From: VonBostel, Richard A (JMD)
Subject: RE: (OLA WF112027) OLP Tyrangiel Draft Testimony for a 10-21-15 hearing re Examining Law Enforcement Use of Cell Phone Tracking Devices
To: Klimavicz, Joseph (JMD); Haas, Michael W (JMD)
Cc: Cantilena, Jennifer (JMD); Schlemmer, Maxwell A. (JMD)
Sent: October 14, 2015 11:27 AM (UTC-04:00)
Attached: Draft SFR Tyrangiel OLP version_SROcomments.docx

(b)(5) per JMD

We'll be down at FBI in Stafford this afternoon, with (b)(6), (7)(C) per FBI visiting the FBI Video Surveillance Unit. (so won't be as reachable as usual for a while)

Rich

From: Klimavicz, Joseph (JMD)
Sent: Wednesday, October 14, 2015 9:25 AM
To: Haas, Michael W (JMD); VonBostel, Richard A (JMD)
Cc: Cantilena, Jennifer (JMD); Schlemmer, Maxwell A. (JMD)
Subject: FW: (OLA WF112027) OLP Tyrangiel Draft Testimony for a 10-21-15 hearing re Examining Law Enforcement Use of Cell Phone Tracking Devices

Rich, Michael,

Please let me know by COB today if you have any comments on the attached draft testimony. Thx, Joe

---

From: (b) (6) (OLA)
Sent: Friday, October 09, 2015 4:09 PM
To: Allen, Michael (JMD DAAG); Atwell, Tonya M (JMD); Cantilena, Jennifer (JMD); Cvrkel, Marny (JMD); Deeley, Kevin (JMD); Faulkner, Lila (JMD); Foltz, Robin (JMD); Gary, Arthur (JMD); Kleppinger, Eric (JMD); Klimavicz, Joseph (JMD); Lauria, Jolene A (JMD); Lofthus, Lee J (JMD); Long, Mariana (JMD); Miguel, Amy (JMD); Plante, Jeanette (JMD); Rodgers, Janice (JMD); Schlemmer, Maxwell A. (JMD); Schwartz, Christine (JMD); Sims, Steven (JMD); Snell, Scott (JMD); Sutton, Jeffrey (JMD); Ward, Lisa (JMD); Davis, Valorie A (OLP); Matthews, Matrina (OLP); White, Cleo (OLP); Boynton, Brian (OLC); Datla, Kirti (OLC); Forrester, Nate (OLC); McKenzie, Troy (OLC); Nitze, Jane (OLC); policy, civil (CIV); Brink, David; Hendley, Scott; Lofton, Betty; Opl, Legislation; Wroblewski, Jonathan; (b)(6), (7)(C) per EOUSA; (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (IR) (FBI); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); Strait, Matthew J. (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); ATF; (b)(7)(E) per ATF @atf.gov; (b)(6) per ATF (ATF); (b)(6) per ATF (ATF); (b)(6), (7)(C) per BOP (BOP); Dawson, Christie (USMS); Oliver, Ashley (USMS); Bernhardt, Gena; Brien, Peter; Carradini, Rosemary Cavanagh; Darden, Silas; Johnson, Anna; Morrow, Meg; Scott, Sabrina N.; Searby, Susan; Solomon, Amy; Spector, Adam T
Cc: (b) (6) (OLA); Williams, Elliot (OLA); (b) (6) (OLA); Dix, Melanie (ODAG); Jain, Samir (ODAG); Tomney, Brian (ODAG); Bullock, Bob (A2J)
Subject: (OLA WF112027) OLP Tyrangiel Draft Testimony for a 10-21-15 hearing re Examining Law Enforcement Use of Cell Phone Tracking Devices

Please provide comments to (b) (6), OLA, no later than 10am 10/14/15.

From: Schlemmer, Maxwell A. (JMD)
Subject: RE: OLA Wkflow 112027, Cell Phone Tracking Devices - OLP (Tyrangiel) Tstmny
To: (b) (6) (OLA)
Cc: Klimavicz, Joseph (JMD); Cantilena, Jennifer (JMD); VonBostel, Richard A (JMD); Haas, Michael W (JMD)
Sent: October 14, 2015 11:30 AM (UTC-04:00)
Attached: Draft SFR Tyrangiel OLP version_SROcomments.docx
(b) (6)

Comments from JMD/CIO are noted in the attached version.

Thanks,
Max Schlemmer

From: (b) (6) (OLA)
Sent: Wednesday, October 14, 2015 11:11 AM
To: Atwell, Tonya M (JMD); Cantilena, Jennifer (JMD); Deeley, Kevin (JMD); Klimavicz, Joseph (JMD); Schlemmer, Maxwell A. (JMD); policy, civil (CIV); (b)(6), (7)(C) per EOUSA ; (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (IR) (FBI); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); (b)(6), (7)(C), (7)(E) per DEA (DEA); Darden, Silas; Johnson, Anna; Morrow, Meg; Scott, Sabrina N.; Searby, Susan; Solomon, Amy; Spector, Adam T
Cc: Fried, Hannah (OLP); Wade Tyson, Jill C (OLA)
Subject: OLA Wkflow 112027, Cell Phone Tracking Devices - OLP (Tyrangiel) Tstmny

Any comment on this item (due at 10 a.m.)?

JMD/CIO
CIV
EOUSA
FBI
DEA
OJP

From: Tocci, Steven (JMD)
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)
To: VonBostel, Richard A (JMD)
Sent: June 29, 2018 3:59 PM (UTC-04:00)

I think we can wait until Monday

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: VonBostel, Richard A (JMD)
Sent: Friday, June 29, 2018 3:58 PM
To: Tocci, Steven (JMD) <(b)(6) per JMD >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Yup, let's discuss on Monday, unless you think it warrants attention today(?).

From: Tocci, Steven (JMD)
Sent: Friday, June 29, 2018 2:55 PM
To: VonBostel, Richard A (JMD) <(b)(6) per JMD >
Subject: FW: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Do you want to discuss this Monday? If needed I can send out an additional email to the components.

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: Freeman, Lindsey (OLP)
Sent: Friday, June 29, 2018 2:50 PM
To: Tocci, Steven (JMD) <(b)(6) per JMD >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Pre-decisional and Deliberative
DRAFT

From: Freeman, Lindsey (OLP)
Subject: Re: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)
To: Tocci, Steven (JMD)
Cc: VonBostel, Richard A (JMD); Rothenberg, Laurence E (OLP); Pazur, Shannon (OLP)
Sent: July 10, 2018 9:49 AM (UTC-04:00)

Thanks, Steve. I am out at a meeting until this afternoon but I will reach out when I am back.

Sent from my iPhone

On Jul 10, 2018, at 9:25 AM, Tocci, Steven (JMD) <(b)(6) per JMD > wrote:

From: Freeman, Lindsey (OLP)
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)
To: Tocci, Steven (JMD)
Cc: VonBostel, Richard A (JMD)
Sent: July 11, 2018 10:34 AM (UTC-04:00)

Thanks so much! Really appreciate it. Look forward to talking then.

Best,
Lindsey

From: Tocci, Steven (JMD)
Sent: Wednesday, July 11, 2018 10:32 AM
To: Freeman, Lindsey (OLP) <(b) (6) >
Cc: VonBostel, Richard A (JMD) <(b)(6) per JMD >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Lindsey,

No worries. 3:30 pm time would be better.

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: Freeman, Lindsey (OLP)
Sent: Wednesday, July 11, 2018 10:30 AM
To: Tocci, Steven (JMD) <(b)(6) per JMD >
Cc: VonBostel, Richard A (JMD) <(b)(6) per JMD >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Hi Steve,

Apologies! (b) (6) I have a meeting that ends at 3:30. I could do 2:30 or after 3:30 pm. Again – sorry!

Thanks for understanding!

Best,
Lindsey

From: Tocci, Steven (JMD)
Sent: Wednesday, July 11, 2018 10:29 AM
To: Freeman, Lindsey (OLP) <(b) (6) >
Cc: VonBostel, Richard A (JMD) <(b)(6) per JMD >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Let's shoot for 3pm.

Call in info below.
(b)(6) per JMD

(b)(6) per JMD

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: Freeman, Lindsey (OLP)
Sent: Wednesday, July 11, 2018 10:24 AM
To: Tocci, Steven (JMD) <(b)(6) per JMD >
Cc: VonBostel, Richard A (JMD) <(b)(6) per JMD >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Hi Steve,

Completely understand, not a problem. Unfortunately, 11:30 is not going to work for me. Could we do this afternoon? After 3 pm would be best if that works.

