~~LAW ENFORCEMENT SENSITIVE~~

OFFICE OF INSPECTOR GENERAL

# Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators (REDACTED)

**~~Warning: This document is Law Enforcement Sensitive (LES). Do not distribute or copy this report without the expressed written consent of the Office of Inspector General.~~**

**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

February 23, 2023

MEMORANDUM FOR: The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security

Kimberly A. Cheatle
Director
United States Secret Service

Tae D. Johnson
Acting Director
U.S. Immigration and Customs Enforcement

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2023.02.16 09:06:09 -07'00'

SUBJECT: *Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators* – ~~Law Enforcement Sensitive~~

Attached for your action is our final report, *Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators* – ~~Law Enforcement Sensitive~~. We incorporated the formal comments provided by your office.

The report contains six recommendations aimed at ensuring compliance with statutes and policies governing the use of cell-site simulators and privacy requirements. Your office concurred with all six recommendations. Based on information provided in your response to the draft report, we consider recommendation 6 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, recommendation 6 will be considered open and unresolved.

Based on information provided in your response to the draft report, we consider recommendations 1 through 5 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General of Audits, at (202) 981-6000.

Attachment

~~LAW ENFORCEMENT SENSITIVE~~

# DHS OIG Highlights

## *Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators*

**February 23, 2023**

## Why We Did This Audit

Department of Homeland Security law enforcement components use CSS to provide real-time cellular device locations for investigative purposes. Our objective was to determine whether DHS and its components have developed, updated, and adhered to policies related to the use of CSS.

## What We Recommend

We recommended that the Secret Service and ICE HSI take corrective actions to ensure they use CSS in accordance with Federal statutes and DHS policies.

**For Further Information:**
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

## What We Found

The United States Secret Service and U.S. Immigration and Customs Enforcement, Homeland Security Investigations (ICE HSI) did not always adhere to Federal statute and cell-site simulator (CSS) policies when using CSS during criminal investigations involving exigent circumstances. Separately, ICE HSI did not adhere to Department privacy policies and the applicable Federal privacy statute when using CSS. For the cases we reviewed, the Secret Service and ICE HSI obtained required search warrants for [redacted] CSS uses, respectively. However, the Secret Service and ICE HSI did not always obtain court orders required by CSS policies and Federal statute when using CSS during investigations that included exigent circumstances.

This occurred for two reasons. First, CSS policies do not include sufficiently detailed guidance on working with external law enforcement agencies. Second, the Secret Service and ICE HSI did not correctly interpret CSS policies reflecting the statutory requirement to obtain court orders before using CSS or, in emergency situations, apply for court orders within 48 hours of installing, or beginning to install CSS.

Additionally, ICE HSI did not adhere to DHS' privacy policy and the *E-Government Act of 2002* that require CSS, as a privacy sensitive technology, to have an approved privacy impact assessment (PIA) before its use. According to ICE officials, resource limitations and changes in personnel resulted in a lengthy review and clearance process for a PIA. Although DHS approved an ICE HSI CSS-related PIA in January 2022, prior to this approval, DHS may not have identified and mitigated the privacy risks associated with CSS use.

## DHS Response

DHS concurred with all six recommendations.

## Table of Contents



## Appendixes



## Abbreviations

| | |
|---|---|
| CSS | cell-site simulator |
| HSI | Homeland Security Investigations |
| ICE | U.S. Immigration and Customs Enforcement |
| IT | information technology |
| OGC | DHS Office of the General Counsel |
| PIA | privacy impact assessment |
| PII | personally identifiable information |
| PTA | privacy threshold analysis |
| U.S.C. | United States Code |

## Background

The United States Secret Service and U.S. Immigration and Customs Enforcement (ICE) are two of the Department of Homeland Security's law enforcement components. Collectively, these components' law enforcement missions include investigating narcotics smuggling, human trafficking, gang activity, money laundering, counterfeiting, and other financial crimes. To help conduct their investigations, the Secret Service and ICE Homeland Security Investigations (HSI) leverage cell-site simulators (CSS) to locate, in real time, subjects of criminal investigations and victims based on their cellular device location. A CSS mimics a cellular phone tower by emitting a signal, which cellular devices within range of the CSS identify as the cellular phone tower in the area with the better-quality signal.

Law enforcement officers use CSS to identify both known and unknown cellular devices related to their investigations. First, CSS help officers locate cellular devices with unique identifiers already known to law enforcement. Once the CSS identifies the targeted cellular device, it obtains signaling information related to that specific device. Second, CSS help officers determine the unique identifiers of an unknown device by collecting limited signaling information from other devices in the vicinity. In this case, the CSS obtains signaling information at multiple locations from non-targeted devices in the target's vicinity for the limited purpose of identifying the target device by a process of elimination. The CSS provides relative signal strength and general direction of a subject device. See Figure 1 for a depiction of CSS operation.

