular telephone”); *In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information*, 515 F.Supp.2d 325, 328 (E.D.N.Y.2007) (“In layman's terms, a pen register is a device capable of recording all digits dialed from a particular phone.”); *United States v. Bermudez*, No. 05-43-CR, 2006 WL 3197181, at \*8 (S.D.Ind. June 30, 2006) (unpublished) (“A ‘pen register’ records telephone numbers dialed for outgoing calls made from the target phone.”). Similarly, a trap and trace device after the Patriot Act still seeks information about a particular phone. See, e.g., \*751 *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers*, 402 F.Supp.2d at 602 (“trap/trace device ... records the telephone numbers of those calling the target phone”); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d at 752 (“A trap and trace device captures the numbers of calls made to the target phone.”); *Bermudez*, 2006 WL 3197181, at \*8 (“a trap/trace device records the telephone numbers of those calling the target phone”).

This approach is consistent with the current version of § 3123. Thus, a court is required to list in any order the identity of the person who is the cell phone subscriber, but only if that identity is known. See 18 U.S.C. § 3123(b)(1)(A). Additionally, the court is also required to include the name of the criminal investigation's subject, but again only if that identity is known. See 18 U.S.C. § 3123(b)(1)(B). However, regarding the telephone number or other

890 F.Supp.2d 747

(Cite as: 890 F.Supp.2d 747)

such identifier, Congress mandated explicitly that information be included within the court order. See 18 U.S.C. § 3123(b)(1)(C).<sup>FN2</sup> The Patriot Act's revised definition of a pen register and trap and trace device in § 3127 simply amplifies the various types of information that are available such as routing and signaling information. See *Jadowe*, 628 F.3d at 6 n. 4; *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F.Supp.2d at 438–39; see also *In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F.Supp.2d at 454 (noting that pen registers and trap and trace devices apply to particular cell phones and provide additional information such as cell site information); *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register Device*, 497 F.Supp.2d 301, 306 (D.P.R.2007) (“the term ‘signaling information’ under 18 U.S.C. § 3127(3) and (4) encompasses cell site information”).

<sup>FN2</sup>. These specific identifiers include, *inter alia*, the Electronic Serial Number, the International Mobile Equipment Identity, the Mobile Equipment Identifier, or the Urban Fleet Mobile Identifier, which are addressed in both the application and the proposed order.

[1] The language of § 3123(b)(1) is straightforward in that a telephone number or similar identifier is necessary for a pen register. The Supreme Court has explained that “in all statutory construction cases, we begin with ‘the language itself [and] the specific context in which that language is used.’” *McNeill v. United States*, — U.S. —, 131 S.Ct. 2218, 2221, 180 L.Ed.2d 35 (2011) (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341, 117 S.Ct. 843, 136 L.Ed.2d 808 (1997)). Moreover, courts are to “look first to the word's ordinary meaning” when interpreting a statute. *Schindler Elevator Corp. v. United States ex rel. Kirk*, — U.S. —, 131 S.Ct. 1885, 1891, 179 L.Ed.2d 825 (2011) (citing *Gross v. FBL Fin. Servs., Inc.*, 557 U.S. 167, 175, 129 S.Ct. 2343, 174 L.Ed.2d 119 (2009)); accord *Wall v. Kholi*, — U.S. —, 131 S.Ct. 1278, 179 L.Ed.2d 252 (2011) (citing *Williams v. Taylor*, 529 U.S. 420, 431, 120 S.Ct. 1479, 146 L.Ed.2d 435

(2000)). Here, the plain language of the statute mandates that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register. The government has not provided any support to the contrary that the pen register statute should be interpreted in this manner.

The special agent leading the investigation referred to the equipment that the government proposes to use as a **stingray**. Other names for this equipment include \*752 triggerfish, cell site simulator, and digital analyzer. Regardless of what it is called, there is scant case law addressing the equipment.

In a decision issued prior to the Patriot Act, one court defined a “digital analyzer” as “a portable device that can detect signals emitted by a cellular telephone ... [including] the electronic serial number (“ESN”) assigned to a particular cellular telephone, the telephone of the cellular telephone itself, and the telephone numbers called by the cellular telephone.” *In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. 197, 198 (C.D.Cal.1995); see also *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d 747, 755 (S.D.Tex.2005) (defining a triggerfish as equipment that “enables law enforcement to gather cell site data directly, without the assistance of the service provider”).

[2] In *United States v. Rigmaiden*, 844 F.Supp.2d 982 (D.Ariz.2012), the defendant was a fugitive who was charged with identity theft and mail and wire fraud. *Id.* at 987–88. “The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetuate the fraudulent scheme.” *Id.* The defendant was seeking extensive discovery based on his allegations “that the technology and methods used to locate the aircard violated his Fourth Amendment rights.” *Id.* In that investigation, the law enforcement officers had both a pen register and trap and trace device as well as a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a mobile tracking device. That court found that “[t]he mobile tracking device used by the FBI to locate the aircard functions as a cell site simulator. The mobile tracking device

890 F.Supp.2d 747  
(Cite as: 890 F.Supp.2d 747)

mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard.” *Id.* at 995; *see also* 18 U.S.C. § 3117 (addressing mobile tracking devices). Moreover, that “mobile tracking device used to simulate a Verizon cell tower is physically separate from the pen register trap and trace device used to collect information from Verizon.” *Rigmaiden*, 844 F.Supp.2d at 995. Finally, the government asserted that “for purposes of Defendant’s motion to suppress, ... the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.” *Id.*

Thus, *Rigmaiden* provides several salient points for the analysis here. The use of what was termed a cell site simulator was deemed a mobile tracking device. The government indicated that this cell site simulator was authorized pursuant to the warrant for the mobile tracking device as opposed to any pen register and trap and trace device. Finally, in that case, the government acknowledged that the proper analysis had to be pursuant to Fourth Amendment search and seizure jurisprudence.

Here, the application seeks an order authorizing the use of this equipment as a pen register as opposed to seeking a warrant. The government has not provided any support that the pen register statute applies to **stingray** equipment. Based on the statutory language and the limited case law analyzing this issue, a pen register does not apply to this type of electronic surveillance.

#### CONCLUSION

Accordingly, the government’s application for a pen register and trap and trace device is hereby denied without prejudice.

S.D.Tex.,2012.

In re the Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device  
890 F.Supp.2d 747

END OF DOCUMENT



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](http://www.dhs.gov/privacy), on DHSCconnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto: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

<b>Project or Program Name:</b>	<b>Cell Site Simulator Technology and Log</b>
(b)(6); (b)(7)(C); (b)(7)(E)	

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

## SPECIFIC PTA QUESTIONS

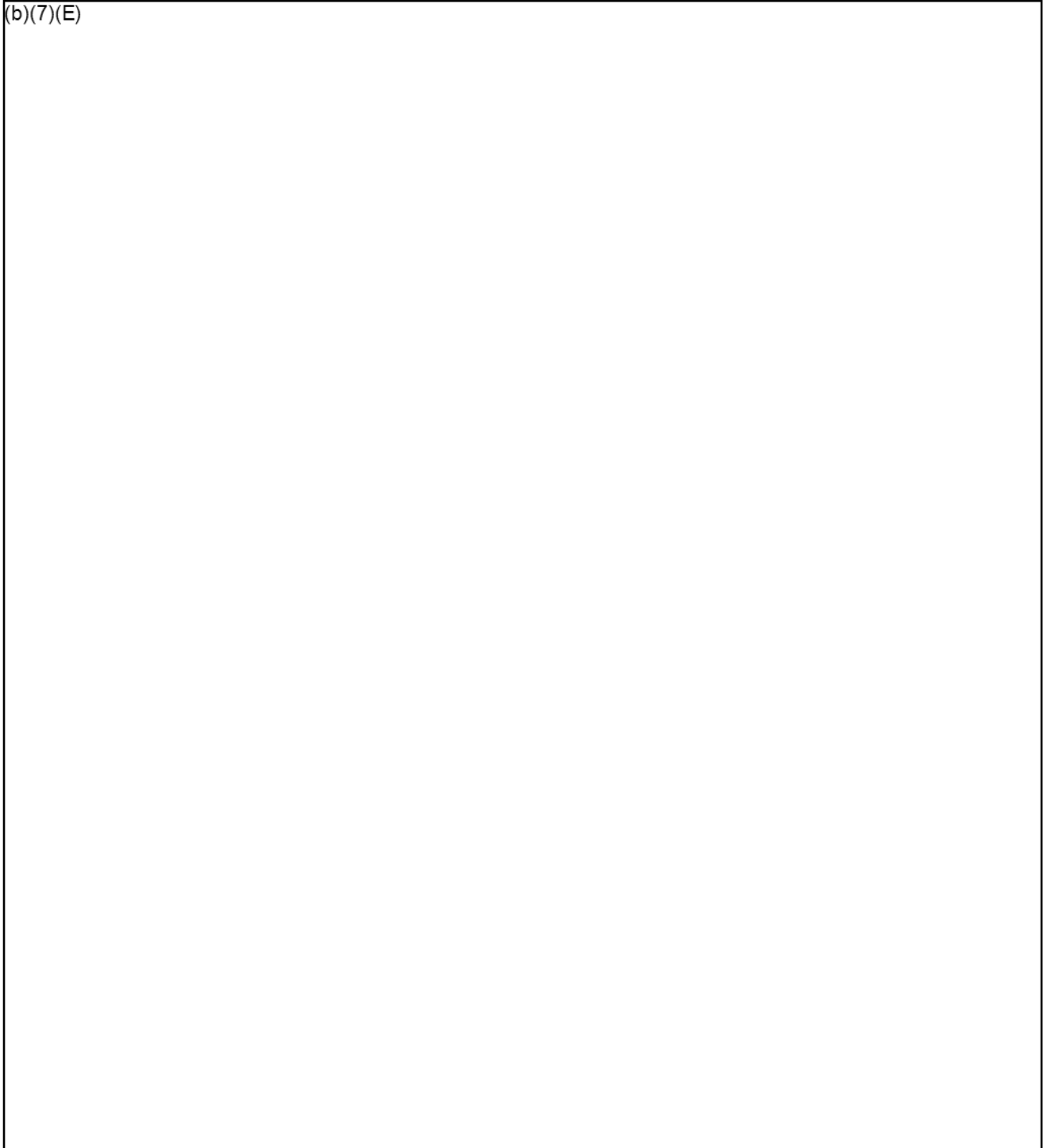
(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE





LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

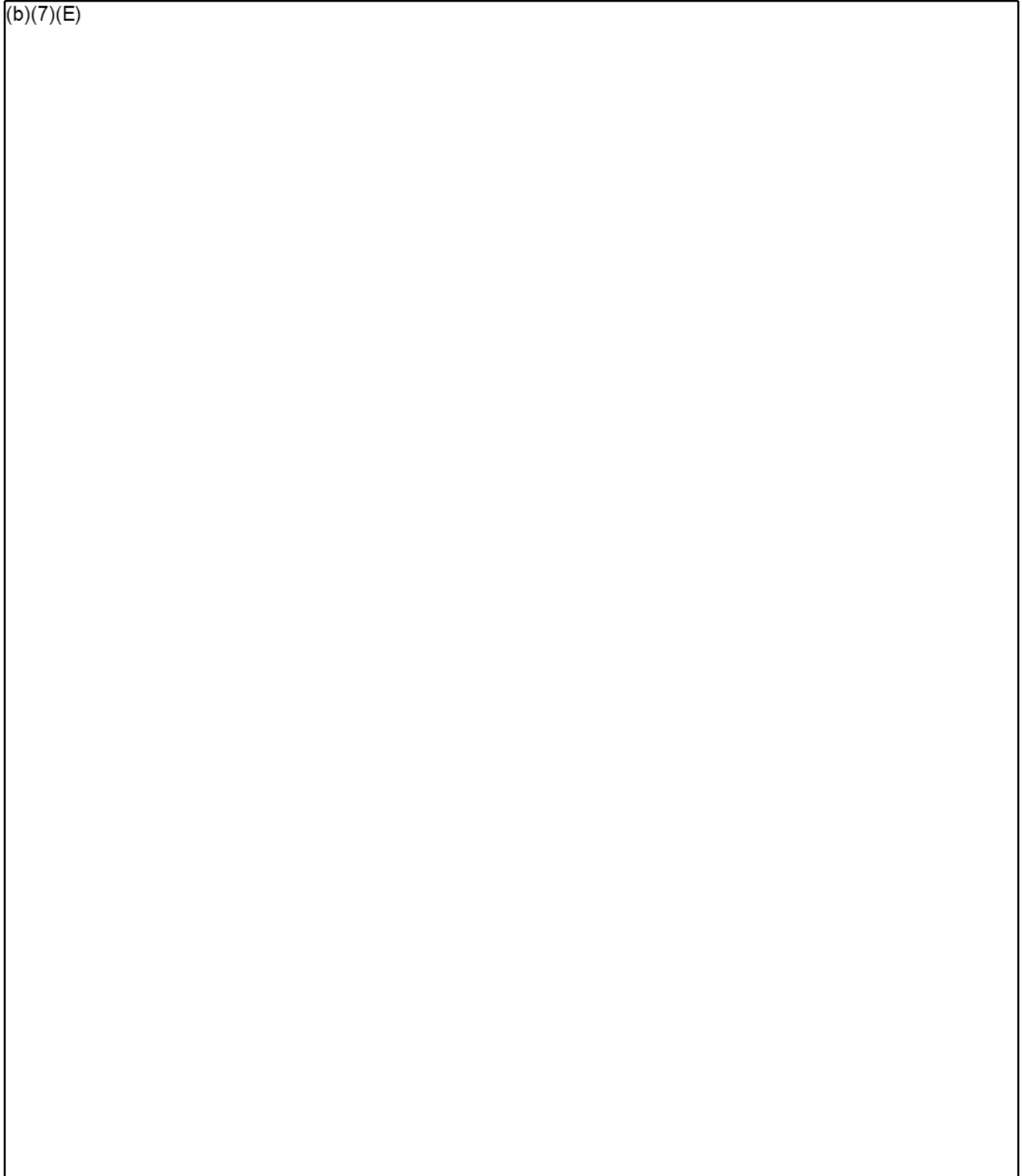
(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

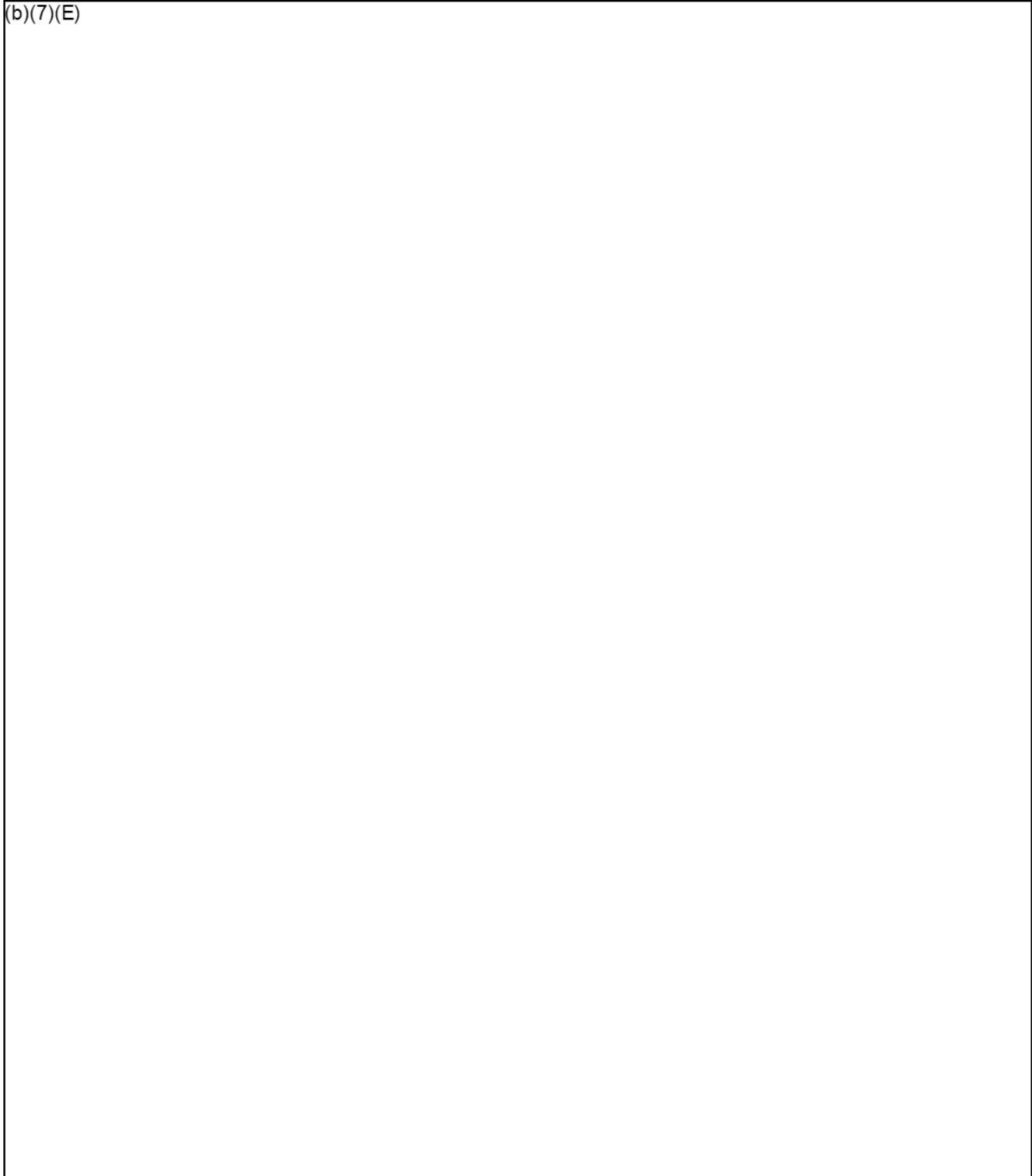


LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(6); (b)(7)(C); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 10 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