Thanks,
Lindsey

From: Tocci, Steven (JMD)
Sent: Wednesday, July 11, 2018 10:08 AM
To: Freeman, Lindsey (OLP) <(b) (6) >
Cc: VonBostel, Richard A (JMD) <(b)(6) per JMD >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Hi Lindsey,

Our afternoon was slammed. We were at OMB until 530pm yesterday. How is 1130 today? Call in info below.

(b)(6) per JMD

(b)(6) per JMD

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation

Mobile (b)(6) per JMD
(b)(6) per JMD

From: Freeman, Lindsey (OLP)
Sent: Tuesday, July 10, 2018 4:09 PM
To: Tocci, Steven (JMD) <(b)(6) per JMD >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Hi Steve,

My apologies; today has been a bit crazy. But I would like to talk about (b) (5) . Would it be possible to get something on the calendar for tomorrow? I'm free from 11:30 – 4 pm and then again after 5 pm.

Best,
Lindsey

From: Tocci, Steven (JMD)
Sent: Tuesday, July 10, 2018 9:26 AM
To: Freeman, Lindsey (OLP) <(b) (6) >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Lindsey,

I have compiled all of the component responses in one document. (b)(5) per JMD If you have any questions, please give me a call.

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: Freeman, Lindsey (OLP)
Sent: Monday, July 9, 2018 3:36 PM
To: Tocci, Steven (JMD) <(b)(6) per JMD >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Thank you, Steve. We will review and let you know if we have any follow-up questions.

Best,
Lindsey

From: Tocci, Steven (JMD)
Sent: Monday, July 9, 2018 3:34 PM
To: Freeman, Lindsey (OLP) <(b) (6) >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Attached are the components responses to the additional questions. I am sti l working on the summary. If you have any questions please give me a call.

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: Freeman, Lindsey (OLP)
Sent: Monday, July 2, 2018 1:04 PM
To: Tocci, Steven (JMD) <(b)(6) per JMD >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Hi Steve,

Thanks very much. If we don't talk, have a nice holiday!

Best,
Lindsey

Lindsey Freeman
Counsel
Office of Legal Policy
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
Office: (b) (6)
Cell: (b) (6)
(b) (6)

From: Tocci, Steven (JMD)
Sent: Monday, July 2, 2018 12:36 PM
To: Freeman, Lindsey (OLP) <(b) (6) >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: RE: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

Lindsey,

Thank you again. I will keep you informed on the progress.

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: Freeman, Lindsey (OLP)
Sent: Friday, June 29, 2018 2:50 PM
To: Tocci, Steven (JMD) <(b)(6) per JMD >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: CSS Report - Follow-up (Pre-decisional and Deliberative; DRAFT)

From: Freeman, Lindsey \(OLP\)
Subject: RE: Draft CSS Congressional Report
To: Tocci, Steven \(JMD\); VonBostel, Richard A \(JMD\)
Cc: Rothenberg, Laurence E \(OLP\); Pazur, Shannon \(OLP\); Crytzer, Katherine \(OLP\)
Sent: July 19, 2018 7:38 PM (UTC-04:00)
Attached: CSS Report.2017.DRAFT.v5.docx

Pre-decisional and Deliberative
DRAFT

Steve and Rich,

First of all – thank you VERY much. The draft was incredibly helpful. Please see our revisions attached. As you'll note, there are a few questions highlighted in blue that we would like to discuss. Moreover, we would appreciate your review to make sure everything is still aligned with your understanding from the components.

Would it be possible to set up a call tomorrow (7/20) or Monday (7/23) to discuss?

Best,
Lindsey

From: Tocci, Steven (JMD)
Sent: Tuesday, July 17, 2018 5:06 PM
To: Freeman, Lindsey (OLP) <(b) (6) >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Subject: Draft CSS Congressional Report

I have attached our draft. Please let me know if you have any questions.

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD
(b)(6) per JMD

From: Tocci, Steven \(JMD\)
Subject: FW: Cell-Site Simulator Report
To: Bargeron, Terran \(JMD\)
Sent: September 10, 2018 11:36 AM (UTC-04:00)
Attached: 20180817 FINALCSSReportExecSec.docx, 20180817DRAFTCSSReportTransmittalLetterOLA.docx

Here is the CSS Congressional Report.

Thanks
Steve

U//FOUO//LES

Steven Tocci
DOJ/JMD – Spectrum Relocation
Mobile (b)(6) per JMD

From: VonBostel, Richard A (JMD)
Sent: Friday, September 7, 2018 11:46 AM
To: Tocci, Steven (JMD) <(b)(6) per JMD >
Subject: FW: Cell-Site Simulator Report

Of course I found it right after I called you!

From: Freeman, Lindsey (OLP)
Sent: Tuesday, August 21, 2018 9:53 AM
To: Tocci, Steven (JMD) <(b)(6) per JMD >; VonBostel, Richard A (JMD) <(b)(6) per JMD >
Cc: Rothenberg, Laurence E (OLP) <(b) (6) >; Pazur, Shannon (OLP) <(b) (6) >
Subject: Cell-Site Simulator Report

Hi Steve and Richard,

Please see attached the final CSS Report and the final transmittal letter to the Hill. Thank you both so much for all your help. It was a true pleasure working with you.

Best,
Lindsey

Lindsey Freeman
Counsel
Office of Legal Policy
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
Office: (b) (6)
Cell: (b) (6)
(b) (6)

Fiscal Year 2017 Department of Justice Cell-Site Simulator Technology Use and Compliance Report

Introduction

The House and Senate Committees on Appropriations directed the Department of Justice (DOJ or Department) to submit this report detailing the Department's use of cell-site simulator (CSS) technology and its compliance with the Department's CSS policy. On September 3, 2015, the Department established a policy regarding its use of CSS technology (the "Policy"). This Policy—and thus this report—only "applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations."[1] The Department recognized that CSS technology supports critical public safety objectives, including apprehending fugitives, locating kidnapping victims, and assisting in drug investigations. In addition, the technology must be used responsibly, consistent with the requirements and protections of the Constitution and applicable statutory authorities.

The Policy covers all four DOJ law enforcement components that use CSS technology—the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), and the U.S. Marshals Service (USMS).

As discussed in more detail below, based on records kept by DOJ's law enforcement components, DOJ followed the September 3, 2015 Policy in all CSS deployments in Fiscal Year (FY) 2017. Deployments were initiated only after following the appropriate process, i.e., obtaining a search warrant and court authorization under the Pen Register Statute or pursuant to lawful emergency procedures. As directed in the Policy, CSS devices were configured only as pen registers and were not used to collect the content of any communications or subscriber account information. Each law enforcement component has also developed an extensive training program for its CSS operators and, as required by the Policy, only personnel trained by qualified experts may deploy CSS equipment. Finally, the Department has adopted rigorous practices for handling and retaining data, as well as auditing the use of CSS technology, in accordance with the Policy.

Background

Law enforcement uses CSS technology "to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity."[2] This technology is "one tool among many" used by law enforcement and "is deployed only in the fraction of cases in which the capability is best suited to achieve public safety objectives."[3]

[1] Dep't of Justice, *Department of Justice Guidance: Use of Cell-Site Simulator Technology* 1 n.1 (Sept. 3, 2015) (hereinafter Policy). The Policy notes separately, "[w]hen acting pursuant to the Foreign Intelligence Surveillance Act, Department of Justice components will make a probable-cause based showing and appropriate disclosures to the court in a manner that is consistent with the guidance set forth in this policy." *Id.*
[2] *Id.* at 1.
[3] *Id.*

As described in the Policy, a CSS acts as a cell tower. In response to the signals emitted by the simulator, cellular devices identify the simulator as the most attractive cell tower in the area and, consistent with industry standard protocols, transmit identifying signals to the simulator to enable communication with the tower. The signals can then be used to identify the devices. Cell-site simulators receive and use an industry standard unique identifying number assigned by a device manufacturer or cellular network provider.[4] When used to locate a known cellular device, a cell-site simulator receives the unique identifying numbers from multiple devices near the simulator. Once the simulator identifies the target device, however, it will obtain the signaling information only for that particular device. If a CSS is used to identify an unknown device, the simulator obtains signaling information from non-target devices within the vicinity for the limited purpose of distinguishing the target device.[5]

While law enforcement uses CSS technology to acquire the identifying information from cellular devices, this information is limited. Moreover, with respect to location information, CSS devices do not function as global positioning system locators, as they do not obtain or download any location information from a subject device or its applications; instead, they acquire only the relative signal strength and general direction of a subject's cellular device.[6] According to the Policy, CSS used by the Department must be configured as pen registers, and thus may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3).[7]

Department's Use of CSS Technology in Fiscal Year 2017

As noted in the September 3, 2015 Policy, "[t]he use of cell-site simulators is permitted only as authorized by law and policy."[8] Accordingly, except in rare situations (discussed in more detail below), DOJ law enforcement components must obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, or the applicable state equivalent, to deploy CSS technology.[9] In addition, components must concurrently obtain a pen register order or include in their warrant all information required by statute to be included in a pen register order. Every Department CSS deployment in FY 2017 complied with the Policy and was initiated only after having followed the appropriate legal process. CSS devices deployed by the Department during FY 2017 were not configured to collect content.