**Figure 1. Depiction of CSS Operation**


*Source*: DHS Office of Inspector General analysis of CSS operations

The Secret Service and ICE HSI have used CSS to identify the locations of devices associated with suspects in homicides, financial crimes, and narcotics

cases. For example, the Secret Service used CSS to help locate a device used by an individual suspected of aggravated identity theft, bank, and wire fraud. In another example, ICE HSI used CSS to assist two Federal law enforcement agencies and a local police department, to locate a cellular phone in the possession of an individual with an active arrest warrant for conspiracy to commit murder. In both examples, the individuals were located and taken into custody.

**DHS Policy Governing CSS Use**

The *Department Policy Regarding the Use of Cell-Site Simulator Technology,* Policy Directive 047-02, October 19, 2015 (Policy Directive 047-02)[1] establishes requirements to ensure DHS' use of CSS inside the United States in furtherance of criminal investigations is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including 18 United States Code (U.S.C.) 3121, et seq., *Pen Registers and Trap and Trace Devices* (Pen Register Statute).[2] To ensure compliance with governing authorities, Policy Directive 047-02 incorporates internal controls and accountability requirements, including requirements for obtaining warrants and court orders, as well as data management requirements related to CSS.

Policy Directive 047-02 includes steps to ensure compliance with Constitutional protections afforded by the Fourth Amendment.[3] Specifically, before using CSS, Policy Directive 047-02 requires law enforcement components obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the *Federal Rules of Criminal Procedure.*[4] Policy Directive 047-02 identifies two exceptions to the warrant requirement. In certain situations, warrants are not required when either "exigent" or "exceptional" circumstances exist. "Exigent circumstances" include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice. "Exceptional circumstances" allow for warrantless use of CSS technology when obtaining a

[1] See Appendix C for a copy of *Department Policy Regarding the Use of Cell-Site Simulator Technology,* Policy Directive 047-02, October 19, 2015.
[2] See Appendix D for a copy of 18 U.S.C. 3121, et seq., *Pen Registers and Trap and Trace Devices.*
[3] *United States Constitution, 4th Amendment*: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[4] 18 U.S.C. Appendix, *Federal Rules of Criminal Procedure*, Rule 41. *Search and Seizure.*

search warrant is impracticable, for example when the use of the technology is in furtherance of Secret Service protective duties.[5]

Policy Directive 047-02 mandates that law enforcement components seeking authorization to use cell-site simulator technology adhere to the Pen Register Statute, 18 U.S.C. § 3121, et seq. The Pen Register Statute prohibits installing or using a pen register[6] or a trap and trace device[7] without first obtaining a court order (pen register order). The statute permits using CSS without a pen register order in "emergency" situations if, with due diligence, a court order authorizing such use cannot be obtained beforehand. Examples of emergency situations include immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in Section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year.[8] In some cases, such as the immediate danger of death or serious injury, an "emergency situation" under the Pen Register Statute will also be an "exigent circumstance" under the CSS policies. In emergency situations, the Pen Register Statute requires application for a court order within 48 hours of installing, or beginning to install, CSS. Such emergency use must immediately terminate when the information sought is obtained, when the application for the order is denied, or within 48 hours have lapsed since the installation of the device, whichever is earlier.[9] In emergency situations, the knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).[10]

There are, therefore, *two separate and distinct* considerations associated with obtaining authorization to use CSS. These considerations are (1) the requirements associated with obtaining search warrants, mandated by Policy Directive 047-02 and (2) court orders mandated by the Pen Register Statute and included in Policy Directive 047-02. When Policy Directive 047-02 permits

[5] 18 U.S.C. § 3056; 18 U.S.C. § 3056A.
[6] As defined by the Pen Register Statute, a pen register is a device or process "which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . ." 18 U.S.C § 3127(3).
[7] As defined by the Pen Register Statute, the term "trap and trace device" is a "device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C § 3127(4).
[8] See Appendix D, 18 U.S.C. § 3125(a)(1).
[9] See Appendix D, 18 U.S.C. § 3125(a)(2) and (b).
[10] See Appendix D, 18 U.S.C. § 3125(c).

dispensing with the warrant requirements, the Pen Register Statue must still be followed. Under exigent or exceptional circumstances, defined by Policy Directive 047-02, use of a CSS still must comply with the Pen Register Statute, which ordinarily requires judicial authorization prior to using CSS, based on the government certifying that the information sought is relevant to an ongoing criminal investigation. The knowing installation or use of a pen register device without first obtaining a court order under 18 U.S.C. § 3123 is a criminal violation under 18 U.S.C. § 3121(d).

The internal controls and accountability requirements articulated in Policy Directive 047-02 include first-level supervisor approval prior to deploying CSS technology and second-level supervisor approval for "emergency use" of CSS technology. Additionally, all data collected by the CSS technology during an investigation must be deleted upon mission completion.

