

From: Blank, Thomas
Sent: Tue, 15 May 2018 18:54:34 +0000
To: (b)(6); (b)(7)(C) Erichs, Alysa
Cc: Turner, James
Subject: RE: IMSI Catchers/Stingrays
Importance: Normal

Thanks (b)(6);

Thomas Blank
Chief of Staff
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
202 732 (b)(6);
Cell 202 591 (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Tuesday, May 15, 2018 2:04 PM
To: Erichs, Alysa (b)(6); (b)(7)(C) @ice.dhs.gov>; Blank, Thomas (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: IMSI Catchers/Stingrays

Thanks! Understood, just wanted you all to be aware (b)(5)

From: Erichs, Alysa
Sent: Tuesday, May 15, 2018 2:03:06 PM
To: (b)(6); (b)(7)(C) Blank, Thomas
Cc: (b)(6);
Subject: RE: IMSI Catchers/Stingrays

I will (b) (5), (b) (7)(E)
(b) (5), (b) (7)(E) Would recommend sending to OCIO as well.

Thanks,
Alysa

From: (b)(6); (b)(7)(C)
Sent: Tuesday, May 15, 2018 1:41 PM
To: Blank, Thomas (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>; Erichs, Alysa (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: IMSI Catchers/Stingrays
Importance: High

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

As discussed, attached is the deck with all proposed redactions, comments removed, and ready for the inter/intra agency coordination requested by leadership. We are sending the attached to ICE, USSS and

FBI for review and comment. As mentioned, this is a very quick turn (b)(5)

(b)(5)

IF you have any questions, please don't hesitate to reach out. Adding Alysa Erichs for her awareness, but haven't had the same conversation with her to explain the backstory (b)(5) Alysa- feel free to reach out and I can bring you up to speed.

Many thanks,

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

Director, Office of Legislative Affairs
National Protection and Programs Directorate
U.S. Department of Homeland Security

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

From: Blank, Thomas <(b)(6); (b)(7)(C)@ice.dhs.gov>

Sent: Tuesday, May 15, 2018 1:32 PM

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

Cc: (b)(6); (b)(7)(C)@ice.dhs.gov>

Subject: RE: IMSI Catchers/Stingrays

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

Please reach out to (b)(6); (b)(7)(C) as I will be in meetings most of the rest of the day. (b)(6) is a SA assigned to the OD

Thanks,

Tom

Thomas Blank
Chief of Staff
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
202 732 (b)(6);
Cell 202 591 (b)(6)

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

Sent: Tuesday, May 15, 2018 1:16 PM

To: Blank, Thomas <(b)(6); (b)(7)(C)@ice.dhs.gov>

Subject: IMSI Catchers/Stingrays

Importance: High

Sir,

Apologies for reaching out directly, but I have a hot issue that I think ICE may have equities on that I want to bring to your attention and also give you a chance to review. I need to get something to S1 today, so it's a quick turn... regarding IMSI catchers/stingrays, (b)(5)

(b)(5)

Hope all is well!

Best,

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

Director, Office of Legislative Affairs
National Protection and Programs Directorate
U.S. Department of Homeland Security

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

From:
MicrosoftExchange (b) (7)(E)
of Blank, Thomas

@icegov.onmicrosoft.com on behalf

Sent: Tue, 15 May 2018 18:55:03 +0000
To: (b)(6); (b)(7)(C) Erichs, Alysa
Cc: (b)(6); (b)(7)(C)
Subject: RE: IMSI Catchers/Stingrays
Attachments: RE: IMSI Catchers/Stingrays
Importance: Normal

Sender: (b)(6); [redacted]@ice.dhs.gov
Subject: RE: IMSI Catchers/Stingrays
Message-Id:
<(b) (5), (b) (7)(E)
com>
To: (b)(6); [redacted]@ice.dhs.gov
Cc: (b)(6); [redacted]@ice.dhs.gov

amprd09.prod.outlook.

From: Blank, Thomas
Sent: Tue, 15 May 2018 18:50:38 +0000
To: (b)(6); (b)(7)(C)
Subject: FW: IMSI Catchers/Stingrays
Attachments: Proposed redactions marked - 5.15.2018.pdf
Importance: High

(b)(6)

NPPD sent this over and HSI looked it over. It was suggested that it be sent to you in case there are concerns. Please have a look and advise (b)(6); (b)(7)(C) if there are.