According to the Policy, "[e]ach division or district office shall report to its agency headquarters annual records reflecting the total number of times a cell-site simulator is deployed in the jurisdiction."[10] For FY 2017, those numbers are as follows:

[4] *Id*. at 2.
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.* at 3.
[9] *Id.*
[10] *Id.* at 7.

Table 1: FY 2017 CSS deployments

FBI	ATF	DEA	USMS	Total DOJ
(b)(7)(E) per FBI	(b)(7)(E) per ATF	(b)(7)(E) per DEA	(b)(7)(E) per USMS	

Each division or district office shall also report "the number of deployments at the request of other agencies, including State or Local law enforcement."[11] These numbers are necessarily a subset of the total number of [redacted] CSS deployments in FY 2017. The number of CSS deployments at the request of other agencies, including state and local partners, in 2017 were:

Table 2: FY 2017 CSS deployments at the request of other agencies, including state and local partners

FBI	ATF	DEA	USMS	Total DOJ
(b)(7)(E) per FBI	(b)(7)(E) per ATF	(b)(7)(E) per DEA	(b)(7)(E) per USMS	

Finally, each division or district office shall report "the number of times the technology is deployed in emergency circumstances."[12] The Policy allows for two circumstances in which DOJ law enforcement components are not required to procure a warrant prior to the use of a CSS: (1) "exigent circumstances under the Fourth Amendment," and (2) "exceptional circumstances."[13]

For "exigent" circumstances, the Policy provides that in circumstances that would qualify for an emergency pen register request pursuant to 18 U.S.C. § 3125 (or the state equivalent), the use of a CSS may be authorized by the same procedure. Pursuant to § 3125, a Deputy Assistant Attorney General (DAAG) or higher-ranking DOJ official may authorize an emergency request for use of pen register and trap and trace devices in certain enumerated emergency situations. For federal cases, the Department's Office of Enforcement Operations (OEO) facilitates the process of procuring high-ranking Department authorization by obtaining the facts from the requesting prosecutor and briefing the relevant DOJ official. Some prosecutors specifically ask for use of a CSS as part of their emergency request. If not specifically requested, OEO may inform the prosecutor that use of a CSS is covered by the emergency authorization. Therefore, authorization for emergency pen register and trap and trace devices may implicitly or explicitly contain a request for use of a CSS. Under the Policy, the prosecutor must seek an appropriate order from the court within 48 hours of installation or use of the emergency pen register trap and trace device. In non-federal cases, the operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.[14] Table 3 describes the instances in which CSS technology was deployed in FY 2017 in "exigent" situations.

[11] *Id.*
[12] *Id.*
[13] *Id.* at 3-4.
[14] *Id.* at 4 n.4.

Table 3: FY 2017 CSS "exigent" deployments

	FBI	ATF	DEA	USMS	Total DOJ
State	(b)(7)(E) per FBI	(b)(7)(E) per ATF	(b)(7)(E) per DEA	(b)(7)(E) per USMS	
Federal					

As illustrated in Table 3, the FBI identified (b)(7)(E) per FBI. DOJ officials facilitated DAAG approval of (b)(7)(E) pe of these, and the other (b)(7)(E) pe instances were requested by state partners and approved using state authority and processes. ATF (b)(7)(E) per ATF. DEA had (b)(7)(E) per "exigent" deployments. (b)(7)(E) per USMS

The Policy also provides for "exceptional circumstances" that may justify the use of a warrantless CSS in another context. As the Policy notes, these exceptions should be "very limited," and require approval from executive-level personnel at the law enforcement agency's headquarters and the relevant U.S. Attorney.[15] Moreover, these situations also require review and approval by a Criminal Division DAAG. The Department is required to track the number of times a CSS is approved for use under "exceptional circumstances."[16] For FY 2017, the Department received zero applications for CSS use for "exceptional circumstances."

Department's Compliance with the September 3, 2015 Policy

The September 3, 2015 Policy outlines particular procedures related to the Department's use of CSS technology, including training, data collection and disposal, and auditing regarding the use of such technology. During FY 2017, the Department was in compliance with the Policy. This section discusses the Department's compliance with these procedures and policies during FY 2017 in more detail below.

Management Controls, Accountability, and Training

The Department has verified that all law enforcement components have specifically trained their CSS operators on the Policy.[17] Moreover, each law enforcement component has developed its own CSS policies, directives, and/or standard operating procedures (SOP), based on the Policy. These materials are available on the components' internal websites. As required, the Policy was also disseminated to all U.S. Attorneys' Offices.

The Policy requires appropriate training and supervision to use CSS technology. Each component has developed an extensive training program for its CSS operators. Qualified experts train personnel who are permitted to deploy CSS equipment. CSS operators are also trained on privacy and

[15] *Id.*
[16] *Id.*
[17] For instance, USMS Technical Operations Group (TOG) and Office of General Counsel personnel have instructed regional and district fugitive task force personnel and other investigators on the Policy and relevant laws, policies, and procedures governing USMS CSS deployments at various trainings and through consultations with the field.

civil liberties as required by DOJ's Policy. Once all of the training is completed, the CSS operators receive a certification.

The Policy also necessitates that each law enforcement agency using CSS technology designate an executive-level point of contact at each division or district office responsible for CSS deployment.[18] Those officials are:

Table 4: Executive-level point of contact for each component, division, or district office

	FBI	ATF	DEA	USMS
Executive-Level Point of Contact	Assistant Director, Operational Technology Division	Deputy Assistant Director, Field Operations (Programs)	Deputy Assistant Administrator, Office of Investigative Technology	Assistant Director, Investigative Operations Division

Moreover, each law enforcement component's specific CSS technology training and supervision protocol is as follows:

FBI: FBI CSS operators are required to complete Operational Technology Division (OTD) specified training and are certified subsequently as FBI CSS operators. The certification process involves computer-based technical and legal training, on-site vendor classroom and practical instruction, legal trends and issues seminars, and a field check ride administered by a senior regional certified CSS operator.[19] All Agents receive privacy and civil liberties training in compliance with FBI policy.

Due to the sensitive-but-unclassified nature of FBI CSS equipment, the capability is law enforcement sensitive and controlled by need-to-know restrictions. Only certified FBI CSS operators may operate the equipment or view the operator's display. No one else, including other agencies' CSS personnel, may have such access absent special authorization from the Unit Chief, Tracking Technology Unit (TTU), OTD.

ATF: All CSS ATF operators receive 64 hours of in-person training, as provided by the manufacturer of the CSS technology. Upon successful completion of training by the manufacturer's qualified experts, each ATF trainee is issued a certificate, at which time ATF considers the trainee an approved ATF CSS operator. Experienced CSS operators receive 32 hours of in-person training, again as provided by the manufacturer of the CSS technology, when a new system upgrade is deployed. During this system upgrade training, the ATF CSS Project Officer is assigned to ensure current Department and ATF policies pertaining to the use of CSS technology are reviewed with the attending

[18] Policy, *supra* note 1, at 3.

[19] FBI CSS basic and advanced training seminars are held multiple times a year, as funding allows. Vendors provide basic training, with advanced training conducted by OTD, the Office of the General Counsel, and certified CSS operators. Basic training consists of two weeks of instruction and practical. Advanced regional training typically consists of a weeklong exercise.

ATF CSS operators. There is also ongoing coordination with ATF's Office of Chief Counsel regarding refresher training on privacy and civil liberties for all current CSS Operators.

DEA: DEA CSS operator is a specialty position; therefore, an employee is only trained to use a CSS device if selected for the program. Prior to operating a CSS, each operator receives a standardized basic operator course and then receives refresher training approximately every two years. DEA's basic CSS operator training course covers the following: (b)(7)(E) per DEA [redacted] (3) CSS operations; and (4) law and policy relating to CSS. DEA instructors currently provide all CSS training, and the minimum training requirement to be certified as a CSS operator is 80 hours. DEA's Office of Chief Counsel reviews CSS instruction and includes a portion on privacy and civil liberties.