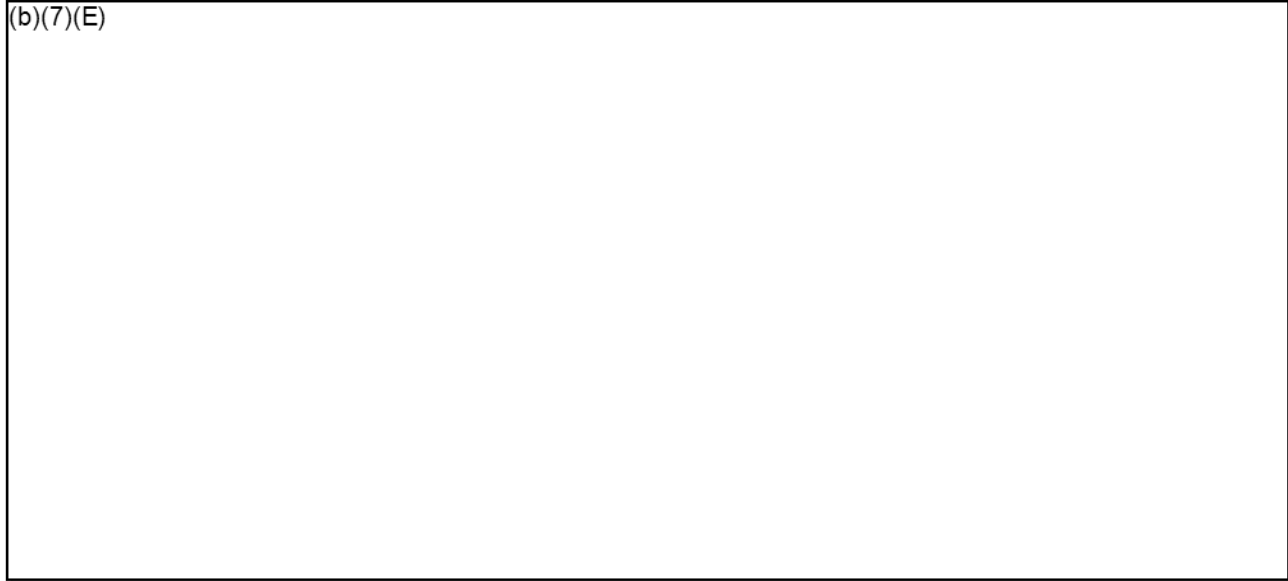
LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1018



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

**From:** (b)(6);  
**Sent:** 31 Jan 2019 17:12:28 +0000  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** PTAs to Assign

Good afternoon,

I met with (b)(6) earlier today to review PTAs that are still pending with her in POTS. (b)(6); last day with ICE is tomorrow, so I will be re-assigning a total of 5 PTAs. Below, I've listed who I would like to take on each PTA. I also indicated the status of the assignment, the POTS matter number, and the shared drive location. Please let me know if you have any questions, or if this would make your workload too daunting.

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

Please feel free to stop by with questions.

(b)(6); (b)(7)(C) **J.D., CIPP/US/G**  
Deputy Privacy Officer  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Desk: 202-732-(b)(6);  
Mobile: 202-701-(b)(6);  
Main: 202-732-(b)(6);  
(b)(7)(C)



Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx>

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** 21 Feb 2019 19:43:45 +0000  
**To:** (b)(6);  
**Subject:** Cell Site Simulator PTA  
**Attachments:** PTA ICE HSI Cell Site Simulator and Log (02 21 2019).docx

Hi (b)(6);  
(b)(7)(C)

I've reviewed the Cell Site Simulator PTA and made updates. It looks like you had included questions for the program. Please take a look to see whether your questions have been answered sufficiently. Also, given my updates, please let me know if you have additional questions or comments.

Thank you!

Best,

(b)(6);

(b)(6);

Supporting the Office of Information Governance & Privacy  
U.S Immigration and Customs Enforcement

(b)(6); @associates.ice.dhs.gov

(Mobile) (b)(6);



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](http://www.dhs.gov/privacy), on DHSCconnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 2 of 12*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1024



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

### **SPECIFIC PTA QUESTIONS**

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



# Homeland Security

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 4 of 12*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(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)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis  
Version number: 01-2014**

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE





# Homeland Security

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 7 of 12*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



# Homeland Security

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 8 of 12*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



# Homeland Security

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 9 of 12*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



# Homeland Security

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 10 of 12*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 12 of 12*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1034

**From:** (b)(6); (b)(7)(C)  
**Sent:** 8 Sep 2017 23:18:11 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)@dhs.gov'  
**Subject:** Cellebrite Forensics Training  
**Attachments:** IGP Comprehensive Contract Clause FINAL (07 25 2017).docx

(b)(6);

ICE Privacy approves your procurement request for Cellebrite Forensics Training as long as the attached Information Governance & Privacy Requirements Clause is included in its entirety in both the Request for Proposal and in the terms and conditions in the final contract.

Thanks,

(b)(6);  
(b)(7)(C)

(b)(6); (b)(7)(C)

Deputy Privacy Officer  
U.S. Immigration and Customs Enforcement  
Phone: 202.732.(b)(6);  
Mobile: 202.89.(b)(7)(C)  
(b)(6);@ice.dhs.gov

---

## Information Governance and Privacy (IGP) Acquisition Review

**Project Name:** Cellebrite Forensics Training

**Contract Number:**

**IGP Reviewer:** (b)(6); (b)(7)(C)

**Date:** 9/8/17

**POTS Ref:** 17-11392

---

**IGP Summary:** (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

---

**The attached Information Governance & Privacy Requirements Clause must be included in its entirety in both the Request for Proposal and in the terms and conditions in the final contract.**

Please contact the IGP Privacy Division (b)(6); [redacted]@ice.dhs.gov) or (b)(6); (b)(7)(C); [redacted] Acting Chief of Staff for OAQ (b)(6); (b)(7)(C); [redacted]@ice.dhs.gov) with any questions.



## **ICE Information Governance and Privacy Requirements Clause (JUL 2017)**

**Guidance:** In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following IGP clause must be included in its entirety in all contracts. No section of this clause may be read as self-deleting unless the terms of the contract meet the requirements for self-deletion as specified in this clause.

### **A. Limiting Access to Privacy Act and Other Sensitive Information**

#### *(1) Privacy Act Information*

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974 the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at [www.dhs.gov/privacy](http://www.dhs.gov/privacy). Applicable SORNs of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at <http://www.gpo.gov/fdsys/>. SORNs may be updated at any time.

#### *(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment*

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

#### *(3) Prior Approval Required to Hire Subcontractors*

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

#### *(4) Separation Checklist for Contractor Employees*

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

## **B. Privacy Training, Safeguarding, and Remediation**

*If the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses are included in this contract, section B of this clause is deemed self-deleting.*

### *(1) Required Security and Privacy Training for Contractors*

Contractor shall provide training for all employees, including Subcontractors and independent contractors who have access to sensitive personally identifiable information (PII) as well as the creation, use, dissemination and/or destruction of sensitive PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle sensitive PII, including security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of sensitive PII. All Contractor employees are required to take the *Privacy at DHS: Protecting Personal Information* training course. This course, along with more information about DHS security and training requirements for Contractors, is available at [www.dhs.gov/dhs-security-and-training-requirements-contractors](http://www.dhs.gov/dhs-security-and-training-requirements-contractors). The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information to take the annual Information Assurance Awareness Training course. These courses are available through the ICE intranet site or the Agency may also make the training available through hypertext links or CD. The Contractor shall maintain copies of employees' certificates of completion as a record of compliance and must submit an annual e-mail notification to the ICE Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

### *(2) Safeguarding Sensitive PII Requirement*

Contractor employees shall comply with the Handbook for Safeguarding sensitive PII at DHS at all times when handling sensitive PII, including the encryption of sensitive PII as required in the Handbook. This requirement will be flowed down to all subcontracts and lower tiered subcontracts as well.