In 2017, both the Secret Service and ICE HSI developed component-specific CSS policies incorporating the requirements of Policy Directive 047-02.[11] Given the Secret Service and ICE HSI policies largely mirror Policy Directive 047-02, unless otherwise cited, we refer to the three policies collectively as "CSS policies."

### *E-Government Act of 2002* and DHS Privacy Policies

In addition to the Pen Register Statute, CSS technology is governed by requirements set forth in the *E-Government Act of 2002.*[12] Congress passed the *E-Government Act of 2002*, among other reasons, to ensure sufficient protections for the privacy of personal information. Under Section 208 of the *E-Government Act of 2002*, agencies are required to conduct a privacy impact assessment (PIA) before developing or procuring information technology (IT) that collects, maintains, or disseminates information in an identifiable form.[13]

The DHS Privacy Office (DHS Privacy) has issued policies that provide guidance for preparing a PIA. A PIA describes what information an agency is collecting and why the information is collected; how the information will be used, stored,

[11] *Secret Service Mobile Wireless Investigations Cell-Site Simulator Manual*, January 10, 2017; and *ICE HSI Use of Cell-Site Simulator Technology*, August 31, 2017.
[12] Public Law 107–347.
[13] Office of Management and Budget, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, defines information in identifiable form as "information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

and shared; how the information may be accessed; how the information will be protected from unauthorized use or disclosure; and how long it will be retained. A PIA also provides an analysis of the privacy considerations posed and the steps an agency has taken to mitigate any impact on privacy. DHS Privacy requires, reviews, and approves PIAs on technologies, rulemakings, programs, and activities, regardless of their type or classification, to ensure that privacy considerations and protections are incorporated into all activities of the Department under Section 208 of the *E-Government Act of 2002*, the *Homeland Security Act of 2002*, and other statutes, as applicable.

DHS Privacy's *Privacy Policy and Compliance* instruction and included references[14] (DHS privacy policies) apply throughout DHS regarding the collection, use, maintenance, disclosure, deletion, and destruction of personally identifiable information (PII)[15] and any other activity that impacts the privacy of individuals as determined by the DHS Chief Privacy Officer. DHS privacy policies describe the policies, procedures, and responsibilities to ensure PII is protected from unauthorized use or disclosure, including completion of the privacy threshold analysis (PTA) and PIA process, when required.

DHS Privacy developed the PTA form to help identify when an IT system, technology, rulemaking, program, or pilot project involves PII and to determine whether additional privacy compliance documentation is necessary. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what PII is collected (and from whom) and how that information is used. In completed PTAs, DHS Privacy generally indicates whether the technology is privacy sensitive, whether an existing PIA is sufficient, or a new PIA is required.

## Results of Audit

The Secret Service and ICE HSI did not always adhere to Federal statute and CSS policies when using CSS during investigations involving exigent circumstances. Separately, ICE HSI did not adhere to Department privacy policies and the applicable Federal privacy statute when using CSS. For the cases we reviewed, the Secret Service and ICE HSI obtained required search warrants for [redacted] CSS uses, respectively. However, the Secret Service and ICE HSI did not always obtain court orders as mandated by the Pen Register Statute when using CSS during investigations that included

[14] *Privacy Policy and Compliance, Department of Homeland Security, DHS Directives System Instruction Number: 047-01-001, Revision Number: 00 Issue Date: 07/25/2011.*
[15] DHS Privacy Office defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

exigent circumstances.

This occurred for two reasons. First, CSS policies do not include sufficiently detailed guidance on working with external law enforcement agencies. Second, the Secret Service and ICE HSI did not correctly interpret CSS policies (reflecting Pen Register Statue requirements) that require pen register orders before using CSS or, in emergency situations, applying for court orders within 48 hours of installing, or beginning to install, CSS. Additionally, ICE HSI did not adhere to DHS' privacy policy and the *E-Government Act of 2002* that require CSS, as a privacy sensitive technology, to have an approved PIA before its use. According to ICE officials, resource limitations and changes in personnel resulted in a lengthy review and clearance process for a PIA. Although DHS approved an ICE HSI CSS-related PIA in January 2022, prior to this, without a PIA, DHS may not have identified and mitigated the privacy risks associated with CSS use.

## Secret Service and ICE HSI Did Not Always Adhere to the Pen Register Statute and CSS Policies

The Secret Service and ICE HSI did not always adhere to the Pen Register Statute incorporated into CSS policies. CSS policies establish requirements to ensure CSS use is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute. However, based on our review of the Secret Service and ICE HSI investigations employing CSS in fiscal years 2020 and 2021, we determined that in exigent circumstances, the Secret Service and ICE HSI did not always obtain pen register court orders pursuant to the Pen Register Statute as incorporated into CSS policies. Finally, the Secret Service and ICE HSI did not always document CSS supervisory approval and data deletion to support compliance with CSS policies that require supervisory approval before CSS use and data deletion upon mission completion.