USMS: The USMS TOG Chief and the USMS Office of General Counsel maintain agency-wide oversight of the USMS's electronic surveillance (and thus CSS) policies and procedures. Only specially trained personnel assigned to the USMS's Investigative Operations Division (IOD)/TOG trained on the 2015 Policy, technical specifications for CSS deployment, and privacy issues and concerns are authorized to possess or operate a CSS on behalf of the USMS. USMS CSS operators' training, which is administered by qualified/certified TOG Inspectors or other qualified outside instructors, involves approximately 40 hours of initial technical equipment training, followed by 8 hours of annual technical proficiency training. In addition, operators are instructed on how to configure hardware/software to prevent the collection of non-targeted identifiers and minimize interference with communications services provided to non-targeted devices, consistent with the Policy. Only after training is successfully completed are TOG personnel authorized to deploy a CSS operationally as investigative needs support and only when authorized by proper lawful process.

USMS TOG personnel are required to adhere to the USMS electronic surveillance policy and SOP, which, *inter alia*, identifies that TOG employees are the only authorized operators of USMS CSS equipment. In addition to federal and/or state legal parameters for the use of CSS, the SOP also covers the proper operation of, and handling of, CSS and non-target data in order to avoid the collection of non-targeted identifiers to safeguard privacy and civil liberties.[20] USMS TOG personnel must undergo annual "TOG Privacy Training," created by the Office of the General Counsel. The training emphasizes the standards of collection and use and retention of records or other information related to privacy interests or concerns.

Legal Process and Court Orders

The Policy also provides guidance regarding applications for use of CSS.[21] To ensure compliance, the Department's Computer Crime and Intellectual Property Section (CCIPS) has created sample warrant applications for law enforcement components to apply to use CSS. United States

[20] Specifically, the Department's CSS Policy was disseminated to TOG personnel at the time of its issuance, is provided to new TOG personnel, and is incorporated as a hyperlink in the USMS electronic surveillance policy and SOP, which have been made available since April 2016 to all USMS personnel via the USMS's internal website.
[21] Policy, *supra* note 1, at 5.

Attorney's Offices must contact CCIPS before they deviate from the sample warrant applications' technical descriptions concerning cell-site simulators. [22]

For a discussion of the Department's deployment of CSS technology in FY 2017 under the Policy's outlined legal processes and pursuant to the relevant court orders, please see the above section, "Department's Use of CSS Technology in Fiscal Year 2017."

Data Collection, Disposal, and Implementation of an Auditing Program

To ensure that law enforcement practices concerning collection or retention of data are lawful, the Policy outlines particular guidelines to "control the collection, retention, dissemination, and disposition of records that contain personal identifying information," including information collected using a CSS.[23] All DOJ law enforcement components have developed policies and/or SOP regarding deletion of data collected on a CSS deployment and have confirmed that a supervisor verifies deletion of the data. The components expunge data in accordance with the Policy as follows:

> 1. When the equipment is used to locate a known cellular device, [the] data must be deleted as soon as that device is located, and no less than once daily.
>
> 2. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days.
>
> 3. Prior to deploying equipment for another mission, the [law enforcement component's] operator must verify that the equipment has been cleared of any previous operational data.[24]

Specifically, the law enforcement components follow the below procedures:

FBI: FBI requires, upon completion of a CSS operation, that all data related to that operation be purged by the CSS operator from the equipment. Moreover, prior to deploying equipment on another mission, a CSS operator must ensure that the equipment has been cleared of any previous operational data. All CSS operators are required to document that the data stored by the system has been deleted via an electronic record-keeping system implemented for Field Offices. On a monthly basis, the data is collected from the electronic record-keeping system and reviewed by TTU personnel for compliance with the data purge policy.

ATF: The ATF Deputy Assistant Director for Field Operations (Programs) is responsible for ensuring compliance with the Policy's guidelines for data collection and disposal. The ATF CSS operators are required to follow the September 3, 2015 Policy. At the conclusion of each CSS deployment, the operator will complete the After Action Report (AAR) and submit the form to a

[22] *Id.* at 5 n.7.
[23] *Id.* at 6.
[24] *Id.*

program manager within one business day. The AAR includes confirmation that the collected data was purged at the conclusion of the deployment and, if it was not, documentation of the reason for an exception. The AARs are submitted to a CSS Project Officer who is responsible for: (1) ensuring that the content of each submitted AAR adheres to the Department's and ATF's policies, including the September 3, 2015 Policy, and (2) providing oversight of annual statistical data collection and reporting.

DEA: All DEA CSS operators are trained to delete data pursuant to the Policy. DEA CSS operators must document the deletion of data and their supervisors conduct quarterly audits, which are available for review by headquarters, to ensure compliance with the data deletion requirements. A DEA CSS supervisor is informed each time a CSS is deployed.

USMS: USMS requires the deletion of all data at the conclusion of each CSS mission. The deletion is conducted and verified by a USMS TOG employee who has attained the rank of at least first line supervisor.

Auditing the Use of CSS Technology

There were no known instances of non-compliance with the Department-level CSS policy in FY 2017.

Conclusion

As discussed in detail in this report, during FY 2017 the Department's law enforcement components have used CSS technology in a manner that is consistent with the Constitution and relevant legal authorities. By drafting and complying with the September 3, 2015 Policy, the Department has utilized CSS technology to "achieve its public safety and law enforcement objectives . . . in an effective, appropriate, and consistent way."[25]

[25] *Id.* at 7.

117TH CONGRESS
1ST SESSION

S. _____

To amend title 18, United States Code, to regulate the use of cell-site simulators, and for other purposes.

IN THE SENATE OF THE UNITED STATES

_____

_____ introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To amend title 18, United States Code, to regulate the use of cell-site simulators, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as [the "_____ Act of 2021"].

SEC. 2. PROHIBITION ON CELL-SITE SIMULATOR USE.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3119. Cell-site simulators

''(a) PROHIBITION OF USE.—

''(1) IN GENERAL.—Except as provided in subsection (d), it shall be unlawful—

''(A) for any individual or entity to knowingly use a cell-site simulator in the United States; or

''(B) for an element of the intelligence community to use a cell-site simulator outside the United States if the subject of the surveillance is a United States person.

''(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to authorize a law enforcement agency of a governmental entity to use a cell-site simulator outside the United States.

''(b) PENALTY.—Any individual or entity that violates subsection (a)(1) shall be fined not more than $250,000.

''(c) PROHIBITION OF USE AS EVIDENCE.—No information acquired through the use of a cell-site simulator in violation of subsection (a)(1), and no evidence derived therefrom, may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

"(d) EXCEPTIONS.—

"(1) IN GENERAL.—

"(A) WARRANT.—

"(i) IN GENERAL.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity under a warrant issued—

"(I) in accordance with this subparagraph; and

"(II) using the procedures described in, and in accordance with the requirements for executing and returning a warrant under, the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant and execution and return procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title and in accordance with the requirements for executing and returning such a warrant, in accordance with regulations

prescribed by the President) by a court of competent jurisdiction.

"(ii) REQUIREMENTS.—A court may issue a warrant described in clause (i) only if the law enforcement agency—

"(I) certifies that other methods of gathering relevant information have failed;

"(II) demonstrates that other means of surveillance that are less likely to impact third parties have failed, or are likely to fail;

"(III) specifies the area of effect of the cell-site simulator to be used and the time that the cell-site simulator will be in operation; and

"(IV) demonstrates that the requested area of effect and time of operation are the narrowest possible to obtain the necessary information.

"(iii) CONSIDERATIONS.—In considering an application for a warrant described in clause (i), the court shall—

"(I) weigh the need of the government to enforce the law and appre-

hend criminals against the likelihood and impact of any potential negative side effects disclosed by the government under subsection (f);

"(II) consider the interests of the community; and

"(III) not grant a request for a warrant that would put public safety at risk or unreasonably inconvenience the community.

"(B) FOREIGN INTELLIGENCE SURVEILLANCE.—Use of a cell-site simulator by an element of the intelligence community in a manner that is conducted in accordance with title I the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) (including testing or training authorized under paragraph (1) or (3) of section 105(g) of such Act (50 U.S.C. 1805(g)), if any information obtained during such testing or training (including metadata) is destroyed after its use for such testing or training) or section 704(c)(1)(E) of such Act (50 U.S.C. 1881c(c)(1)(E)) shall not be subject to subsection (a)(1).