Tom

Thomas Blank
Chief of Staff
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
202 731 (b)(6):
Cell 202 591 (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) (5), (b) (6), (b) (7)(C), (b) (7)(E)

From: (b)(6); (b)(7)(C)
Sent: Tue, 15 May 2018 20:33:30 +0000
To: Erichs, Alysya; Blank, Thomas
Cc: Turner, James; Benner, Derek N
Subject: RE: IMSI Catchers/Stingrays
Importance: Normal

Alysya,

Great to talk to you! Thanks again to all of you for taking the time and the quick turn. I very much appreciate it. (b)(5)

(b)(5) I will be sure to keep you all posted.

Let me know if you all ever need anything from this end!

Best,

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

From: Erichs, Alysya
Sent: Tuesday, May 15, 2018 4:29:42 PM
To: (b)(6); (b)(7)(C) Blank, Thomas
Cc: Turner, James; Benner, Derek N
Subject: RE: IMSI Catchers/Stingrays

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

(b)(5)

If you need additional information, please let me know.

Thank you,
Alysya

Alysya D. Erichs
Acting Deputy Executive Associate Director
Homeland Security Investigations
Washington, DC
202-732-(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)



From: MicrosoftExchange (b) (5), (b) (7)(E) @icegov.onmicrosoft.com on behalf of (b)(6); (b)(7)(C)
Sent: Tue, 15 May 2018 20:34:39 +0000
To: Erichs, Alysa; Blank, Thomas
Cc: Turner, James; Benner, Derek N
Subject: RE: IMSI Catchers/Stingrays
Attachments: RE: IMSI Catchers/Stingrays
Importance: Normal

Sender: (b)(6); (b)(7)(C)
Subject: RE: IMSI Catchers/Stingrays
Message-Id: <(b) (7)(E)>
Recipient: (b)(6); @ice.dhs.gov
Recipient: (b)(7)(C) @ice.dhs.gov
Recipient: (b)(6); @ice.dhs.gov
Recipient: (b)(6); (b)(7)(C) @ice.dhs.gov

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);

(b)(7)(C)

I have copied in TechOps Unit Chief (b)(6); (b)(7)(C) as the Stingray program for HSI is under his shop with (b)(7)(E) (b)(6); (b)(7)(C) 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/oop/>.

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)

Stingray: A portable, electronic surveillance device for remotely capturing data from cell phones. Designed to simulate a cell phone tower and capture information, including location data, which can be done even when the phone is not making a phone call.

The technology is being used by the FBI and other law enforcement agencies.

- 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
- 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

(b)(5)

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

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



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

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

PIA@hq.dhs.gov

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

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

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

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

PROJECT OR PROGRAM MANAGER

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

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

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

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA
<p>U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) is renewing the Over the Air Technology PTA (last adjudicated April 3, 2015) and replacing it with this PTA for Cell Site Simulators (CSS).</p> <p>HSI uses CSS to track mobile phones within the course of carrying out criminal investigations. HSI's use of this technology has always proceeded under established internal practices (e.g., obtaining first-level supervisor approval prior to applying for a court order) and appropriate legal process. Before this technology is used, HSI obtains court orders or search warrants (depending on the judicial district) through the appropriate United States Attorneys' Offices which authorize the use of this technology. If HSI partners with another department or agency on a case, that office may be responsible for obtaining the court order or warrant. This can include such partnerships with the U.S. Department of Justice, U.S. Drug Enforcement Administration (DEA), or state and local law enforcement agencies.</p>
(b)(7)(E)
(b) (5), (b) (7)(E) (b)(7)(E)
(b)(7)(E)
(b)(7)(E)

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

(b)(7)(E)

Any relevant information learned through the use of this technology will be documented by the agent in a Report of Investigation (ROI) and placed in an HSI case file to document agent activity in the investigation (b)(7)(E)

(b)(7)(E)

Device Indicators:

(b)(7)(E)

¹ A pen register, or dialed number recorder (DNR), is an electronic device that records all numbers called from a particular telephone line. The term has come to include any device or program that performs similar functions to an original pen register, including programs monitoring Internet communications. More information about Pen Registers, and legal restrictions can be found at: <http://uscode.house.gov/view.xhtml?path=/prelim@title18/part2/chapter206&edition=prelim>.