### Secret Service and ICE HSI Did Not Always Obtain Court Orders When Using CSS in Exigent Circumstances

Under normal circumstances,[16] CSS policies require the Secret Service and ICE HSI to obtain a search warrant supported by probable cause prior to using CSS. Secret Service and ICE HSI can either obtain a warrant that includes all information required for a pen register order pursuant to the Pen Register

[16] We use the term "normal circumstances" to describe CSS investigations with deployments not conducted under exigent or exceptional circumstances as defined by CSS policies.

Statute (or state equivalent)[17] or seek a warrant and pen register order concurrently. Under exigent circumstances or emergency situations, Secret Service and ICE HSI must still obtain a court order pursuant to CSS policy incorporating the Pen Register Statute, even when no warrant was obtained.[18] Specifically, during exigent circumstances CSS policies require that the Secret Service[19] and ICE HSI obtain a court order pursuant to the Pen Register Statute, which ordinarily requires judicial authorization before use of the CSS.[20] CSS may be used in an "emergency situation" as defined in the Pen Register Statute[21] if, with due diligence, a court order authorizing such use cannot be obtained beforehand. In some cases, an "emergency situation" under the Pen Register Statute will also be an "exigent circumstance" under the CSS policies, for example when there is an immediate danger of death or serious injury. In emergency situations, the Pen Register Statute[22] and CSS policies require the Secret Service and ICE HSI apply for court orders within 48 hours of installing or beginning to install CSS.[23]

Secret Service CSS Use

We reviewed [redacted] Secret Service investigations from FYs 2020 through 2021, in which a CSS was used. We determined that [redacted] investigations used CSS under normal circumstances for which the Secret Service obtained the required search warrant and complied with CSS policies. However, the Secret Service did not obtain pen register court orders for [redacted] investigations using CSS under exigent circumstances, as required by policy and statute. For these [redacted] investigations, the Secret Service's investigative records defined the CSS use as "emergency/exigent." The investigative records for [redacted] investigations further defined exigent circumstances as the legal authority for using a CSS. In [redacted] investigations, the Secret Service did not provide additional records clarifying the legal authority for using CSS, but according to the Secret Service, the CSS was used for exigent circumstances.

[17] See Appendix D, 18 U.S.C. § 3123.
[18] Generally, a court will issue an order authorizing the installation and use of a pen register device if the court finds that the attorney for the Government, state law enforcement, or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
[19] Secret Service's CSS policy does not explicitly reference 18 U.S.C. § 3121 but does indicate that the use of CSS under exigent circumstances must comply with the Pen Register Statute, which requires a court order before using CSS unless "emergency circumstances" exist.
[20] See Appendix C, Policy Directive 047-02, page 4, *Legal Process & Court Orders*.
[21] 18 USC § 3125(a)(1).
[22] See Appendix D, 18 U.S.C. § 3125 (a)(2).
[23] See Appendix C, Policy Directive 047-02, page 4, *Legal Process & Court Orders, Exigent Circumstances under the Fourth Amendment*.

Of the [redacted] exigent uses of CSS without warrant or court order, [redacted] were conducted by a field office in support of a local law enforcement agency. In these [redacted] instances, the Secret Service explained that, according to the county prosecutor's office, the county judges did not understand why the prosecutor's office sought to file an "emergency pen trap order" and believed it to be unnecessary. Therefore, moving forward, the county prosecutor's office decided it "would not file" emergency pen trap orders following exigent missions. Although Secret Service explained that the prosecutor's office sought to file an "emergency pen trap order" for these investigations, its investigative records did not indicate that the exigent circumstances were also emergencies as defined by the Pen Register Statute and included in CSS policies.

The Pen Register Statute permits CSS use before obtaining a court order if, with due diligence, a court order authorizing such use cannot be obtained beforehand. The "emergency situation" must involve immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year. If those conditions are met, the Pen Register Statute requires application for a court order within 48 hours of installing, or beginning to install, CSS. Yet, the Secret Service did not apply for court orders in these investigations. Since our review, the Secret Service has worked with the county prosecutor to develop a CSS application template for future use to ensure compliance with the Pen Register Statute as incorporated into CSS policies.

In [redacted] examples of exigent use of a CSS, the Secret Service used CSS to support its own operations. [redacted]
According to the Secret Service, the United States Attorney's Office indicated it would not file the emergency pen trap order because the mission involved Secret Service property, was conducted with the Secret Service's consent, and the Secret Service received no data from the carrier. The Secret Service indicated that the CSS use was under exigent circumstances, which, per CSS policies, dispenses with the warrant requirement. However, even if the Secret Service considered this to be an emergency situation as defined in the Pen Register Statute, if a court order cannot be obtained before use, the Pen Register Statute requires that the order issue within 48 hours of installing, or beginning to install, the device. The Secret Service did not obtain or apply for a court order for this investigation.