### *(3) Non-Disclosure Agreement Requirement*

All Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (DHS Form 11000-6) prior to commencing work. The Contractor shall maintain signed copies of the NDA for all employees as a record of

compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

*(4) Prohibition on Use of PII in Vendor Billing and Administrative Records*

The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII that is created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the Contracting Officer, Contracting Officer's Representative, or other ICE personnel associated with the administration of the contract in the invoices as needed.

*(5) Reporting Suspected Loss of Sensitive PII*

Contractors must report the suspected loss or compromise of sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of sensitive PII.
2. The Contractor must report the suspected loss or compromise of sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-6627), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.
3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of sensitive PII by its employees or Subcontractors. The report must contain the following information:
  - a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
  - b. Date, time, and location of the incident.
  - c. Type of information lost or compromised.
  - d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
  - e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
  - f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
  - g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
  - h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.
4. The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all

requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access sensitive PII or to work on that contract based on their actions related to the loss or compromise of sensitive PII.

*(6) Victim Remediation*

The Contractor is responsible for notifying victims and providing victim remediation services in the event of a loss or compromise of sensitive PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.

### **C. Government Records Training, Ownership, and Management**

*(1) Records Management Training and Compliance*

(a) The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to sensitive PII as well as to those involved in the creation, use, dissemination and/or destruction of sensitive PII. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site or it may be made available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance and must submit an e-mail notification annually to the Contracting Officer's Representative verifying that all employees working under this contract have completed the required records management training.

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

*(2) Records Creation, Ownership, and Disposition*

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency data. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases)

and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

#### **D. Data Privacy and Oversight**

*Section D applies to information technology (IT) contracts. If this is not an IT contract, section D may read as self-deleting.*

##### *(1) Restrictions on Testing or Training Using Real Data Containing PII*

The use of real data containing sensitive PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible. ICE policy requires that any proposal to use of real data or de-identified data for IT system testing or training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing or training purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

*If this IT contract contains the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses, section D(2) of this clause is deemed self-deleting.*

##### *(2) Requirements for Contractor IT Systems Hosting Government Data*

The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

##### *(3) Requirement to Support Privacy Compliance*

(a) The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA)

and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide adequate support to complete the PIA in a timely manner, and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website ([www.dhs.gov/privacy](http://www.dhs.gov/privacy)) under “Compliance.” DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under “Key Personnel.” The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Office, the Office of the Chief Information Officer, and the Records Management Branch to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion. The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

(c) If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required.

The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion.

(End of Clause)

EW  
JH

# United States Senate

WASHINGTON, DC 20510

December 9, 2014

SCANNED/RECEIVED  
BY EXEC SEC  
2014 DEC 18 PM 12: 27

The Honorable Eric H. Holder, Jr.  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Avenue NW  
Washington, DC 20530

The Honorable Jeh Johnson  
Secretary of Homeland Security  
Department of Homeland Security  
Washington, D.C. 20528

Dear Attorney General Holder and Secretary Johnson,

We are writing to express our concern about recent news reports revealing that the U.S. Marshals Service is flying airplanes over the United States equipped with surveillance devices that transmit electronic signals into the homes of thousands of Americans in order to locate individuals via their mobile phones. These International Mobile Subscriber Identity Catcher surveillance devices (IMSI-catcher), commonly known as “DRTBoxes,” “dirtboxes” or “Stingrays,” simulate legitimate cell phone towers, thus compelling all nearby phones to identify themselves. As a result, agencies that use these devices collect the information of thousands of Americans, potentially infringing on the Fourth Amendment and disrupting normal cell phone usage.

The U.S. Marshals Service is apparently not the only agency using these devices from the air—it has come to our attention that other agencies with the Department of Justice (DOJ), including the Drug Enforcement Administration (DEA), as well as the Department of Homeland Security (DHS), more specifically Immigration and Customs Enforcement (ICE), are also using airborne IMSI-catchers.

Whether used on an automobile or plane, these devices potentially violate the Fourth Amendment and represent a significant intrusion into the private lives of thousands of Americans. While we all want law enforcement agencies to use cutting-edge tools to catch criminals and protect our borders, Americans should not have to sacrifice their privacy rights in the process. Furthermore, given the extreme lengths to which federal agencies have gone to keep surveillance technologies like this a secret,<sup>1</sup> it is vital that their use be subject to strict oversight by the courts and Congress.

---

<sup>1</sup> See Martin Kaste, *Should Police Be Able To Keep Their Devices Secret?*, NPR, October 22, 2014, *available at* <http://www.npr.org/2014/10/22/358120429/should-police-be-able-to-keep-their-devices-secret>. See also Kim Zetter, *Florida Cops' Secret Weapon: Warrantless Cellphone Tracking*, *Wired*, March 3, 2014, *available at* <http://www.wired.com/2014/03/stingray/>.

We would like to know if your departments, or its components, utilize these devices along the borders and in our states. Accordingly, we request the following information:

1. To what extent does your department use IMSI-catchers (Stingrays, DRTboxes, etc.) or other similar technology? Specifically:
  - a. Which components within your department use such devices? If multiple components use such devices, is there department-wide guidance governing their use?
  - b. Since FY 2010, how many times has such technology been deployed, and how many phones were identified or tracked by this technology, including devices used by the targets of the operation as well as non-targets whose information was incidentally swept up?
  - c. In what types of operations are these devices deployed?
  - d. What statutory authority permits the use of this surveillance technology?
  - e. Do DHS and/or DOJ obtain a court order prior to using such devices? If so, do DHS and/or DOJ inform the courts of the number of individuals likely to be impacted; the scope of acquisition; or the specific technology being deployed?
2. Did the DOJ Office of Privacy and Civil Liberties, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties review and/or conduct a privacy impact assessment or other review regarding the use of these technologies prior to deployment? If so, please provide copies of such reviews or assessments.
3. To what extent is your department coordinating or providing assistance to other federal agencies in order to help them purchase or otherwise obtain this type of technology?
4. The Federal Communication Commission requires that “state and local law enforcement agencies must coordinate with the Federal Bureau of Investigation (FBI) ... prior to the acquisition and use of the [IMSI-catchers or other similar] equipment/technology.”<sup>2</sup> What does the FBI require of departments and agencies as part of this coordination process?
5. To what extent does your department provide assistance to state and local agencies in order to help them purchase or otherwise obtain this type of technology?
  - a. To the extent that these devices have been purchased through DHS and DOJ grant programs, how much federal money has been used to purchase them? What, if any, limitations or requirements are imposed on agencies that receive and use federal grant money to acquire this type of surveillance technology?

---

<sup>2</sup> Muckrock, FCC and FBI disagree over NDA requirement for police StingRays, October 8, 2014, <https://www.beaconreader.com/muckrock/fcc-claims-nondisclosure-agreement-not-required-for-police-to-use-stingrays>.




- b. What training and conditions are given to state and local agencies who receive this technology, as it relates to protecting innocent Americans' privacy?
  - c. How many times have DHS and/or DOJ loaned or otherwise permitted the use of such devices by state or local agencies?
6. Public documents reveal that the DEA has acquired airborne IMSI-catchers for use along the southwestern border.<sup>3</sup> Is this technology also being utilized by the DEA or other DOJ office along the Northern Border? How many miles inland from both borders is this technology being deployed?
7. Does DHS also deploy this or similar technology along northern and/or southern borders? If so, in what areas? What legal authority is your agency using to conduct flights whilst using such devices?
8. Are operations conducted within existing high-crime designated areas (i.e. High Intensity Drug Trafficking Area)?
9. What policies and guidance govern the use, retention, and dissemination of information collected by these devices? Specifically:
  - a. What information is collected using these devices? How is the acquired information stored?
  - b. When are department personnel permitted to search through information acquired by these devices?
  - c. How long is the collected information retained? How is this information disposed of, and what timeframe is your agency using to dispose of information collected by such devices?
  - d. When is this information shared with other federal, state, or local agencies, or international partners? How much is information shared with other federal agencies, how often is information shared, and to which agencies?
  - e. Is information collected used in criminal prosecutions or immigration proceedings? If so, does DHS or DOJ have a policy in place requiring that defendants be notified of how such information was collected so they may raise relevant legal challenges?
10. Do DHS and/or DOJ have policies in place requiring that individuals who are not targets be informed when their information is inadvertently collected, reviewed, or retained?
11. What efforts are made to ascertain and minimize civilian interference?