(b)(7)(E)

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

(b)(7)(E)

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

(b)(7)(E)

2. Does this system employ any of the following technologies:

If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.

- Closed Circuit Television (CCTV)
- Social Media
- Web portal⁴ (e.g., SharePoint)
- Contact Lists
- None of these

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

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

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

<p>4. What specific information about individuals is collected, generated or retained?</p>
<p>No information about individuals is maintained on the CSS device itself.</p>
<p>(b)(7)(E)</p>

⁵ DHS defines personal information as “Personally Identifiable Information” or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. “Sensitive PII” is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



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~~

Any information included in the warrant, court order, or subpoena can also include name and email of the agent(s)/officer(s) working the case and can include name of the Department/Agency, state, local law enforcement agency (as applicable) that is part of the investigation. This information is stored in the ROI.	
4(a) Does the project, program, or system retrieve information by personal identifier?	<input type="checkbox"/> No. Please continue to next question. <input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: Name of the HSI case agent
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	NA
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	NA
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data⁶ is stored in the communication traffic log, please detail the data elements stored.	
N/A	

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

⁶ When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

(b) (7)(E)

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

<p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p>	<p>(b) (5), (b) (7)(E)</p>
<p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p>	<p>(b) (5), (b) (7)(E)</p>
<p>7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?</p>	<p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: Per an HSI policy memo, personnel who use this technology are required be trained on how to operate it and with respect to privacy and civil liberties.</p>
<p>8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?</p>	<p>(b) (5), (b) (7)(E)</p>
<p>9. Is there a FIPS 199 determination?⁸</p>	<p><input type="checkbox"/> Unknown.</p>

⁸ FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

	<input checked="" type="checkbox"/> No. ICE OCIO has yet to issue a FIPS-199 determination. <input type="checkbox"/> Yes. Please indicate the determinations for each of the following: Confidentiality: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	--

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b) (6), (b) (7) (C)
Date submitted to Component Privacy Office:	May 29, 2019
Date submitted to DHS Privacy Office:	Click here to enter a date.
Component Privacy Office Recommendation:	
<i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
ICE is submitting this PTA to renew and update the information provided in the 2015 Over the Air Tracking Technology PTA. The ICE Privacy Division recognizes that (b) (5), (b) (7)(E) and (b) (5), (b) (7)(E) recommends (b) (5), (b) (7)(E) As such, a PIA is required. ICE recommends (b) (5), (b) (7)(E) SORN coverage is provided under DHS/ICE-009 - External Investigations (Jan. 5, 2010, 75 FR 404).	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

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

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



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~~

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

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.
PIA:	New PIA is required. If covered by existing PIA, please list: Forthcoming ICE Surveillance Technologies PIA
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ICE-009 External Investigations January 5, 2010 75 FR 404
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
ICE is submitting this PTA to discuss the use of Cell Site Simulators (CSS), which are used to track mobile phones within the course of carrying out criminal investigations. Before this technology is used, HSI obtains court orders or search warrants (depending on the judicial district) through the appropriate United States Attorneys' Offices which authorize the use of this technology. (b)(7)(E)	
(b)(7)(E)	

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~

(b)(7)(E)

HSI captures information from the devices and about the investigation in a CSS sharepoint log, and also may create a copy of data form the CSS that is stored locally. (b)(5)

(b)(5)

~~LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE~~



~~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~~

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	Over The Air Tracking Technology		
Component:	Immigration and Customs Enforcement (ICE)	Office or Program:	HSI- Technical Operations /Investigative Intercept
Xacta FISMA Name (if applicable):	n/a	Xacta FISMA Number (if applicable):	n/a
Type of Project or Program:	Choose an item.	Project or program status:	Existing
Date first developed:	January 4, 2005	Pilot launch date:	January 17, 2005
Date of last PTA update	Click here to enter a date.	Pilot end date:	Click here to enter a date.
ATO Status (if applicable)	Choose an item.	ATO expiration date (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b)(6); (b)(7)(C)		
Office:	Investigative Intercept Section	Title:	Section Chief, Investigative Intercept Section
Phone:	(b)(6); (b)(7)(C)	Email:	(b)(6); (b)(7)(C)@ice.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