ICE HSI CSS Use

We reviewed [redacted] ICE HSI investigations from FYs 2020 through 2021, in which a CSS was used. We determined that ICE HSI obtained required search warrants for [redacted] investigations using CSS. Specifically, [redacted] investigations used CSS under normal circumstances for which ICE HSI obtained the required search warrant. ICE HSI records indicated that [redacted] investigations with CSS deployments were for exigent circumstances in support of other Federal or local law enforcement. For [redacted] investigations, ICE HSI obtained search warrants authorizing CSS use. In the other [redacted], ICE HSI did not obtain warrants and was unable to provide evidence it applied for or obtained pen register court orders. [redacted] If these were "emergency situations" and ICE HSI could not obtain a court order prior to using CSS, ICE HSI should have applied for court orders within 48 hours of installing, or beginning to install, CSS, as required by CSS policies reflecting Pen Register Statute requirements. Yet, ICE HSI did not apply for court orders in these [redacted] investigations.[24]

Table 1 summarizes the number of Secret Service and ICE HSI investigations using CSS and number of investigations with and without warrants, court orders, or applications for court orders for deployments in FYs 2020 and 2021.

[24] ICE HSI operated the CSS equipment in support of another agency's investigations and, according to ICE HSI officials, they relied on those agencies to obtain the required judicial authorizations.

**Table 1. Secret Service and ICE HSI Investigations Using a CSS With or Without Associated Warrants, Court Orders, or Applications for Court Orders FYs 2020 and 2021**

| CSS Use with Warrants, Court Orders, or Applications for Orders Within 24 Hours | Component | |
|---|---|---|
| | Secret Service | ICE HSI |
| **Total Investigations Using CSS** | | |
| **Investigations Using CSS Under Normal Circumstances** | | |
| Investigations with warrant authorizing CSS use | | |
| Investigations without warrant authorizing CSS use | | |
| **Investigations Using CSS Under Exigent Circumstances** | | |
| Investigations with warrant or court order authorizing CSS use | | |
| Investigations without court order authorizing CSS use | | |
| **Total Investigations Using CSS Without a Warrant, Court Order, or Application for Court Order** | | |
| CSS used to support component | | |
| CSS used to support other Federal, state, or local law enforcement | | |

*Source*: DHS OIG analysis of Secret Service and ICE HSI investigative records

## CSS Policies are Missing Guidance and Secret Service and ICE HSI Incorrectly Interpreted the CSS Policies, as well as the Pen Register Statute

The Secret Service and ICE HSI did not always obtain court orders for two reasons. First, CSS policies mandate that all applicable requirements, namely obtaining court orders, apply to all instances of CSS use — whether in support of component or external law enforcement investigations. However, the policies do not provide sufficiently detailed guidance for how to comply with requirements when other entities, such as local law enforcement, are responsible for obtaining the required CSS judicial authorizations. According to Secret Service and ICE HSI officials, when providing CSS support to other agencies, they rely on other Federal, state, and local law enforcement agencies to obtain required court authorizations.

Second, the Secret Service and ICE HSI did not correctly interpret the terms of, or meet requirements, in CSS policies, which reflect the Pen Register Statute's mandate. Specifically, the Secret Service and ICE HSI investigative records provided did not distinguish between "exigent circumstance" and "emergency situations" as necessary to show compliance with CSS policies reflecting the Pen Register Statute's requirements. Identifying whether "exigent circumstances" and "emergency situations" exist are two distinct fact-specific decisions, which must be evaluated to determine the necessary legal process to authorize the use of the CSS. During "exigent circumstances" CSS policies require that the Secret Service and ICE HSI obtain a court order pursuant to the Pen Register Statute, which ordinarily requires judicial authorization before

use of CSS. CSS may be used in an "emergency situation" if, with due diligence, a court order authorizing such use cannot be obtained beforehand and the facts meet the definition of "emergency." In some cases, such as the immediate danger of death or serious injury, an "emergency situation" under the Pen Register Statute will also be an "exigent circumstance" under the CSS policies. If the Secret Service and ICE HSI considered the exigent circumstances equated to emergency situations under CSS policies and the Pen Register Statute, they were required to apply for a pen register order within 48 hours of installing, or beginning to install, CSS but failed to do so.

Additionally, ICE HSI did not believe court authorization was required for [redacted] CSS uses. ICE HSI noted in [redacted] that court authorization was not required because the family provided consent and there was no reasonable expectation of privacy.[25] In [redacted], ICE HSI indicated that due to the exigent nature of [redacted], court authorization was not required. Despite ICE HSI's belief that court authorization was not required for these [redacted], ICE HSI should have either obtained a court order before using CSS; or if the exigent circumstance met the definition of an "emergency" under the Pen Register Statute, applied for a court order within 48 hours of installing, or beginning to install, CSS.

