



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

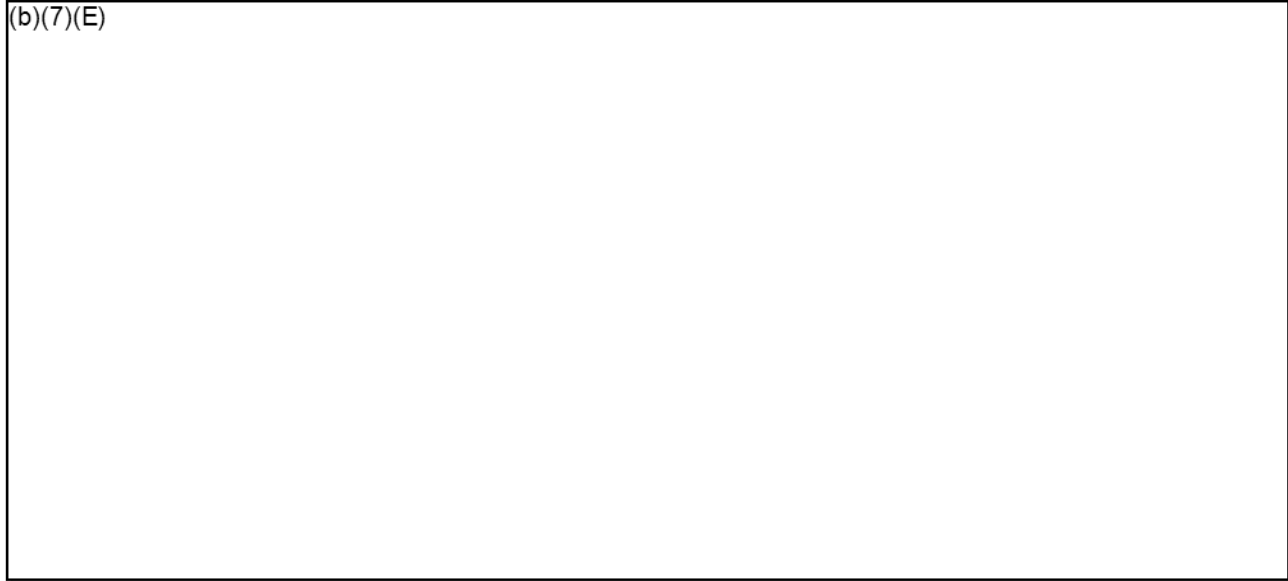
(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

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, on DHSCconnect and directly from the DHS Privacy Office via email: 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



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. 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. 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) 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
Jm

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,¹ it is vital that their use be subject to strict oversight by the courts and Congress.

¹ 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.”² 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?

² 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.³ 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?

³ See "Prime Award Spending Data," available at 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.