---

<sup>3</sup> See "Prime Award Spending Data," available at [http://www.usaspending.gov/explore?fiscal\\_year=all&comingfrom=searchresults&piid=DJD14HQP0798&typeofview=complete](http://www.usaspending.gov/explore?fiscal_year=all&comingfrom=searchresults&piid=DJD14HQP0798&typeofview=complete)

Thank you for your attention to this important matter. We look forward to your response.

Sincerely,



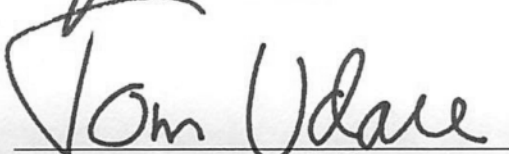
---

Senator Jon Tester



---

Senator Bernard Sanders



---

Senator Tom Udall




---

Senator Christopher Coons



---

Senator Mark Begich



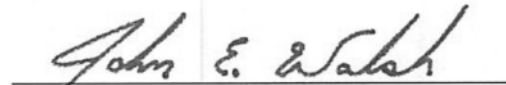
---

Senator Tammy Baldwin



---

Senator Al Franken



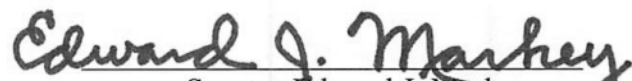
---

Senator John Walsh



---

Senator Jeff Merkley



---

Senator Edward J. Markey



---

Senator Martin Heinrich

United States Senate

WASHINGTON, DC 20510

CAPITOL DISTRICT 208

30 DEC 2014 PM 6 L



485

DEC 16 2014

The Honorable Jeh Johnson  
Secretary of Homeland Security  
Department of Homeland Security  
Washington, D.C. 20528

✓ #040

202010013 1047



**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Feb 2015 23:13:48 -0500  
**To:** (b)(6); (b)(7)(C)  
**Subject:** WP story stingray

Secrecy around spy device is case's undoing  
An FBI-imposed gag order about the StingRay, a sophisticated surveillance device that mimics cell towers, endangers some criminal cases when its use is questioned by defendants or judges.  
<http://wapo.st/1CZT8mG>

-----

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** 29 May 2019 18:47:04 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:** PIA; (b)(6); (b)(7)(C) (CTR)  
**Subject:** Cell Site Simulator and Log PTA  
**Attachments:** Cell Site Simulator and Log PTA (to DHS Privacy 05 29 19).docx

Hello (b)(6);

Attached please find the Cell Site Simulator and Log PTA for DHS Privacy review and adjudication.

Best,

(b)(6);  
(b)(7)(C)

Supporting the Office of Information Governance & Privacy  
U.S. Immigration and Customs Enforcement

(b)(6); (b)(7)(C)  
(Mobile) 571-230 (b)(6)

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** 19 Jun 2019 20:43:37 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell Site Simulator and Log PTA  
**Attachments:** Cell Site Simulator and Log PTA (to DHS Privacy 05 29 19).docx

Hi (b)(6);

I took a look at the PTA (b)(6) had submitted. Before HSI uses the technology, they obtain court orders or search warrants (depending on the judicial district) through the appropriate United States Attorneys' Offices which authorize the use of this technology.

In the Carpenter case, the Supreme Court ruled that a "warrant is required for police to access cell site location information from a cell phone company—the detailed geolocation information generated by a cellphone's communication with cell towers." <https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states>.

Please let me know if you have any additional information in response to (b)(6); (b)(7)(C) question.

Thanks,

(b)(6);  
(b)(7)(C)

---

**From:** (b)(6); (b)(7)(C) >  
**Sent:** Wednesday, June 19, 2019 4:05 PM  
**To:** (b)(6); (b)(7)(C) >  
**Cc:** PIA (b)(6); (b)(7)(C) (CTR)  
(b)(6); (b)(7)(C) >  
**Subject:** RE: Cell Site Simulator and Log PTA

Good afternoon,

Has there been a legal analysis of this activity in light of the Carpenter case? It affects cell site simulator activity, so I wanted to make sure that this had been reviewed for legal sufficiency.

Respectfully,

(b)(6); (b)(7)(C)

Privacy Analyst  
DHS Privacy Office

Desk: (202) 343-(b)(6);

Cell: (202) 503-(b)(6);

Email: (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C) >  
**Sent:** Wednesday, May 29, 2019 2:47 PM

To: (b)(6); (b)(7)(C)  
Cc: PIA (b)(6); (b)(7)(C) (CTR)  
<(b)(6); (b)(7)(C)>  
**Subject:** Cell Site Simulator and Log PTA

Hello (b)(6);

Attached please find the Cell Site Simulator and Log PTA for DHS Privacy review and adjudication.

Best,

(b)(6);  
(b)(7)(C)

Supporting the Office of Information Governance & Privacy  
U.S. Immigration and Customs Enforcement

(b)(6); (b)(7)(C)  
(Mobile) 571-230-(b)(6);

**From:** (b)(6); (b)(7)(C)  
**Sent:** 18 Jul 2019 15:32:52 +0000  
**To:** (b)(6); (b)(7)(C) CTR  
**Cc:** PIA (b)(6); (b)(7)(C)  
**Subject:** RE: Cell Site Simulator and Log PTA  
**Attachments:** PTA, ICE - Cell Site Simulator and Log, 20190718, PRIV Final.pdf

Good morning,

I have attached the adjudication of the Cell Site Simulator and Log PTA. I agree coverage will be provided by the new ICE Surveillance Technologies PIA.

Respectfully,

(b)(6); (b)(7)(C)  
Privacy Analyst  
DHS Privacy Office  
Desk: (202) 343-(b)(6);  
Cell: (202) 503-(b)(6);  
Email: (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, June 20, 2019 9:42 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** PIA <(b)(6); (b)(7)(C)>  
**Subject:** RE: Cell Site Simulator and Log PTA

Good morning (b)(6);

Thank you for the email. Before HSI uses the Cell Site Simulator technology, they receive supervisory permission to obtain court orders or search warrants (depending on the judicial district) through the appropriate United States Attorneys' Offices, which fulfils the Supreme Court ruling in the Carpenter case, that a warrant is required for police to access cell site location information from a cell phone company.

As such, we will like to proceed with adjudication. Please let me know if you have additional questions.

Thanks again,

(b)(6); (b)(7)(C) MPH, CPH, CIPP/G  
Privacy Analyst  
Office of Information Governance and Privacy (IGP)  
U.S. Immigration and Customs Enforcement (ICE)  
Office: 202-87-(b)(6);  
Mobile: 240-421-(b)(6);  
Email: (b)(6); (b)(7)(C)  
Privacy Mailbox: (b)(6); (b)(7)(C)

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx>



---

**From:** (b)(6); (b)(7)(C) }  
**Sent:** Wednesday, June 19, 2019 4:05 PM  
**To:** (b)(6); (b)(7)(C) }  
**Cc:** PIA (b)(6); (b)(7)(C) (CTR)  
(b)(6); (b)(7)(C) }  
**Subject:** RE: Cell Site Simulator and Log PTA

Good afternoon,

Has there been a legal analysis of this activity in light of the Carpenter case? It affects cell site simulator activity, so I wanted to make sure that this had been reviewed for legal sufficiency.

Respectfully,

(b)(6); (b)(7)(C)

Privacy Analyst

DHS Privacy Office

Desk: (202) 343-(b)(6);

Cell: (202) 503-(b)(6);

Email: (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C) (CTR) (b)(6); (b)(7)(C) }  
**Sent:** Wednesday, May 29, 2019 2:47 PM  
**To:** (b)(6); (b)(7)(C) }  
**Cc:** PIA (b)(6); (b)(7)(C) (CTR)  
(b)(6); (b)(7)(C) }  
**Subject:** Cell Site Simulator and Log PTA

Hello (b)(6); (b)(7)(C)

Attached please find the Cell Site Simulator and Log PTA for DHS Privacy review and adjudication.

Best,

(b)(6);  
(b)(7)(C)

Supporting the Office of Information Governance & Privacy

U.S. Immigration and Customs Enforcement

(b)(6); (b)(7)(C)

(Mobile) 571-230-(b)(6);



# Homeland Security

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 1 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1054



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 2 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1055



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

## SPECIFIC PTA QUESTIONS

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 6 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1059



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 7 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1060





LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 9 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1062



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 10 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1063



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 11 of 11*

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1064

**From:** (b)(6); (b)(7)(C)  
**Sent:** 17 Jul 2017 13:59:09 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Folder (b)(7)(C) (Cell Site Simulator (b)(6); (b)(7)(C) response)

Hi (b)(6);

Will do.