**Secret Service and ICE HSI Did Not Document CSS Supervisory Approval and Data Deletion**

CSS policies also require supervisory approval before CSS use and data deletion upon mission completion. However, in reviewing Secret Service and ICE HSI investigations using CSS we determined that the components did not always have documented support of supervisory approval and data deletion. Documented supervisory approval and data deletion would better ensure compliance with CSS policy and improve monitoring consistent with the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*, September 2014.

Neither DHS' nor the Secret Service's CSS policy requires personnel to document supervisory approval and data deletion. According to the Secret Service, supervisors verbally approved each instance of CSS use and Secret Service's Mobile Wireless Investigations office sends monthly reminders to CSS operators to ensure data is deleted according to policy. The Secret Service has

[25] The only exception to the requirement to obtain a court order under the Pen Register Statute applies to electronic or wire communication service providers who may install or use a Pen Register for purposes such as operations, maintenance, and testing of wire or electronic communication service, or with the consent of the user of that service has been obtained. 18 U.S.C. § 3121(b)(1) and (2).

taken corrective action to increase accountability by adding fields to its investigative reporting system to ensure evidence of supervisory approval and data deletion are documented.

ICE HSI's CSS policy states that supervisory approval should be documented if circumstances permit and requires data deletion following each mission. We identified [redacted] instances in which ICE HSI did not document supervisory approval and [redacted] instances in which ICE HSI did not document data deletion. ICE HSI addressed the supervisory approval issue with an update to its reporting system to ensure CSS approvals are documented. According to ICE HSI, the data associated with employment of CSS was deleted but the documentation was not completed correctly. ICE HSI indicated it would address the data deletion issue in a future policy update.

## ICE HSI Did Not Adhere to Department Privacy Policies and the *E-Government Act of 2002* Before Using CSS

ICE HSI did not adhere to DHS privacy policies and the Federal statute that requires CSS, as a privacy sensitive technology, to have an approved PIA before it is used. DHS privacy policies require components acquiring new or substantially changed technology to complete a PTA to determine whether additional compliance documents, such as a PIA, are required to comply with Section 208 of the *E-Government Act of 2002*.

The first step of the PIA process is to submit a PTA to determine if a system, project, or program is privacy sensitive and currently in compliance with relevant privacy documentation. DHS Privacy approves the PTA, provides the expiration date for the PTA, and indicates whether, among other things, a new or updated PIA is required. DHS Privacy stated that in the event a new or updated PIA is required, components cannot use the technology or system until such a PIA is approved. The PIA should include an overview of the project's purpose, mission, and justification for operating a privacy sensitive project. It should also include legal authorities for collecting the information, characterization and uses of the information, additional notice requirements and data retention, information sharing, redress and correction actions, and auditing and accountability processes and procedures. Additionally, any privacy risks and mitigation strategies should be identified. Although DHS approved an ICE HSI CSS-related PIA in January 2022, prior to this approval, DHS may not have identified and mitigated the privacy risks associated with CSS use. In addition, individuals were not informed about the collection and use of PII and steps to mitigate privacy risks.

We reviewed ICE HSI's CSS-related PIAs and determined that, although ICE

HSI had an approved PTA, it did not have an approved PIA during the FYs 2020 and 2021 investigations using CSS, despite DHS Privacy requiring ICE HSI to submit a new PIA. DHS Privacy approved ICE HSI's CSS-related PTA on April 3, 2015 and determined that the CSS technology was privacy sensitive and required a new PIA. According to an ICE Office of Information Governance and Privacy official, ICE began drafting the PIA shortly after the PTA was adjudicated. However, resource limitations and changes in personnel resulted in a lengthy review and clearance process. ICE could not provide evidence the new PIA was submitted to DHS Privacy for approval prior to the FYs 2020 and 2021 investigations.

On July 18, 2019, DHS Privacy approved a different ICE HSI CSS-related PTA and determined that, once again, the technology was privacy sensitive and required a new PIA. Thereafter, ICE HSI drafted and submitted a PIA for DHS Privacy review and approval. DHS Privacy approved ICE HSI's CSS-related PIA on January 24, 2022.

Relatedly, we determined that the Secret Service had an approved CSS-related PIA for the period of relevant investigations covered by our audit.

## Recommendations

**Recommendation 1:** We recommend that the Assistant Director, Office of Investigations, United States Secret Service develop and implement internal controls to ensure compliance with 18 U.S.C. 3121, et seq., *Pen Registers and Trap and Trace Devices*, particularly when assisting other Federal, state, and local law enforcement agencies.