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

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



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

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Choose an item.	
Homeland Security Investigations in U.S. Immigration and Customs Enforcement uses government-purchased technology that permits over-the-air (OTA) tracking of mobile telephones in the course of criminal investigations. (b)(7)(E)	
(b)(7)(E)	
Before this technology is used, HSI agents obtain court orders or search warrants (depending on the judicial district) via the local US Attorney's Offices authorizing the use of this technology. HSI's use of this technology has always proceeded only under appropriate legal process.	
HSI uses these devices in two operational scenarios: (b)(7)(E)	
(b)(7)(E)	

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



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

(b)(7)(E)

The technology that is used is considered a law enforcement technique that is not generally known and is protected by a confidentiality agreement between the equipment manufacturer and the government.

Any relevant information learned as a result of use of this technology will be documented by the agent in a Report of Investigation and placed in an HSI case file to document agent activity in the investigation. The raw records produced by the OTA tracker are not maintained in the case file.

<p>2. Does this system employ any of the following technologies: <i>If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.</i></p>	<p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal¹ (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input checked="" type="checkbox"/> None of these</p>
--	--

<p>3. From whom does the Project or Program collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information²</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p>
--	--

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

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

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



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

4. What specific information about individuals is collected, generated or retained?	
The following mobile phone identifiers may be collected or retained: (b)(7)(E)	
(b)(7)(E)	
(b)(7)(E) This information on its own does not identify individuals, however, unless additional information is obtained from a service provider.	
4(a) Does the project, program, or system retrieve information by personal identifier?	<input checked="" type="checkbox"/> No. Please continue to next question. N.B. The mobile phone information that is collected is ultimately placed in an investigative case file, which typically is filed by the name of the investigation. In many cases, the name of the investigation is a person's name. <input type="checkbox"/> Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	NA
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	NA
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.	

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

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



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

<p>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems⁴?</p>	<p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: Click here to enter text.</p>
<p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p>	<p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: Click here to enter text.</p>
<p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p>	<p>Choose an item. N/A</p>
<p>7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?</p>	<p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: Personnel who use this technology must be trained on how to operate it.</p>
<p>8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?</p>	<p><input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: Not applicable. Any accounting of disclosures, to the extent they are authorized, would be from the case file when the information is kept. <input type="checkbox"/> Yes. In what format is the accounting maintained:</p>
<p>9. Is there a FIPS 199 determination?⁴</p>	<p><input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following: Confidentiality:</p>

⁴ PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

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

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



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

	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	---

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Lyn Rahilly
Date submitted to Component Privacy Office:	January 9, 2015
Date submitted to DHS Privacy Office:	Click here to enter a date.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b)(7)(E)	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6); (b)(7)(C)
PCTS Workflow Number:	1063714
Date approved by DHS Privacy Office:	April 3, 2015
PTA Expiration Date	April 3, 2016

DESIGNATION

~~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 8

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

Privacy Sensitive System:	Yes If “no” PTA adjudication is complete.
Category of System:	Form/Information Collection If “other” is selected, please describe: Click here to enter text.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.
PIA:	New PIA is required. If covered by existing PIA, please list: Click here to enter text.
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ICE-009 - External Investigations January 5, 2010 75 FR 404
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
PRIV finds that Over the Air Tracking Technology is a privacy sensitive tool. Mobile phones are often used by one person and are linkable to an individual. Although review by a neutral magistrate before use significantly mitigates improper search concerns, PRIV finds that the use of this technology requires a PIA. PRIV understands that there will be LES portions of this PIA. SORN coverage is provided by the DHS/ICE-009 External Investigations SORN.	

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

United States Senate

November 18, 2015

The Honorable Jeh Johnson
Secretary of Homeland Security
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Johnson,

I am writing regarding the use and transfer of cell-site simulator technology, also referred to as International Mobile Subscriber Identity (IMSI) catchers, "DRTBoxes," "Dirtboxes," or "Stingrays." While I am pleased that the Department of Homeland Security (DHS) released its *Policy Regarding the Use of Cell-Site Simulator Technology*, I remain concerned that these guidelines are too broad and create loopholes that allow the continued abuse of this technology.