(b)(6);

Privacy Compliance Specialist  
Information Governance and Privacy (IGP)  
U.S. Immigration & Customs Enforcement  
Direct: (202) 732-(b)(6)  
Main: (202) 732-3

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, July 17, 2017 9:59 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Folder (b)(7)(C) (Cell Site Simulator (b)(6); (b)(7)(C) response)

Hi (b)(6);

Can you please make a POTS matter for this OESIMS tasker that Lvn completed? In the summary section, please add the path to the shared drive: (b)(7)(E) (b)(7)(E) and the following key words: stingray technology; cell site simulators; over the air tracking technology.

Thanks,

(b)(6); (b)(7)(C)

(A) Chief of Staff  
Senior Advisor for Information Sharing  
Office of Information Governance & Privacy  
U.S. Immigration and Customs Enforcement  
Department of Homeland Security  
500 12<sup>th</sup> St. SW, Mail Stop 5004, Washington DC 20536

(b)(6); (b)(7)(C) @ice.dhs.gov | Phone 202.732 (b)(6);

For help with IGP questions, visit our website on the ICE Intranet: <https://insight.ice.dhs.gov/mgt/ooop/>

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, July 06, 2017 2:48 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Folder (b)(7)(C) (Cell Site Simulator (b)(6); (b)(7)(C) response)

(b)(6); here's the response I uploaded – can you ensure this gets added to POTS please. I've saved relevant materials to the shared drive folder already.

Task response for IGP:

Please see my suggested edits to bring this response in line with ICE's response to Senator Tester's letter on cell-site simulators in 2015. I've uploaded the Tester response as background.

Please re-clear through HSI. I spoke to Acting Deputy EAD (b)(6); by phone about this letter and my suggestions for changes.

(b)(6); (b)(7)(C) AD for IGP, (b)(6); (b)(7)(C)

(b)(7)(E)

(b)(6);

**Assistant Director for Information Governance & Privacy**

**U.S. Immigration & Customs Enforcement**

**Direct: (202) 734-(b)(6);**

**Main: (202) 734-(b)(6);**

Questions? Please visit the Information Governance & Privacy Office website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** 11 Dec 2018 19:27:51 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Cell Site Simulator (CSS) PTA - Walk through (this updates the Over the Air PTA)  
**Attachments:** PTA ICE HSI Cell Site Simulator and Log 20181211 Final Draft CF to Jordan.docx, PTA, ICE - Over The Air Tracking Technology - LES, 20150403, PRIV FINAL.PDF

(b)(6);

(b)(5); (b)(7)(E)

(b)(6);

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, December 10, 2018 2:50 PM

**To:** (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6);

(b)(6); @ice.dhs.gov>

**Cc:** (b)(6); (b)(7)(C) (CTR); (b)(6); @associates.ice.dhs.gov; (b)(6); (b)(7)(C) (CTR)

(b)(6); (b)(7)(C) @associates.ice.dhs.gov; (b)(6); (b)(7)(C) (CTR)

(b)(6); (b)(7)(C) @associates.ice.dhs.gov>

**Subject:** RE: Cell Site Simulator (CSS) PTA - Walk through (this updates the Over the Air PTA)

This is great (b)(6); I will clean it up and submit it up to our Privacy Officer.

Thanks!

(b)(6);

---

**From:** (b)(6);

**Sent:** Monday, December 10, 2018 2:11 PM

**To:** (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6); (b)(7)(C) @ice.dhs.gov;

(b)(6); (b)(7)(C) @ice.dhs.gov>

**Cc:** (b)(6); (b)(7)(C) (CTR); (b)(6); (b)(7)(C) @associates.ice.dhs.gov; (b)(6); (b)(7)(C) (CTR)

(b)(6); (b)(7)(C) @associates.ice.dhs.gov; (b)(6); (b)(7)(C) (CTR)

(b)(6); (b)(7)(C) @associates.ice.dhs.gov>

**Subject:** RE: Cell Site Simulator (CSS) PTA - Walk through (this updates the Over the Air PTA)

(b)(6);

I am OK with the PTA. To answer your question about the all data deleted: All we are doing is confirming the data from the actual CSS device has been deleted in accordance with HSI policy. Also, as part of the policy, we are to have oversight on the deletion.

Thanks,

(b)(6);

Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-(b)(6) Desk  
571-839-(b)(6) Mobile  
(b)(6); @ICE.DHS.gov



Technical Support: ICE Service Desk: (b)(6); (b)(7)(C)  
VECADS Support: VECADS 24/7 Support Desk: (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov  
CVN Support: Spectrum Support Desk: (703) 551-(b)(6); (b)(7)(C) @ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, December 07, 2018 2:00 PM  
**To:** (b)(6); (b)(7)(C) @ice.dhs.gov <(b)(6); (b)(7)(C) @ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov  
(b)(6); @ice.dhs.gov  
**Cc:** (b)(6); (b)(7)(C) (CTR) (b)(6); @associates.ice.dhs.gov <(b)(6); (b)(7)(C) (CTR)>  
(b)(6); (b)(7)(C) @associates.ice.dhs.gov <(b)(6); (b)(7)(C) (CTR)>  
(b)(6); (b)(7)(C) @associates.ice.dhs.gov  
**Subject:** Cell Site Simulator (CSS) PTA - Walk through (this updates the Over the Air PTA)

All,  
Apologies for the delay in getting this PTA back to you – and also for the abrupt ending of our call yesterday.  
But as promised, I've updated the PTA making edits where we discuss during our call to include more for the CSS Log SharePoint site.

I hope this better reflects what we're trying to bring across.  
Let me know if you have any questions. If you have none, or are good with the document as written, let me know. Otherwise, if you do have any comments, or edits to the document, please update using tracked changes and send back to me. I'd like to finalize next week and send up to our ICE Privacy Officer by Wednesday and to DHS HQ Privacy by the end of next week.



(b)(6); (b)(7)(C)

Sr. Privacy Analyst (detailed to)  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement

202-394-(b)(6); Mobile

(b)(6); (b)(7)(C) @ice.dhs.gov

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx>



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](http://www.dhs.gov/privacy), on DHSCconnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.

LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)



LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE

**SPECIFIC PTA QUESTIONS**

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE

LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE

LAW ENFORCEMENT SENSITIVE



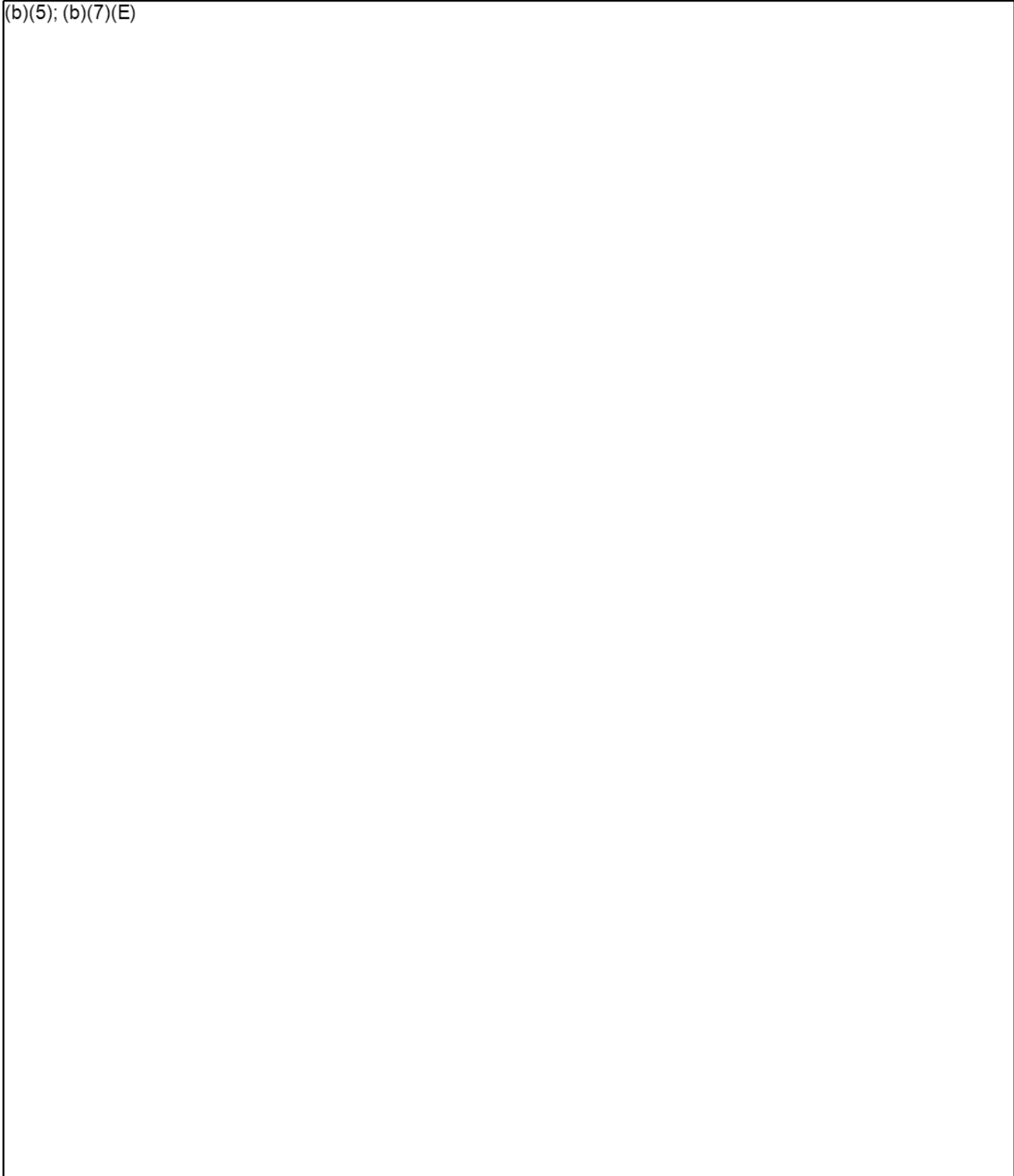
LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)



LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)



LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE





LAW ENFORCEMENT SENSITIVE    LAW ENFORCEMENT SENSITIVE

(b)(5); (b)(7)(E)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 28 Nov 2018 19:59:42 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: PTA - Cell Site Simulator (CSS) Technology and Log PTA (formerly Over the Air)  
**Attachments:** PTA, ICE - Over The Air Tracking Technology - LES, 20150403, PRIV FINAL.PDF, CSS PTA 2018.docx

All,

(b)(5); (b)(7)(E)

I've updated POTS with this background and copied the CSS PTA 2018 to the shared drive.

(b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, November 27, 2018 11:38 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Cc:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** FW: PTA

Thank you (b)(6);

(b)(6); please see the attachments. We've changed the "Over The Air" wording to Cell Site Simulator (CSS).

(b)(6); (b)(7)(C)

Section Chief  
Title - III / Communications Intercept  
U.S. Immigration and Customs Enforcement  
Homeland Security Investigations  
(b)(6); (b)(7)(C) Lorton, VA 22079  
Work (703) 551-(b)(6);  
Cell (202) 359-(b)(7)(C)

**Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this report should be furnished to the media, either in written or verbal form.**

**From:** (b)(6);  
**Sent:** Tuesday, November 27, 2018 11:19 AM  
**To:** (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Subject:** PTA

(b)(6);

I have attached the proposed update to the CSS PTA to include language for the CSS program and CSS log. Please let me know if you have any questions. I also attached the original PTA completed in 2015.

Thanks,

(b)(6);  
(b)(7)(C)

Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-(b)(6); Desk  
571-839-(b)(7)(C) Mobile  
(b)(6); @ICE.DHS.gov



Technical Support: ICE Service Desk: (b)(6); (b)(7)(C)  
VECADS Support: VECADS 24/7 Support Desk (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov  
CVN Support: Spectrum Support Desk: (b)(6); (b)(7)(C) @ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 15 Oct 2018 14:26:47 +0000  
**To:** (b)(6); (b)(7)(C) CTR  
**Subject:** RE: Cell Site Simulator

Hi (b)(6);

This PTA Renewal was among several of (b)(6); (b)(7)(C) PTAs where the POC just has not been responding. I will reach out again but like (b)(6); (b)(7)(C) haven't been able to get an update about Cell Site, Falcon TL, Workbench, or Cellebrite.

Best,

(b)(6);

---

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** Monday, October 15, 2018 10:20 AM  
**To:** (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Subject:** Cell Site Simulator

Hey (b)(6); (b)(7)(C)

I have you listed in POTS as the assignee for HSI Cell Site Simulator aka Over the Air Tracking System. However, I wasn't sure if this was done before or after your detail. Do you know the status of this PTA renewal?

Thanks (b)(6); (b)(7)(C)

(b)(6);  
**Supporting Information Governance and Privacy**  
**U.S. Immigration and Customs Enforcement**  
(b)(6); (b)(7)(C) [associates.ice.dhs.gov](mailto:associates.ice.dhs.gov)  
**Phone** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 27 Aug 2019 18:10:59 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Cellular Data Geolocation Procurement  
**Attachments:** G3T19-056.docx

Hello hello,

(b)(5)

Best,

(b)(6):

Mobile: 202-870-(b)(6);

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Tuesday, August 27, 2019 2:02 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Cellular Data Geolocation Procurement

Let's have (b)(6); take this one. I know (b)(6); reviewed a similar procurement but it's been a while since (b)(6); has looked at a PTA.

You might want to flag the potential PIA issue for him.

Sent with BlackBerry Work  
(www.blackberry.com)

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Date:** Tuesday, Aug 27, 2019, 2:00 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Cellular Data Geolocation Procurement

(b)(5)

Best,

(b)(6); (b)(7)(C)

Mobile: 202-870-(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Tuesday, August 27, 2019 1:33 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Cellular Data Geolocation Procurement

Perfect. Then we can approve this procurement.

(b)(5)

(b)(6); (b)(7)(C)  
Acting Privacy Officer  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Desk: 202-732-(b)(6);  
Mobile: 202-701-(b)(6);  
Main: 202-732-(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Tuesday, August 27, 2019 1:31 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Cellular Data Geolocation Procurement

Correct!

Best,  
(b)(6); (b)(7)(C)

Mobile: 202-870-(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Tuesday, August 27, 2019 1:30 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Cellular Data Geolocation Procurement

H (b)(6); (b)(7)(C)

Thanks for the review. To confirm, ICE is only looking (b)(5)

(b)(5)

(b)(6); (b)(7)(C)  
Acting Privacy Officer

Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Desk: 202-732-(b)(6);  
Mobile: 202-701-(b)(6);  
Main: 202-732-(b)(6);  
(b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Friday, August 23, 2019 1:21 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** Cellular Data Geolocation Procurement

Good Afternoon (b)(6);

Find enclosed a procurement for your review. There's not much information on the documents they provided, but I got the answer from the POCs over the phone

(b)(5)

Best,

(b)(6);

Mobile: 202-870-(b)(6);

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Tuesday, August 20, 2019 1:09 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov> (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)@ice.dhs.gov>  
**Cc:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

(b)(6);  
(b)(7)(C); ...I am open all day on Friday...so call me whenever you have an opening.

Thanks,

(b)(6); (b)(7)(C);  
(b)(7)(C)

Homeland Security Investigations  
Technical Operations Unit  
(703) 551-(b)(6)-Office  
(520) 631-(b)(6)-Cell

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Date:** Tuesday, Aug 20, 2019, 11:39 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Cc:** (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

Great, thanks. I'll ping him then.

Best,

(b)(6);  
(b)(7)(C)

Mobile: 202-870-(b)(6);  
(b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 20, 2019 11:39 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Cc:** (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)  
(b)(6);@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

I think (b)(6); (b)(7)(C) would be the best – he will be back in the office on the 23<sup>rd</sup>.

(b)(6);

Homeland Security Investigations  
Technical Operations Unit  
(703) 551-(b)(6)-Office  
(520) 631-(b)(7)(C)-Cell

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 20, 2019 11:23 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

Thanks (b)(6). Is there someone on your team available for a call this week to walk me through this technology and HSI's use of it?

Best,

(b)(6);  
(b)(7)(C)

Mobile: 202-870-(b)(6);



---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 20, 2019 10:57 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

I did send to the box again also  
Thanks

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 20, 2019 10:55 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

You can just send them to me now that the matter is created in the portal. Thanks!

Best,  
(b)(6); (b)(7)(C)

Mobile: 202-870-(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 20, 2019 10:46 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

Do you want me to upload them or just send them to you

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 20, 2019 10:44 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Cc:** (b)(6); (b)(7)(C)@ice.dhs.gov> (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: Privacy checklist

Good Morning (b)(6);

Thanks for uploading the documents to the Privacy Portal. Do you have anything else on the procurement, like a SOO or SOW? I'm looking for something with a description of what we are asking the vendor to do. Thanks in advance.