**Recommendation 2:** We recommend that the Assistant Director, Office of Investigations, United States Secret Service develop and implement internal controls to ensure cell-site simulator users differentiate between cell-site simulator-policy defined exigent circumstances and 18 U.S.C. 3125-defined emergency situations to comply with 18 U.S.C. 3121, et seq., *Pen Registers and Trap and Trace Devices*.

**Recommendation 3:** We recommend that the Assistant Director, Cyber and Operational Technology, U.S. Immigration and Customs Enforcement develop and implement internal controls to ensure compliance with 18 U.S.C. 3121, et seq., *Pen Registers and Trap and Trace Devices*, particularly when assisting other Federal, state, and local law enforcement agencies.

**Recommendation 4:** We recommend that the Assistant Director, Cyber and Operational Technology, U.S. Immigration and Customs Enforcement develop

and implement internal controls to ensure cell-site simulator users differentiate between cell-site simulator policy-defined exigent situations and 18 U.S.C. 3125-defined emergency circumstances to comply with 18 U.S.C. 3121, et seq., *Pen Registers and Trap and Trace Devices*.

**Recommendation 5:** We recommend that the Assistant Director, Cyber and Operational Technology, U.S. Immigration and Customs Enforcement develop and implement internal controls to ensure cell-site simulator data deletion is accurately documented in the Incident Case Management system.

**Recommendation 6:** We recommend that the Assistant Director, Cyber and Operational Technology, U.S. Immigration and Customs Enforcement develop and implement internal controls to ensure privacy compliance documentation is completed and approved before developing or procuring information technology that collects, maintains, or disseminates information in identifiable form.

## Management Comments and OIG Analysis

DHS concurred with all six recommendations. Appendix B contains a copy of DHS' management response in its entirety. We also received technical comments to our draft report, and we revised the report as appropriate. A summary of DHS' response to each recommendation with our analysis follows.

**DHS Response to Recommendation 1:** Concur. To ensure compliance with 18 U.S.C. 3121, the Secret Service Office of Investigations has begun implementing internal controls, which will require CSS operators to document the legal process followed when conducting CSS investigations. Once complete, the Secret Service Office of Investigations will communicate these new controls via a training session for all active personnel. Further, the Office of Investigations, in partnership with the Secret Service Office of Chief Counsel, will continue to provide training to current and new operators on statutory and policy requirements, to include when assisting other law enforcement agencies. Current and future CSS operators will also be instructed to articulate these requirements to the Federal, state, local, tribal, and territorial law enforcement agencies that request CSS assistance. Estimated Completion Date (ECD): June 30, 2023.

**OIG Analysis of DHS Comments:** DHS' corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation showing the new processes, training, and training rosters.

**DHS Response to Recommendation 2:** Concur. The Secret Service Office of Investigations has already begun implementing controls to require operators to distinguish between exigent circumstances (as recognized by the Fourth Amendment of the Constitution) and emergency situations (as recognized by the Pen Register Statute). Specifically, operators will first determine whether a recognized exigency exists, then separately determine if an emergency situation exists, as well. Depending on the operator's determination, the application will indicate what type of legal process is likely required. Once these internal controls are complete, the Secret Service Office of Investigations will also communicate these updates via a training session for all active personnel, and the updates will be incorporated into all future training courses and procedures. In addition, the Office of Investigations, in partnership with the Office of Chief Counsel, will continue to provide training to current and new operators on statute and policy requirements, to include differentiating between emergency situations and exigent circumstances. ECD: June 30, 2023.

**OIG Analysis of DHS Comments:** DHS' corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation showing its updated guidance, training, and training rosters.

**DHS Response to Recommendation 3:** Concur. To ensure compliance with 18 U.S.C. 3121, ICE HSI will update its CSS policy to clarify the requirements when assisting other Federal, state, local, tribal, and territorial law enforcement agencies. The policy will be updated to include language on complying with requirements when other entities, such as local law enforcement, are responsible for obtaining the required CSS judicial authorizations. ECD: June 30, 2023.

**OIG Analysis of DHS Comments:** DHS' corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation showing its updated policy and distribution of the policy to end users.

**DHS Response to Recommendation 4:** Concur. ICE HSI will update its "Use of Cell-Site Simulator Technology," policy, dated August 31, 2017, to differentiate between exigent circumstances and emergency situations, including the respective legal processes that must be followed for compliance and use of CSS. Specifically, the policy will clarify that, during an exigent circumstance, ICE will obtain a court order pursuant to 18 U.S.C. 3121. During an emergency situation, with due diligence, if a court order authorizing such use cannot be obtained beforehand and the facts meet the definition of

"emergency;" then, a Pen Register order will be obtained within 48 hours of installation or beginning of install. ECD: June 30, 2023.

**OIG Analysis of DHS Comments:** DHS' corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation showing its updated policy and distribution of the policy to end users.