"(C) EMERGENCY.—Subject to subsection (e), subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity if—

"(i) the law enforcement agency reasonably determines an emergency exists that—

"(I) involves immediate danger of death or serious physical injury to any person; and

"(II) requires use of a cell-site simulator before a warrant can, with due diligence, be obtained;

"(ii) there are grounds upon which a warrant could be entered to authorize such use; and

"(iii) the law enforcement agency applies for a warrant approving such use not later than 48 hours after such use begins, and takes such steps to expedite the consideration of such application as may be possible.

"(2) RESEARCH.—Subsection (a)(1) shall not apply to the use of a cell-site simulator in order to

engage, in good-faith, in research or teaching by a person that is not—

"(A) a law enforcement agency of a governmental entity;

"(B) an element of the intelligence community; or

"(C) acting as an agent thereof.

["(3) PROTECTIVE SERVICES.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by the United States Secret Service as part of protective services provided under section 3056 or as otherwise authorized by law.**]**

["(4) CONTRABAND INTERDICTION BY CORRECTIONAL FACILITIES.—Subsection (a)(1) shall not apply to the use of a contraband interdiction system if—**]**

"(A) the correctional facility or the entity operating the contraband interdiction system for the benefit of the correctional facility has—

"(i) taken reasonable steps to restrict transmissions by the contraband interdiction system to cellular devices physically located within the property of the correctional facility;

"(ii) coordinated the installation and operation of the contraband interdiction system with providers of commercial mobile services and private mobile services that are licensed by the Federal Communications Commission that provide such services in the area in which the correctional facility is located;

"(iii) posted signs around the correctional facility informing visitors and staff about the operation of the contraband interdiction system; and

"(iv) complied with any relevant regulations promulgated by the Federal Communications Commission and policies issued by the National Telecommunications and Information Administration;

"(B) the contraband interdiction system has been configured to permit from any mobile device—

"(i) emergency calls (including 9–1–1 calls);

"(ii) calls to the universal telephone number within the United States for the purpose of the national suicide prevention

and mental health crisis hotline system under designated under paragraph (4) of section 251(e) of the Communications Act (47 U.S.C. 251(e)), as added by the National Suicide Hotline Designation Act of 2020 (Public Law 116–172; 134 Stat. 832); and

''(iii) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71); and

''(C) the correctional facility or the entity operating the contraband interdiction system for the benefit of the correctional facility—

''(i) annually tests and evaluates compliance with subparagraphs (A) and (B) in accordance with best practices, which shall be issued by the Federal Communications Commission; and

''(ii) promptly submits a report to the Federal Communications Commission describing any issues discovered during the testing and evaluation and the steps taken to address the issues.

"(5) TESTING AND TRAINING BY LAW ENFORCEMENT.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity in the normal course of official duties that is not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

"(A) test the capability of electronic equipment, if—

"(i) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

"(ii) the test is limited in extent and duration to that necessary to determine to capability of the equipment;

"(iii) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and

"(iv) the test is for a period of not longer than 90 days, unless the law en-

forcement agency obtains the prior approval of the Attorney General; or

''(B) train law enforcement personnel in the use of electronic surveillance equipment, if—

''(i) it is not reasonable to—

''(I) obtain the consent of the persons incidentally subjected to the surveillance;

''(II) train persons in the course of otherwise authorized law enforcement activities; or

''(III) train persons in the use of such equipment without engaging in surveillance;

''(ii) such surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

''(iii) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

''(6) FCC TESTING.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by the

Federal Communications Commission, or an accredited testing laboratory recognized by the Federal Communications Commission, in order to test the cell-site simulator.

''(7) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to exempt a State or local government from complying with regulations promulgated by the Federal Communications Commission, including the requirement to obtain a license to transmit on spectrum controlled by the Federal Communications Commission.

''(e) TERMINATION OF EMERGENCY USE.—

''(1) IN GENERAL.—A law enforcement agency of a governmental entity shall immediately terminate use of a cell-site simulator under subsection (d)(1)(C) at the earlier of the time the information sought is obtained or the time the application for a warrant is denied.

''(2) WARRANT DENIED.—If an application for a warrant under subsection (d)(1)(C) is denied—

''(A) any information or evidence derived from use of the cell-site simulator shall be—

''(i) subject to subsection (c); and

''(ii) promptly destroyed by the applicable law enforcement agency; and

''(B) the applicable law enforcement agency shall serve an inventory on each person named in the application.

''(f) DISCLOSURES REQUIRED IN APPLICATION.—In any application for a warrant or order authorizing the use of a cell-site simulator under an exception under subsection (d)(1), the governmental entity shall include the following:

''(1) A disclosure of any potential disruption of the ability of the subject of the surveillance or bystanders to use commercial mobile radio services or private mobile services, including using advanced communications services, to make—

''(A) emergency calls (including 9–1–1 calls);

''(B) calls to the universal telephone number within the United States for the purpose of the national suicide prevention and mental health crisis hotline system under designated under paragraph (4) of section 251(e) of the Communications Act (47 U.S.C. 251(e)), as added by the National Suicide Hotline Designation Act of 2020 (Public Law 116–172; 134 Stat. 832);

"(C) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71);

"(D) calls using telecommunications relay services; or

"(E) any other communications or transmissions.

"(2) A certification that the specific model of the cell-site simulator to be used has been inspected by a third party that is an accredited testing laboratory recognized by the Federal Communication Commission to verify the accuracy of the disclosure under paragraph (1).

"(3) A disclosure of the methods and precautions that will be used to minimize disruption, including—

"(A) any limit on the length of time the cell-site simulator can be in continuous operation; and

"(B) any user-defined limit on the transmission range of the cell-site simulator.

"(4) A disclosure as to whether the cell-site simulator will primarily be used at a gathering

where constitutionally protected activity, including speech, will occur.

''(g) LIMIT ON LAWFUL USE NOT CONDUCTED PURSUANT TO WARRANTS AND ORDERS.—Any use of a cell-site simulator that may lawfully be conducted without obtaining a warrant or order issued by a court under a provision of law other than this section may only be carried out using a specific model of a cell-site simulator for which the disclosures required under paragraphs (1) and (2) were included with respect to the specific model in connection with—

''(1) for use by an element of the intelligence community under title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), an application for an order under such Act that was approved; or

''(2) for use by a law enforcement agency of a governmental entity, an application for a warrant—

''(A) under the Federal Rules of Criminal Procedure that was approved by a judge of the judicial district in which the law enforcement agency intends to use the cell-site simulator; or

''(B) using State warrant procedures that was approved by a judge of the State in which

the law enforcement agency intends to use the cell-site simulator.

''(h) MINIMIZATION.—

''(1) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of information obtained through the use of a cell-site simulator under an exception under subsection (d)(1) that pertains to any person who is not an authorized subject of the use.

''(2) USE BY AGENCIES.—If a law enforcement agency of a governmental entity or element of the intelligence community acquires information pertaining to a person who is not an authorized subject of the use of a cell-site simulator under an exception under subsection (d)(1), the law enforcement agency or element of the intelligence community shall minimize the acquisition and retention, and prohibit the dissemination, of the information in accordance with the procedures adopted under paragraph (1).

''(i) DISCLOSURE TO DEFENDANT.—Any information acquired through the operation of a cell-site simulator, or derived from such information, shall be disclosed to the

defendant in any action in which the information is introduced into evidence.

''(j) SCOPE OF COLLECTION.—

''(1) AUTHORIZED USE.—Information collected under this section may only include information identifying nearby electronic devices communicating with the cell-site simulator and the strength and direction of transmissions from those electronic devices.

''(2) COMPLIANCE WITH WIRETAPPING REQUIREMENTS TO OBTAIN CONTENTS.—In the case of any interception of an electronic communication by the cell-site simulator—

''(A) with respect to an interception by a law enforcement agency of a governmental entity, the provisions of chapter 119 shall apply in addition to the provisions of this section; and

''(B) with respect to an interception by an element of the intelligence community, the element of the intelligence community may only conduct the surveillance using the cell-site simulator in accordance with an order authorizing the use issued in accordance with title I of the Foreign Intelligence Surveillance Act of 1978

(50 U.S.C. 1801 et seq.), in addition to complying with the provisions of this section.

''(3) COMPLIANCE WITH TRACKING DEVICE REQUIREMENTS.—If a cell-site simulator is to be used by a law enforcement agency of a governmental entity to track the movement of a person or object, the provisions of section 3117 and rule 41 of the Federal Rules of Criminal Procedure shall apply in addition to the provisions of this section.

''(k) CIVIL ACTION.—Any person subject to an unlawful operation of a cell-site simulator may bring a civil action for appropriate relief (including declaratory and injunctive relief, actual damages, statutory damages of not more than $500 for each violation, and attorney fees) against the person, including a governmental entity, that conducted that unlawful operation before a court of competent jurisdiction.