Best,  
(b)(6);

Mobile: 202-870-(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, August 19, 2019 2:56 PM

To: (b)(6); (b)(7)(C)@ice.dhs.gov  
Cc: (b)(6); (b)(7)(C)@ice.dhs.gov; (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)@ice.dhs.gov  
**Subject:** RE: Privacy checklist

Good Afternoon (b)(6);  
Do you have the SOW/PWS for the procurement? You can upload everything at  
(b)(7)(E) That's our  
procurement review portal. Just click on step 3 and fill in the field and attach the files. Thanks!

Best,  
(b)(6); (b)(7)(C)  
Mobile: 202-870 (b)(6);  
(b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, August 19, 2019 2:52 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov  
**Cc:** (b)(6); (b)(7)(C)@ice.dhs.gov; (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)@ice.dhs.gov  
**Subject:** Privacy checklist

Good afternoon  
Can you please process  
Thanks

(b)(6); (b)(7)(C)  
ICE/HSI Homeland Security Investigations  
Technical Operations Unit  
(b)(6); (b)(7)(C) Mail Stop 5118  
Lorton, VA 22079  
703-551 (b)(6);  
I-Phone 202-534 (b)(6);

*WARNING: The information contained herein remains under the control of the Department of Homeland Security (DHS), through the U.S. Immigration and Customs Enforcement (ICE). It is being disseminated for authorized law enforcement purposes only. This E-Mail and/or information accompanying this E-Mail are confidential belonging to the sender and are protected. This information is intended only for the use of the individual or entity named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or E-Mail.*

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** 15 Oct 2018 14:51:11 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Cell Site Simulator

Oh good to know. I will make a note of it. Thanks (b)(6);

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, October 15, 2018 10:27 AM  
**To:** (b)(6); (b)(7)(C)@associates.ice.dhs.gov>  
**Subject:** RE: Cell Site Simulator

Hi (b)(6); (b)(7)(C)

This PTA Renewal was among several of (b)(6); (b)(7)(C) PTAs where the POC just has not been responding. I will reach out again but like (b)(6); I haven't been able to get an update about Cell Site, Falcon TL, Workbench, or Cellebrite.

Best,

(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C) (CTR)  
**Sent:** Monday, October 15, 2018 10:20 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** Cell Site Simulator

Hi (b)(6);

I have you listed in POTS as the assignee for HSI Cell Site Simulator aka Over the Air Tracking System. However, I wasn't sure if this was done before or after your detail. Do you know the status of this PTA renewal?

Thanks (b)(6);

(b)(6);  
**Supporting Information Governance and Privacy**  
**U.S Immigration and Customs Enforcement**  
(b)(6); (b)(7)(C)@associates.ice.dhs.gov  
**Phone:** (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 20 Jul 2018 16:13:30 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Re: Cell Site Simulator Log

Good afternoon (b)(6);

Have you had a chance to take a look at the PTA template that (b)(6); sent you in January? We would need to have a PTA on file to ensure compliance. If you have any questions I would be happy to help.

Best,

(b)(6); (b)(7)(C)

Presidential Management Fellow  
Office of Information Governance and Privacy

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, January 25, 2018 2:27 PM  
**To:** (b)(6);  
**Subject:** Cell Site Simulator Log

(b)(6);  
(b)(7)(C)

I have spoken with (b)(6); and we think (b)(5)

(b)(5)

Thank you,

(b)(6); (b)(7)(C)

Privacy Compliance Specialist  
Privacy Branch  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Main: (202) 732 (b)(6);  
Direct: (202) 732 (b)(6);  
Mobile: (202) 878 (b)(6);

Questions? Please visit the Office of Information Governance & Privacy website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, January 16, 2018 11:21 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: Link

Thanks for the update.

(b)(6); (b)(7)(C)

Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-(b)(6); Desk  
571-839-(b)(7) Mobile  
(b)(6); @ICE.DHS.gov



Technical Support: ICE Service Desk (b)(6); (b)(7)(C)  
VECADS Support: VECADS 24/7 Support Desk: (b)(6); (b)(7)(C) pr  
(b)(6); (b)(7)(C) rt@ice.dhs.gov  
CVN Support: Spectrum Support Desk (b)(6); (b)(7)(C) pr  
(b)(6); (b)(7)(C) @ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, January 16, 2018 11:21 AM  
**To:** (b)(6);  
**Subject:** RE: Link

(b)(6); (b)(7)(C) is out with (b)(6); (b)(7)(C) know it's on my list of things to resolve with her this week, upon her return.

(b)(6); (b)(7)(C)

Privacy Compliance Specialist  
Privacy Branch  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Main: (202) 732-(b)(6); (b)(7)(C)  
Direct: (202) 732-(b)(6); (b)(7)(C)  
Mobile: (202) 878-(b)(6); (b)(7)(C)

Questions? Please visit the Office of Information Governance & Privacy website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.

---

**From:** (b)(6);  
**Sent:** Tuesday, January 16, 2018 10:59 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Link

(b)(6); (b)(7)(C)

I wanted to follow up on the approval for this site.

Thanks,

(b)(6); (b)(7)(C)

Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-(b)(6); Desk  
571-839-(b)(7)(C) Mobile  
(b)(6); @ICE.DHS.gov



Technical Support: ICE Service Desk: (b)(6); (b)(7)(C)  
VECADS Support: VECADS 24/7 Support Desk: (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov  
CVN Support: Spectrum Support Desk: (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5

U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

---

**From:** (b)(6);  
**Sent:** Wednesday, January 03, 2018 11:01 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Link

H (b)(6); (b)(7)(C) – When is your S1 briefing? Also, what sort of additional detail are you looking to include on the site?

(b)(6);  
Privacy Officer  
Information Governance & Privacy  
U.S. Immigration & Customs Enforcement  
Direct: (202) 732- (b)(6)  
Mobile: (202) 487- (b)(6)  
Main: (202) 73- (b)(6);

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.

---

**From:** (b)(6);  
**Sent:** Wednesday, January 3, 2018 8:35 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Link

(b)(6);  
(b)(7)(C)

I wanted to check on the status of the approval for this site? We are having a briefing for S1 and would like to include information on the site in the briefing.

Thanks,

(b)(6); (b)(7)(C)  
Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551- (b)(6); Desk  
571-839- (b)(7)(C) Mobile  
(b)(6); (b)(7)(C) ICE.DHS.gov



Technical Support: ICE Service Desk: (b)(6); (b)(7)(C) or  
VECADS Support: VECADS 24/7 Support Desk (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov  
CVN Support: Spectrum Support Desk (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, December 20, 2017 12:10 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Link

Thanks, (b)(6); Could you also please send the final cell-site simulator policy?

(b)(6);  
Privacy Officer  
Information Governance & Privacy  
U.S. Immigration & Customs Enforcement  
Direct: (202) 732-(b)(6);  
Mobile: (202) 487-(b)(6);  
Main: (202) 732-(b)(6);

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/ooop/Pages/index.aspx>.

---

**From:** (b)(6);  
**Sent:** Wednesday, December 20, 2017 12:06 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Link

All of you have been added.

Thanks,

(b)(6); (b)(7)(C)



Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-(b)(6); Desk  
571-839-(b)(7)(C) Mobile  
(b)(6); @ICE.DHS.gov



Technical Support: ICE Service Desk: (b)(6); (b)(7)(C)  
VECADS Support: VECADS 24/7 Support Desk (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov  
CVN Support: Spectrum Support Desk (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, December 20, 2017 11:59 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Link

Hi (b)(6); (b)(7)(C) - I don't have access. Can you please add permissions for me to view? I would like (b)(6); (b)(7)(C) and (b)(6); (b)(7)(C) from my office to review, as well.

(b)(6);  
Privacy Officer  
Information Governance & Privacy  
U.S. Immigration & Customs Enforcement  
Direct: (202) 732-(b)(6);  
Mobile: (202) 48-(b)(7)(C)  
Main: (202) 73-(b)(6);

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.

---

**From:** (b)(6);  
**Sent:** Thursday, December 14, 2017 12:48 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: Link

(b)(6);  
(b)(7)(C)

Here is the link to the Cell Site Simulator Log SharePoint site. We would like to keep more detailed records of operations while maintaining a location for search warrants. Please let me know if you have any questions.

(b)(7)(E)

Click on the + button to see the different fields.

Thanks,

(b)(6); (b)(7)(C)

Homeland Security Investigations  
National Program Manager  
Technical Enforcement Officer  
703-551-(b)(6); Desk  
571-839-(b)(7)(C) Mobile  
(b)(6); @ICE.DHS.gov



Technical Support: ICE Service Desk: (b)(6); (b)(7)(C)  
VECADS Support: VECADS 24/7 Support Desk (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov  
CVN Support: Spectrum Support Desk (b)(6); (b)(7)(C) or  
(b)(6); (b)(7)(C) @ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.