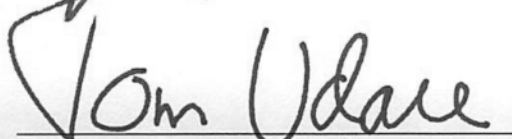
Sincerely,



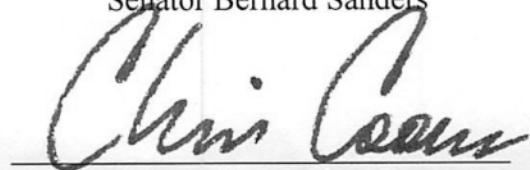
Senator Jon Tester



Senator Bernard Sanders




Senator Tom Udall



Senator Christopher Coons



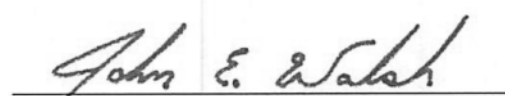
Senator Mark Begich



Senator Tammy Baldwin



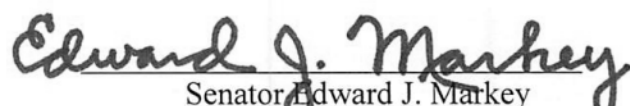
Senator Al Franken



Senator John Walsh



Senator Jeff Merkley



Senator Edward J. Markey



Senator Martin Heinrich

United States Senate

WASHINGTON, DC 20510

CAPITAL DISTRICT 208

10 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



2020 ICE 0013 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

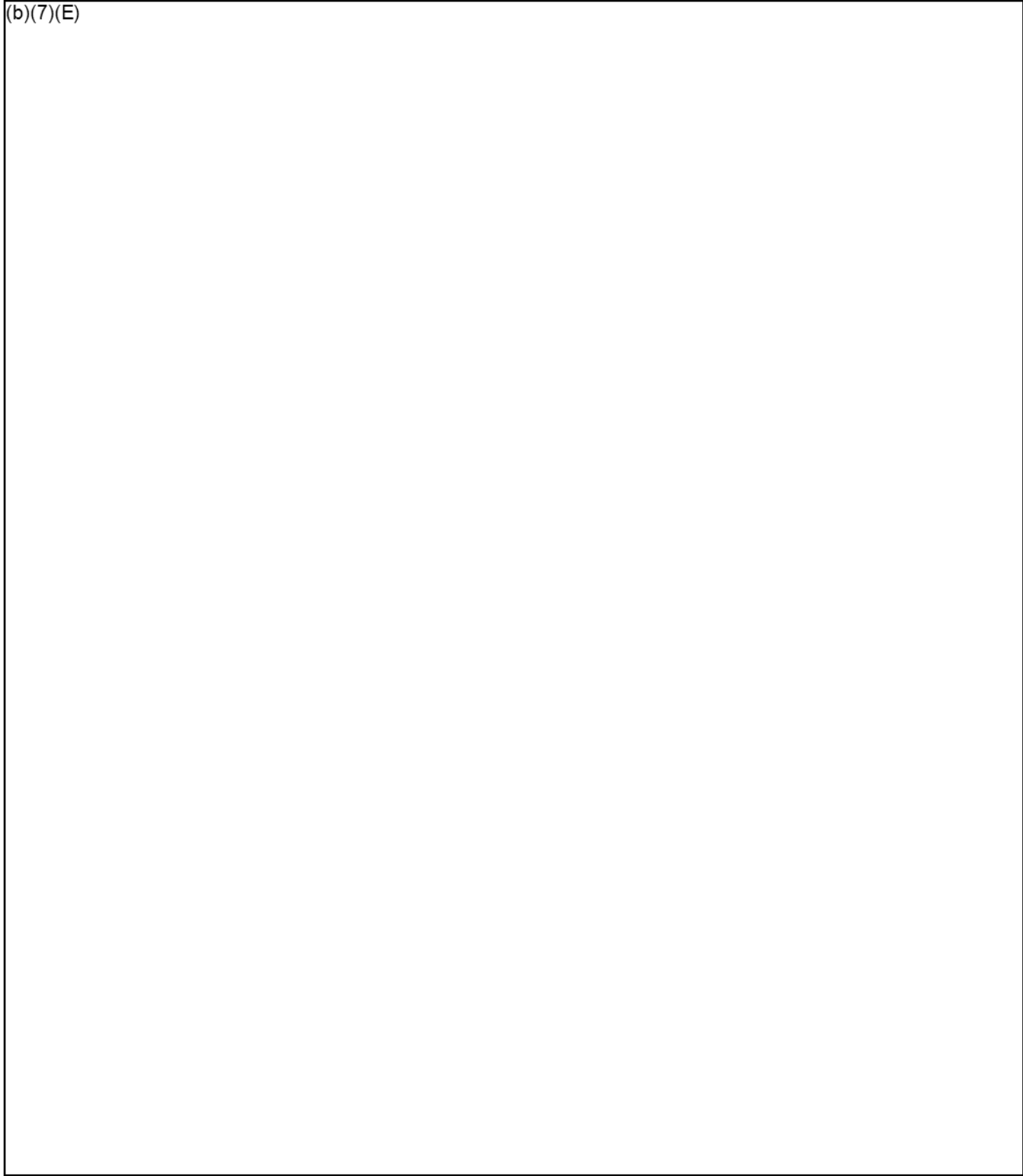
(b)(7)(E)

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



**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 11

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

2020-ICLI-00013 1061



**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



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

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-

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) 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 12th 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, on DHSCconnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(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