''(l) DEFINITIONS.—As used in this section—

''(1) the terms defined in section 2711 have, respectively, the definitions given such terms in that section;

''(2) the term 'advanced communications services' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

''(3) the term 'cell-site simulator' means any device that functions as a base station for commercial mobile services or private mobile services and that identifies, locates, or intercepts transmissions from cellular devices for purposes other than providing ordinary commercial mobile services or private mobile services;

''(4) the term 'commercial mobile radio service' has the meaning given that term in section 20.3 of title 47, Code of Federal Regulations, or any successor thereto;

''(5) the term 'contraband interdiction system' means any device that functions as a base station for commercial mobile services or private mobile services for purposes of identifying, locating, or intercepting transmissions from contraband cellular devices in correctional facilities;

''(6) the term 'derived' means, with respect to information or evidence, that the government would not have originally possessed the information or evidence but for the use of a cell-site simulator, and regardless of any claim that the information or evidence is attenuated from the surveillance would inevitably have been discovered, or was subsequently reobtained through other means;

"(7) the term 'electronic communication' has the meaning given that term in section 2510;

"(8) the term 'electronic device' has the meaning given the term 'computer' in section 1030(e);

"(9) the term 'emergency call' has the meaning given that term in section 6001 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1401));

"(10) the term 'intelligence community' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003);

"(11) the term 'mitigation' means the deletion of all information collected about a person who is not the subject of the warrant or investigation;

"(12) the term 'private mobile service' has the meaning given that term in section 332 of the Communications Act of 1934 (47 U.S.C. 332);

"(13) the term 'telecommunications relay service' has the meaning given that term in section 225 of the Communications Act of 1934 (47 U.S.C. 225); and

"(14) the term 'United States person' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).".

(b) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 REQUIREMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) in section 101 (50 U.S.C. 1881), by adding at the end the following:

''(q) 'Cell-site simulator' has the meaning given that term in section 3119 of title 18, United States Code.'';

(2) in section 105 (50 U.S.C. 1805), by adding at the end the following:

''(k)(1) A judge having jurisdiction under section 103 may issue an order under this section that authorizes the use of a cell-site simulator only if the applicant—

''(A) certifies that other methods of gathering relevant information have failed;

''(B) demonstrates that other means of surveillance that are less likely to impact third parties have failed, or are likely to fail;

''(C) specifies the area of effect of the cell-site simulator to be used and the time that the cell-site simulator will be in operation; and

''(D) demonstrates that the requested area of effect and time of operation are the narrowest possible to obtain the necessary information.

"(2) In any application for an order under this section authorizing the use of a cell-site simulator, the applicant shall include the following:

"(A) A disclosure of any potential disruption of the ability of the subject of the surveillance or bystanders to use commercial mobile radio services or private mobile services, including using advanced communications services, to make—

"(i) emergency calls (including 9–1–1 calls);

"(ii) calls to the universal telephone number within the United States for the purpose of the national suicide prevention and mental health crisis hotline system under designated under paragraph (4) of section 251(e) of the Communications Act (47 U.S.C. 251(e)), as added by the National Suicide Hotline Designation Act of 2020 (Public Law 116–172; 134 Stat. 832);

"(iii) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71);

"(iv) calls using telecommunications relay services; or

"(v) any other communications or transmissions.

"(B) A certification that the specific model of the cell-site simulator to be used has been inspected by a third party that is an accredited testing laboratory recognized by the Federal Communications Commission to verify the accuracy of the disclosure under paragraph (1).

"(C) A disclosure of the methods and precautions that will be used to minimize disruption, including—

"(i) any limit on the length of time the cell-site simulator can be in continuous operation; and

"(ii) any user-defined limit on the transmission range of the cell-site simulator.

"(D) A disclosure as to whether the cell-site simulator will primarily be used at a gathering where constitutionally protected activity, including speech, will occur.

"(3) In considering an application for an order under this section that authorizes the use of a cell-site simulator, the court shall—

"(A) weigh the need of the Government to obtain the information sought against the likelihood

and impact of any potential negative side effects disclosed by the Government under paragraph (2);

''(B) consider the interests of the community; and

''(C) not grant a request for an order that would put public safety at risk or unreasonably inconvenience the community.'';

(3) by inserting after section 112 (50 U.S.C. 1812) the following:

''SEC. 113. LIMITS ON USE OF CELL-SITE SIMULATORS WITHOUT AN ORDER.

''(a) IN GENERAL.—As part of any electronic surveillance or other activity in which the Government is authorized to engage under this title without obtaining an order under section 105, the Government may only use a cell-site simulator if the Government has implemented measures that are reasonably likely to limit the collection activities to only facilities owned by the foreign power or agent of a foreign power that is the subject of the electronic surveillance or other activity.

''(b) ORDER REQUIRED.—If it is not possible for the Government to implement measures that make it reasonably likely that the collection activities will be limited to facilities owned by the foreign power or agent of a foreign power that is the subject of the electronic surveillance or

other activities, the Government may only use a cell-site simulator under an authority under this title pursuant to an order issued in accordance with section 105(k).''; and

(4) in section 704(c)(1) (50 U.S.C. 1881c(c)(1))—

(A) in subparagraph (C), by striking ''and'' at the end;

(B) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(E) if the applicant is seeking to use a cell-site simulator (as defined in section 101), the requirements that would apply for the use of a cell-site simulator in the United States under section 105(k) have been satisfied.''.

(c) CONFORMING AMENDMENTS.—

(1) Section 3127 of title 18, United States Code, is amended—

(A) in paragraph (3) by striking ''but such term does not include any'' and inserting ''except such term does not include any cell-site simulator, as that term is defined in section 3119, or''; and

(B) in paragraph (4) by striking ''of any communication'' and inserting ''of any commu-

nication, except such term does not include any cell-site simulator, as that term is defined in section 3119''.

(2) The table of contents for the Foreign Intelligence Surveillance Act of 1978

(d) INSPECTOR GENERAL REPORTS.—

(1) DEFINITION.—In this subsection, the term ''covered Federal entity'' means—

(A) a law enforcement agency of a department or agency of the Federal Government; and

(B) an element of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(2) REPORTS.—The Inspector General of the Department of Justice, the Inspector General of the Department of Homeland Security, and the Inspector General of the Intelligence Community shall annually submit to Congress a joint report, and publish an unclassified version of the report on the website of each such inspector general, on—

(A) the overall compliance of covered Federal entities with this Act and the amendments made by this Act;

(B) the number of applications by covered Federal entities for use of a cell-site simulator

that were applied for and the number that were granted;

(C) the number of emergency uses of a cell-site simulator under section 3119(d)(1)(C) of title 18, United States Code, as added by this Act;

(D) the number of such emergency uses for which a court subsequently issued a warrant authorizing the use and the number of such emergency uses in which an application for a warrant was denied;

(E) which components of a law enforcement agency of a department or agency of the Federal Government are using cell-site simulators and how many are available to that component; and

(F) instances in which a law enforcement agency of a department or agency of the Federal Government made cell-site simulators available to a State or unit of local government.

(3) FORM OF REPORTS.—Each report submitted under paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

Title: To amend title 18, United States Code, to regulate the use of cell-site simulators, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as [the "_____ Act of 2021"].

SEC. 2. PROHIBITION ON CELL-SITE SIMULATOR USE.

(a) In General.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3119. Cell-site simulators

"(a) Prohibition of Use.—

"(1) IN GENERAL.—Except as provided in subsection (d), it shall be unlawful—

"(A) for any individual or entity to knowingly use a cell-site simulator in the United States; or

"(B) for an element of the intelligence community to use a cell-site simulator outside the United States if the subject of the surveillance is a United States person.

"(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to authorize a law enforcement agency of a governmental entity to use a cell-site simulator outside the United States.

"(b) Penalty.—Any individual or entity that violates subsection (a)(1) shall be fined not more than $250,000.

"(c) Prohibition of Use as Evidence.—No information acquired through the use of a cell-site simulator in violation of subsection (a)(1), and no evidence derived therefrom, may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

"(d) Exceptions.—

"(1) IN GENERAL.—

"(A) WARRANT.—

"(i) IN GENERAL.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity under a warrant issued—

"(I) in accordance with this subparagraph; and

"(II) using the procedures described in, and in accordance with the requirements for executing and returning a warrant under, the Federal Rules

of Criminal Procedure (or, in the case of a State court, issued using State warrant and execution and return procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title and in accordance with the requirements for executing and returning such a warrant, in accordance with regulations prescribed by the President) by a court of competent jurisdiction.