One of my primary concerns is that DHS guidance states that it only applies to "the use of cell-site simulator technology inside the United States in furtherance of criminal investigations." I am concerned that these technologies are also being used for types of investigations other than criminal, raising the possibility of mission creep into any number of areas that fall under the broad umbrella of national security. In order to ensure this technology is not used in opposition to constitutionally guaranteed rights for Americans, at home and abroad, what guidelines apply when this technology is used in investigations and for purposes not outlined in this policy?

Additionally, I am concerned that the guidance does not apply to states and localities that receive federal financial assistance or authorization to purchase or use this technology. In the Department's response to my letter on this topic earlier this year inquiring about the use of this technology, DHS stated that it compels grantees to abide by Standard Form 424B (SF-424B), "Assurances for Non-Construction Programs." How does your Department ensure compliance at the state and local level, and what systems are in place to track and monitor the use of these devices when they are operated by DHS grantees? DHS must conduct comprehensive oversight of the use of this technology and must actively audit metrics associated with the use of IMSI-catchers and related technology. As part of this guidance, DHS should require training for DHS grantees on the use of these devices to ensure they are properly operated and that information collected by this technology is obtained in accordance with the Constitution, all legal authorities, and Department-wide guidance.

Moreover, while I am relieved to see in the guidelines that DHS does not listen to or collect the context of communications using cell-site simulator technology for criminal investigations, failure to apply these guidelines outside the Department leaves open the possibility that federal funding – or authorization – could still be used to support these and other troubling practices.

I am also encouraged that DHS and its agencies now require a search warrant based on probable cause to deploy this technology. This is a positive step towards protecting the privacy of innocent Americans. While I understand the need for an expedited process in specific “exigent” and “exceptional” circumstances, the Department should still be required to meet the probable cause standard, instead of the lower standard under 18 U.S.C. § 3125. In addition, the guidance should specifically state what constitutes an “exceptional circumstance,” including the factors that must be considered to permit such a determination. It is important the policy clarifies whether aerial operations utilizing cell-site simulator technology to apprehend fugitives fall under the exigent or exceptional circumstance exception.

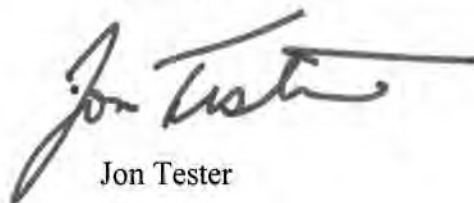
Furthermore, additional guidance should include a requirement that an individual be notified in cases where this technology is or has been used to apprehend them or gather evidence relevant to their case. DHS guidance still remains unclear as to whether criminal defendants in pending or future cases will be provided notice of the legal and illegal use of these devices, which is necessary to ensure appropriate judicial oversight.

I believe that the use of such technology requires diligent Congressional oversight. As a member of the Senate Appropriations Committee and the Senate Committee on Homeland Security and Governmental Affairs, I will actively be seeking report language in the appropriations process to ensure the proper use of this technology. Given the scope of use of cell-site simulator technology, I will request that DHS submit to the appropriate Congressional Committees, including the Appropriations Committee—at minimum on an annual basis—reports on the details of DHS and DHS grantees’ purchase, deployment, and investigation results of utilizing this technology.

Finally, I have followed reports that Datong plc, a United Kingdom-based company that produces cell phone surveillance systems, counts the U.S. Secret Service and U.S. Immigration and Customs Enforcement as clients. According to reports, Datong’s cell site simulators have the capability to intercept calls and messages and shut off phones altogether. More troubling is that Datong was awarded \$1.6 million in contracts between 2004 and 2009 with the Department. I therefore request further details about the capabilities of the Datong devices that DHS purchased, and in what capacity they are being utilized within the Department.

Given the tremendous capabilities this technology affords law enforcement officials, I am pleased that DHS has taken steps to regulate these devices. I am encouraged by the Department’s efforts to ensure that the use of these devices is consistent with the Constitution and other legal authorities. I believe it is in everyone’s best interest to clarify and strengthen cell-site simulator technology policy guidelines, and I look forward to working with you to increase the transparency and accountability of its use.