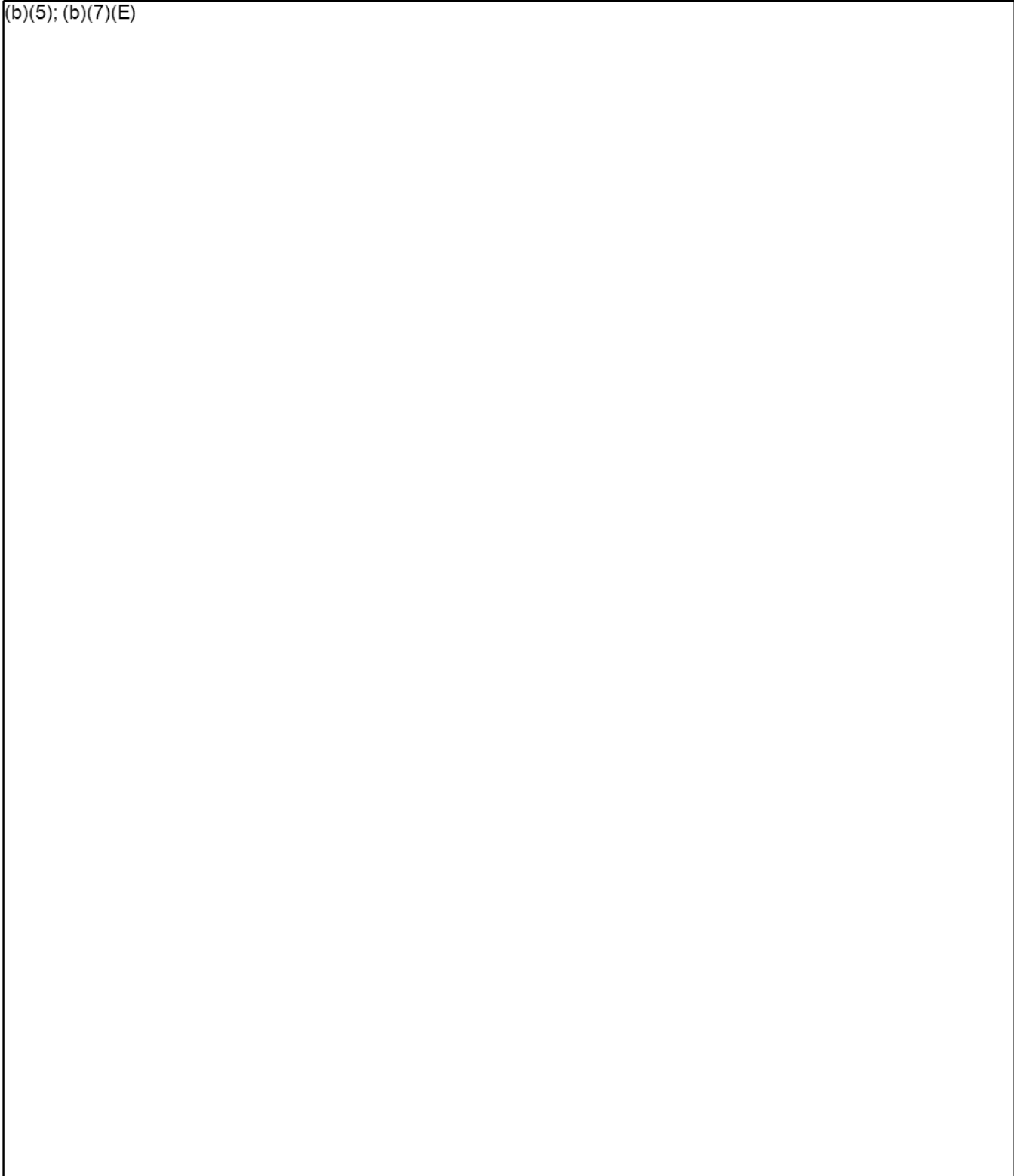
LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(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)(7)(C)

(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
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); (b)(7)(C)
Mobile: 202-701-(b)(6); (b)(7)(C)
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 23rd.

(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

He (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) 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 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) 481-(b)(7)(C)
Main: (202) 732-(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.