"(ii) REQUIREMENTS.—A court may issue a warrant described in clause (i) only if the law enforcement agency—

"(I) certifies that other methods of gathering relevant information have failed;

"(II) demonstrates that other means of surveillance that are less likely to impact third parties have failed, or are likely to fail;

"(III) specifies the area of effect of the cell-site simulator to be used and the time that the cell-site simulator will be in operation; and

"(IV) demonstrates that the requested area of effect and time of operation are the narrowest possible to obtain the necessary information.

"(iii) CONSIDERATIONS.—In considering an application for a warrant described in clause (i), the court shall—

"(I) weigh the need of the government to enforce the law and apprehend criminals against the likelihood and impact of any potential negative side effects disclosed by the government under subsection (f);

"(II) consider the interests of the community; and

"(III) not grant a request for a warrant that would put public safety at risk or unreasonably inconvenience the community.

"(B) FOREIGN INTELLIGENCE SURVEILLANCE.—Use of a cell-site simulator by an element of the intelligence community in a manner that is conducted in accordance with title I the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) (including testing or training authorized under paragraph (1) or (3) of section 105(g) of such Act (50 U.S.C. 1805(g)), if any information obtained during such testing or training (including metadata) is destroyed after its use for such testing or training) or section 704(c)(1)(E) of such Act (50 U.S.C. 1881c(c)(1)(E)) shall not be subject to subsection (a)(1).

"(C) EMERGENCY.—Subject to subsection (e), subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity if—

"(i) the law enforcement agency reasonably determines an emergency exists that—

"(I) involves immediate danger of death or serious physical injury to any person; and

"(II) requires use of a cell-site simulator before a warrant can, with due diligence, be obtained;

"(ii) there are grounds upon which a warrant could be entered to authorize such use; and

"(iii) the law enforcement agency applies for a warrant approving such use not later than 48 hours after such use begins, and takes such steps to expedite the consideration of such application as may be possible.

"(2) RESEARCH.—Subsection (a)(1) shall not apply to the use of a cell-site simulator in order to engage, in good-faith, in research or teaching by a person that is not—

"(A) a law enforcement agency of a governmental entity;

"(B) an element of the intelligence community; or

"(C) acting as an agent thereof.

["(3) PROTECTIVE SERVICES.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by the United States Secret Service as part of protective services provided under section 3056 or as otherwise authorized by law.]

["(4) CONTRABAND INTERDICTION BY CORRECTIONAL FACILITIES.—Subsection (a)(1) shall not apply to the use of a contraband interdiction system if—]

"(A) the correctional facility or the entity operating the contraband interdiction system for the benefit of the correctional facility has—

"(i) taken reasonable steps to restrict transmissions by the contraband interdiction system to cellular devices physically located within the property of the correctional facility;

"(ii) coordinated the installation and operation of the contraband interdiction system with providers of commercial mobile services and private mobile services that are licensed by the Federal Communications Commission that provide such services in the area in which the correctional facility is located;

"(iii) posted signs around the correctional facility informing visitors and staff about the operation of the contraband interdiction system; and

"(iv) complied with any relevant regulations promulgated by the Federal Communications Commission and policies issued by the National Telecommunications and Information Administration;

"(B) the contraband interdiction system has been configured to permit from any mobile device—

"(i) emergency calls (including 9–1–1 calls);

"(ii) calls to the universal telephone number within the United States for the purpose of the national suicide prevention and mental health crisis hotline system under designated under paragraph (4) of section 251(e) of the Communications Act (47 U.S.C. 251(e)), as added by the National Suicide Hotline Designation Act of 2020 (Public Law 116–172; 134 Stat. 832); and

"(iii) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71); and

"(C) the correctional facility or the entity operating the contraband interdiction system for the benefit of the correctional facility—

"(i) annually tests and evaluates compliance with subparagraphs (A) and (B) in accordance with best practices, which shall be issued by the Federal Communications Commission; and

"(ii) promptly submits a report to the Federal Communications Commission describing any issues discovered during the testing and evaluation and the steps taken to address the issues.

"(5) TESTING AND TRAINING BY LAW ENFORCEMENT.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity in the normal course of official duties that is not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

"(A) test the capability of electronic equipment, if—

"(i) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

"(ii) the test is limited in extent and duration to that necessary to determine to capability of the equipment;

"(iii) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and

"(iv) the test is for a period of not longer than 90 days, unless the law enforcement agency obtains the prior approval of the Attorney General; or

"(B) train law enforcement personnel in the use of electronic surveillance equipment, if—

"(i) it is not reasonable to—

"(I) obtain the consent of the persons incidentally subjected to the surveillance;

"(II) train persons in the course of otherwise authorized law enforcement activities; or

"(III) train persons in the use of such equipment without engaging in surveillance;

"(ii) such surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

"(iii) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

"(6) FCC TESTING.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by the Federal Communications Commission, or an accredited testing laboratory recognized by the Federal Communications Commission, in order to test the cell-site simulator.

"(7) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to exempt a State or local government from complying with regulations promulgated by the Federal Communications Commission, including the requirement to obtain a license to transmit on spectrum controlled by the Federal Communications Commission.

"(e) Termination of Emergency Use.—

"(1) IN GENERAL.—A law enforcement agency of a governmental entity shall immediately terminate use of a cell-site simulator under subsection (d)(1)(C) at the earlier of the time the information sought is obtained or the time the application for a warrant is denied.

"(2) WARRANT DENIED.—If an application for a warrant under subsection (d)(1)(C) is denied—

"(A) any information or evidence derived from use of the cell-site simulator shall be—

"(i) subject to subsection (c); and

"(ii) promptly destroyed by the applicable law enforcement agency; and

"(B) the applicable law enforcement agency shall serve an inventory on each person named in the application.

"(f) Disclosures Required in Application.—In any application for a warrant or order authorizing the use of a cell-site simulator under an exception under subsection (d)(1), the governmental entity shall include the following:

"(1) A disclosure of any potential disruption of the ability of the subject of the surveillance or bystanders to use commercial mobile radio services or private mobile services, including using advanced communications services, to make—

"(A) emergency calls (including 9–1–1 calls);

"(B) calls to the universal telephone number within the United States for the purpose of the national suicide prevention and mental health crisis hotline system under designated under paragraph (4) of section 251(e) of the Communications Act (47 U.S.C. 251(e)), as added by the National Suicide Hotline Designation Act of 2020 (Public Law 116–172; 134 Stat. 832);

"(C) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71);

"(D) calls using telecommunications relay services; or

"(E) any other communications or transmissions.

"(2) A certification that the specific model of the cell-site simulator to be used has been inspected by a third party that is an accredited testing laboratory recognized by the Federal Communication Commission to verify the accuracy of the disclosure under paragraph (1).

"(3) A disclosure of the methods and precautions that will be used to minimize disruption, including—

"(A) any limit on the length of time the cell-site simulator can be in continuous operation; and

"(B) any user-defined limit on the transmission range of the cell-site simulator.

"(4) A disclosure as to whether the cell-site simulator will primarily be used at a gathering where constitutionally protected activity, including speech, will occur.

"(g) Limit on Lawful Use Not Conducted Pursuant to Warrants and Orders.—Any use of a cell-site simulator that may lawfully be conducted without obtaining a warrant or order issued by a court under a provision of law other than this section may only be carried out using a specific model of a cell-site simulator for which the disclosures required under paragraphs (1) and (2) were included with respect to the specific model in connection with—

"(1) for use by an element of the intelligence community under title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), an application for an order under such Act that was approved; or

"(2) for use by a law enforcement agency of a governmental entity, an application for a warrant—

"(A) under the Federal Rules of Criminal Procedure that was approved by a judge of the judicial district in which the law enforcement agency intends to use the cell-site simulator; or

"(B) using State warrant procedures that was approved by a judge of the State in which the law enforcement agency intends to use the cell-site simulator.

"(h) Minimization.—

"(1) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of information obtained through the use of a cell-site simulator under an exception under subsection (d)(1) that pertains to any person who is not an authorized subject of the use.

"(2) USE BY AGENCIES.—If a law enforcement agency of a governmental entity or element of the intelligence community acquires information pertaining to a person who is not an authorized subject of the use of a cell-site simulator under an exception under subsection (d)(1), the law enforcement agency or element of the intelligence community shall minimize the acquisition and retention, and prohibit the dissemination, of the information in accordance with the procedures adopted under paragraph (1).