Sincerely,

A handwritten signature in black ink, appearing to read "Jon Tester", with a long horizontal flourish extending to the right.

Jon Tester

MEMORANDUM FOR: Christian Marrone
DHS Chief of Staff

FROM: Alan D. Bersin
Assistant Secretary for International Affairs
& Chief Diplomatic Officer, PLCY

SUBJECT: **Request for Approval: Response to Senator John Tester's
November 18, 2015 Letter Regarding the Department's
Policies on Cell-Site Simulators (WF #1112753)**

Context: This response addresses Senator John Tester's questions about DHS's cell-site simulator policy. The response: (b)(5)

(b)(5)

Clearance:

- CRCL:
- FEMA:
- ICE:
- MGMT:
- OGC:
- OLA:
- PRIV:
- TSA:
- USSS:

Timeliness: There are no timeliness concerns related to this letter which has been fully cleared and is being submitted to ESEC within the eight business day standard.

Page 1134

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1135

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1136

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1137

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

~~FOR OFFICIAL USE ONLY~~

(This slide UNCLASSIFIED)

Cellular Threats

Briefing for the Federal Mobile Technology Forum

Hosted by Federal CIO Council's Mobile Technology Tiger Team (MTTT)

6 February 2018

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

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

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

National Coordinating Center for Communications (NCC)

National Cybersecurity & Communications

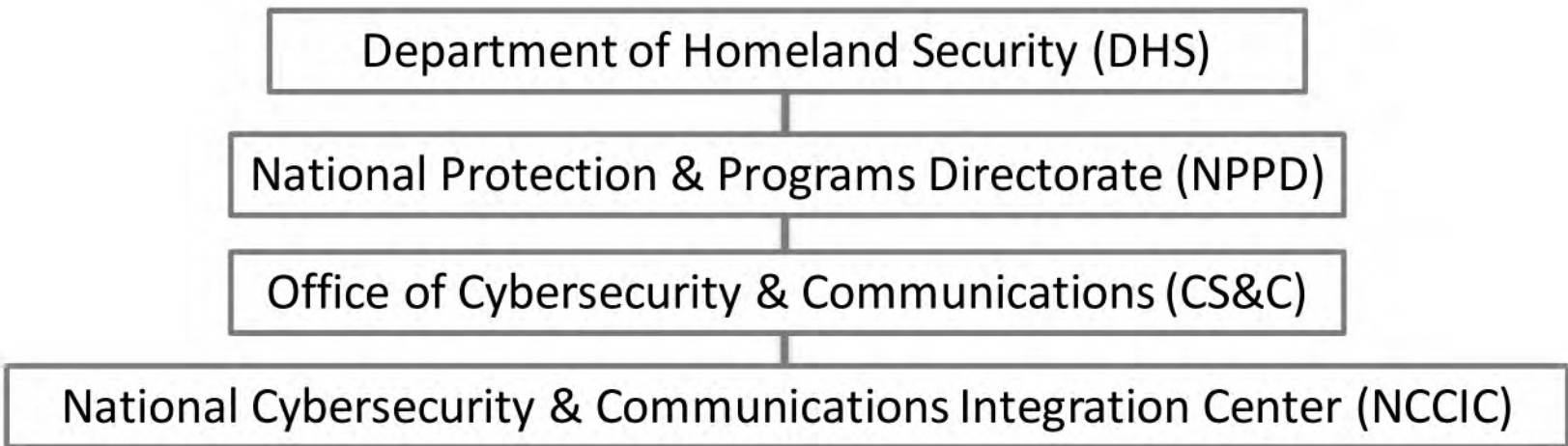
Integration Center (NCCIC)

2020-ICLI-00013 1138



**Homeland
Security**

National Cybersecurity & Communications Integration Center (NCCIC)



The NCCIC mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation’s critical information technology and communications networks.