"(i) Disclosure to Defendant.—Any information acquired through the operation of a cell-site simulator, or derived from such information, shall be disclosed to the defendant in any action in which the information is introduced into evidence.

"(j) Scope of Collection.—

"(1) AUTHORIZED USE.—Information collected under this section may only include information identifying nearby electronic devices communicating with the cell-site

simulator and the strength and direction of transmissions from those electronic devices.

"(2) COMPLIANCE WITH WIRETAPPING REQUIREMENTS TO OBTAIN CONTENTS.—In the case of any interception of an electronic communication by the cell-site simulator—

"(A) with respect to an interception by a law enforcement agency of a governmental entity, the provisions of chapter 119 shall apply in addition to the provisions of this section; and

"(B) with respect to an interception by an element of the intelligence community, the element of the intelligence community may only conduct the surveillance using the cell-site simulator in accordance with an order authorizing the use issued in accordance with title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), in addition to complying with the provisions of this section.

"(3) COMPLIANCE WITH TRACKING DEVICE REQUIREMENTS.—If a cell-site simulator is to be used by a law enforcement agency of a governmental entity to track the movement of a person or object, the provisions of section 3117 and rule 41 of the Federal Rules of Criminal Procedure shall apply in addition to the provisions of this section.

"(k) Civil Action.—Any person subject to an unlawful operation of a cell-site simulator may bring a civil action for appropriate relief (including declaratory and injunctive relief, actual damages, statutory damages of not more than $500 for each violation, and attorney fees) against the person, including a governmental entity, that conducted that unlawful operation before a court of competent jurisdiction.

"(l) Definitions.—As used in this section—

"(1) the terms defined in section 2711 have, respectively, the definitions given such terms in that section;

"(2) the term 'advanced communications services' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

"(3) the term 'cell-site simulator' means any device that functions as a base station for commercial mobile services or private mobile services and that identifies, locates, or intercepts transmissions from cellular devices for purposes other than providing ordinary commercial mobile services or private mobile services;

"(4) the term 'commercial mobile radio service' has the meaning given that term in section 20.3 of title 47, Code of Federal Regulations, or any successor thereto;

"(5) the term 'contraband interdiction system' means any device that functions as a base station for commercial mobile services or private mobile services for purposes of identifying, locating, or intercepting transmissions from contraband cellular devices in correctional facilities;

"(6) the term 'derived' means, with respect to information or evidence, that the government would not have originally possessed the information or evidence but for the use of a cell-site simulator, and regardless of any claim that the information or evidence is attenuated from the surveillance would inevitably have been discovered, or was subsequently reobtained through other means;

"(7) the term 'electronic communication' has the meaning given that term in section

2510;

"(8) the term 'electronic device' has the meaning given the term 'computer' in section 1030(e);

"(9) the term 'emergency call' has the meaning given that term in section 6001 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1401));

"(10) the term 'intelligence community' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003);

"(11) the term 'mitigation' means the deletion of all information collected about a person who is not the subject of the warrant or investigation;

"(12) the term 'private mobile service' has the meaning given that term in section 332 of the Communications Act of 1934 (47 U.S.C. 332);

"(13) the term 'telecommunications relay service' has the meaning given that term in section 225 of the Communications Act of 1934 (47 U.S.C. 225); and

"(14) the term 'United States person' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).".

(b) Foreign Intelligence Surveillance Act of 1978 Requirements.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) in section 101 (50 U.S.C. 1881), by adding at the end the following:

"(q) 'Cell-site simulator' has the meaning given that term in section 3119 of title 18, United States Code.";

(2) in section 105 (50 U.S.C. 1805), by adding at the end the following:

"(k)(1) A judge having jurisdiction under section 103 may issue an order under this section that authorizes the use of a cell-site simulator only if the applicant—

"(A) certifies that other methods of gathering relevant information have failed;

"(B) demonstrates that other means of surveillance that are less likely to impact third parties have failed, or are likely to fail;

"(C) specifies the area of effect of the cell-site simulator to be used and the time that the cell-site simulator will be in operation; and

"(D) demonstrates that the requested area of effect and time of operation are the narrowest possible to obtain the necessary information.

"(2) In any application for an order under this section authorizing the use of a cell-site simulator, the applicant shall include the following:

"(A) A disclosure of any potential disruption of the ability of the subject of the surveillance or bystanders to use commercial mobile radio services or private mobile services, including using advanced communications services, to make—

"(i) emergency calls (including 9–1–1 calls);

"(ii) calls to the universal telephone number within the United States for the purpose of the national suicide prevention and mental health crisis hotline system under

designated under paragraph (4) of section 251(e) of the Communications Act (47 U.S.C. 251(e)), as added by the National Suicide Hotline Designation Act of 2020 (Public Law 116–172; 134 Stat. 832);

"(iii) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71);

"(iv) calls using telecommunications relay services; or

"(v) any other communications or transmissions.

"(B) A certification that the specific model of the cell-site simulator to be used has been inspected by a third party that is an accredited testing laboratory recognized by the Federal Communications Commission to verify the accuracy of the disclosure under paragraph (1).

"(C) A disclosure of the methods and precautions that will be used to minimize disruption, including—

"(i) any limit on the length of time the cell-site simulator can be in continuous operation; and

"(ii) any user-defined limit on the transmission range of the cell-site simulator.

"(D) A disclosure as to whether the cell-site simulator will primarily be used at a gathering where constitutionally protected activity, including speech, will occur.

"(3) In considering an application for an order under this section that authorizes the use of a cell-site simulator, the court shall—

"(A) weigh the need of the Government to obtain the information sought against the likelihood and impact of any potential negative side effects disclosed by the Government under paragraph (2);

"(B) consider the interests of the community; and

"(C) not grant a request for an order that would put public safety at risk or unreasonably inconvenience the community.";

(3) by inserting after section 112 (50 U.S.C. 1812) the following:

"SEC. 113. LIMITS ON USE OF CELL-SITE SIMULATORS WITHOUT AN ORDER.

"(a) In General.—As part of any electronic surveillance or other activity in which the Government is authorized to engage under this title without obtaining an order under section 105, the Government may only use a cell-site simulator if the Government has implemented measures that are reasonably likely to limit the collection activities to only facilities owned by the foreign power or agent of a foreign power that is the subject of the electronic surveillance or other activity.

"(b) Order Required.—If it is not possible for the Government to implement measures that make it reasonably likely that the collection activities will be limited to facilities owned by the foreign power or agent of a foreign power that is the subject of the electronic surveillance or other activities, the Government may only use a cell-site simulator under an authority under this title pursuant to an order issued in accordance with section 105(k)."; and

(4) in section 704(c)(1) (50 U.S.C. 1881c(c)(1))—

(A) in subparagraph (C), by striking "and" at the end;

(B) in subparagraph (D), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following:

"(E) if the applicant is seeking to use a cell-site simulator (as defined in section 101), the requirements that would apply for the use of a cell-site simulator in the United States under section 105(k) have been satisfied.".

(c) Conforming Amendments.—

(1) Section 3127 of title 18, United States Code, is amended—

(A) in paragraph (3) by striking "but such term does not include any" and inserting "except such term does not include any cell-site simulator, as that term is defined in section 3119, or"; and

(B) in paragraph (4) by striking "of any communication" and inserting "of any communication, except such term does not include any cell-site simulator, as that term is defined in section 3119".

(2) The table of contents for the Foreign Intelligence Surveillance Act of 1978

(d) Inspector General Reports.—

(1) DEFINITION.—In this subsection, the term "covered Federal entity" means—

(A) a law enforcement agency of a department or agency of the Federal Government; and

(B) an element of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(2) REPORTS.—The Inspector General of the Department of Justice, the Inspector General of the Department of Homeland Security, and the Inspector General of the Intelligence Community shall annually submit to Congress a joint report, and publish an unclassified version of the report on the website of each such inspector general, on—

(A) the overall compliance of covered Federal entities with this Act and the amendments made by this Act;

(B) the number of applications by covered Federal entities for use of a cell-site simulator that were applied for and the number that were granted;

(C) the number of emergency uses of a cell-site simulator under section 3119(d)(1)(C) of title 18, United States Code, as added by this Act;

(D) the number of such emergency uses for which a court subsequently issued a warrant authorizing the use and the number of such emergency uses in which an application for a warrant was denied;

(E) which components of a law enforcement agency of a department or agency of the Federal Government are using cell-site simulators and how many are available to that component; and

(F) instances in which a law enforcement agency of a department or agency of the Federal Government made cell-site simulators available to a State or unit of local government.

(3) FORM OF REPORTS.—Each report submitted under paragraph (2) shall be submitted in unclassified form, but may include a classified annex.