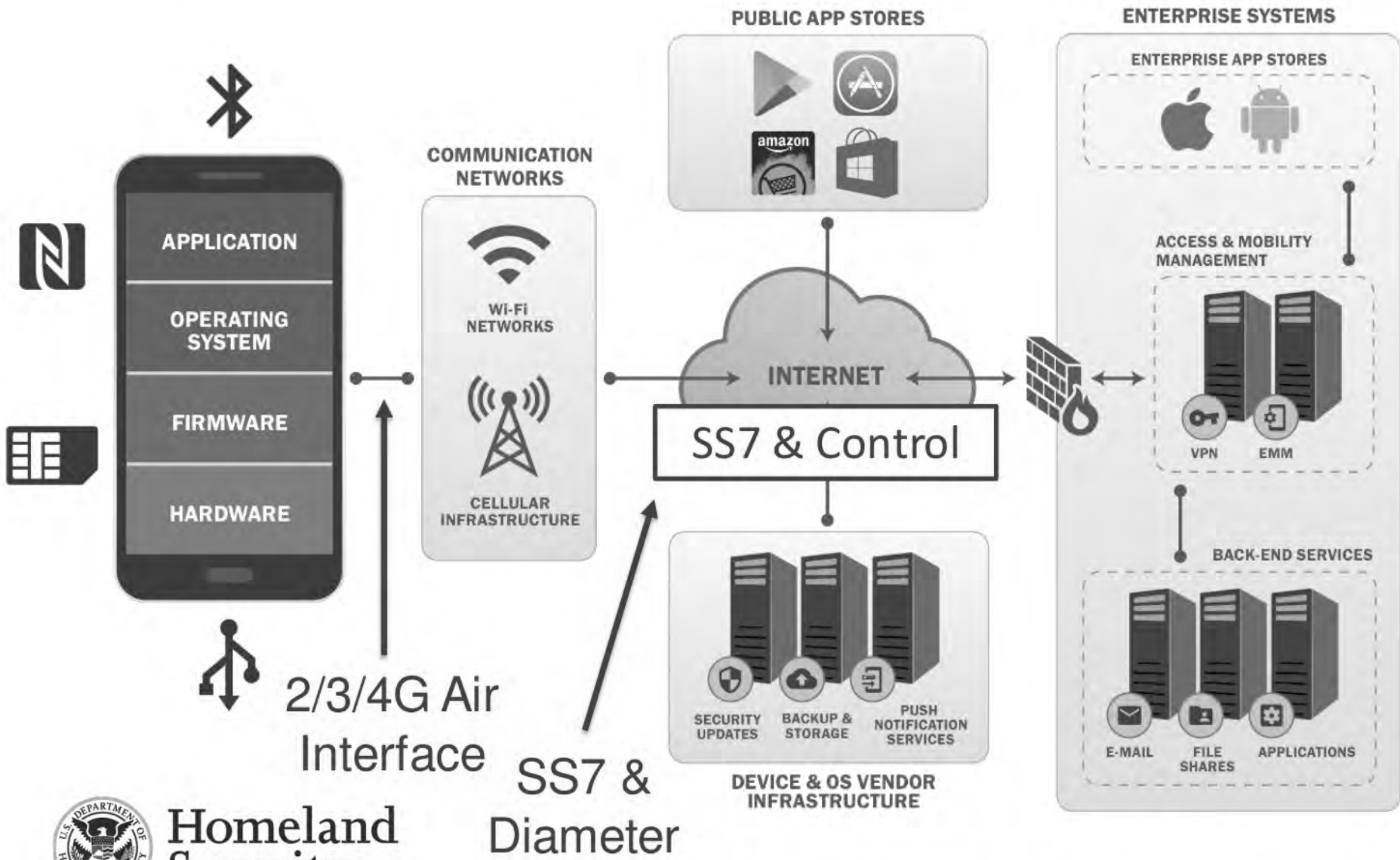
National Coordinating Center for Communications

- NCC is a joint government and industry partnership that coordinates efforts to protect, restore, and reconstitute communications infrastructures
- White House designated the NCC as the Information Sharing & Analysis Center (ISAC) for communications
- **The NCC facilitates the exchange of vulnerability, threat, and mitigation information amongst government and industry partners**



Homeland Security

Mobile Ecosystem & the focus of this brief



2/3/4G Air Interface
SS7 & Diameter



Homeland Security