**DHS Response to Recommendation 5:** Concur. As the OIG noted in the draft report, ICE HSI has addressed the supervisory approval requirement during the course of the audit with an update to its reporting system to ensure CSS approvals are properly documented. However, HSI will also revise its policy to add language ensuring CSS data deletion is accurately documented in its case management system. The policy update will also remind, and guide, users through this policy requirement. ECD: June 30, 2023.

**OIG Analysis of DHS Comments:** DHS' corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation showing its updated policy and distribution of the policy to end users.

**DHS Response to Recommendation 6:** Concur. DHS Privacy Office approved the ICE HSI Surveillance Technologies PIA on January 24, 2022. If ICE HSI seeks to use any technology outlined in this PIA for a new purpose, it will confer with the ICE Office of the Principal Legal Advisor for legal advice and guidance to ensure adherence to Federal statutes. If the technologies are updated or further developed for any purposes not contemplated by the ICE CSS PIA, then HSI will coordinate with the DHS and ICE Privacy Offices to update the PIA, as appropriate. We request that the OIG consider this recommendation resolved and closed, as implemented.

**OIG Analysis of DHS Comments:** DHS' actions are partially responsive to this recommendation, which we consider unresolved and open. Although ICE HSI is ensuring required CSS privacy documentation is current, ICE HSI used the CSS for several years without an approved PIA. Additionally, ICE HSI needs internal controls to ensure privacy compliance documentation is completed and approved before developing or procuring any technology that collects, maintains, or disseminates information in identifiable form, not just for CSS. This recommendation will remain open and unresolved until DHS provides a plan to address the recommendation and evidence showing controls are in place to meet privacy requirements.

## Appendix A
## Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

Our original audit objective was to determine whether DHS and its components have developed, updated, and adhered to policies related to the use of cell-phone surveillance devices and commercial location-sharing databases. Our objective referenced two separate technologies: cell phone surveillance devices and commercial location-sharing databases. We have decided to report our audit results separately based on the type of technology. For this report, we sought to determine whether DHS and its components have developed, updated, and adhered to policies related to the use of CSS. DHS and component development, updates, and adherence to policies for the use of commercial telemetry data will be reported separately.

The scope of this audit included investigations using CSS devices during FYs 2020 and 2021. To accomplish our objective, we surveyed 22 DHS headquarters offices and components and reviewed CSS procurement documents. Based on our survey, we determined that only the Secret Service and ICE HSI used CSS within our scope period.

We evaluated relevant Federal laws, as well as DHS guidance, policies, and procedures related to its CSS programs, privacy requirements, and legal analysis. Specifically, we reviewed:

- 18 U.S.C. Ch. 206: *Pen Registers and Trap and Trace Devices*
- *E-Government Act of 2002,* Section 208
- U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*, September 2014
- *Department Policy Regarding the Use of Cell-Site Simulator Technology,* Policy Directive 047-02, October 19, 2015
- DHS Privacy Office, *Privacy Policy Guidance Memorandum*, Memorandum Number: 2008-02, December 30, 2008
- *Privacy Policy and Compliance*, Department of Homeland Security, DHS Directives System Instruction Number: 047-01-001, Revision Number: 00 Issue Date: 07/25/2011
- *DHS Privacy Impact Assessments, The Privacy Office Official Guidance, June 2010*
- *ICE Use of Cell-Site Simulator Technology,* August 31, 2017

- *Secret Service Mobile Wireless Investigations Cell-Site Simulator Manual,* January 10, 2017

Due to COVID-19-related travel restrictions, we were limited to three site visits for CSS demonstrations to observe the capabilities and limitations of the devices. We visited ICE locations in Maryland and Virginia and a Secret Service location in Maryland. Although travel was limited, we were able to accomplish our objective through review of CSS investigation case files, interviewing Secret Service and ICE officials, and corroborating evidence to support our findings.

We worked with the DHS OIG Office of Counsel, DHS Office of the General Counsel, Department of Justice, and DHS and component officials to verify our interpretation of the Pen Register Statute and CSS policy.

To understand how DHS and components used the CSS and adhered to Federal laws and DHS policy, we interviewed officials from DHS Offices of Strategy, Policy, and Plans; Privacy; Civil Rights and Civil Liberties; Chief Security Officer; and General Counsel. We also interviewed officials from the following operational components: Secret Service Criminal Investigative Division and Office of Intergovernmental and Legislative Affairs; and ICE Homeland Security Investigations Cyber and Operational Technology and Office of Information Governance and Privacy.

We selected a sample of Secret Service's and ICE HSI's CSS investigations to assess their compliance with laws and regulations. We requested closed cases to avoid interfering with ongoing investigations. Secret Service's investigative records differentiate between CSS use to support Secret Service operations and when Secret Service provides CSS support to other Federal, state, or local law enforcement. When providing CSS support to other Federal, state, or local law enforcement, Secret Service's investigative records generally indicate when the CSS support mission is complete; however, the Federal, state, or local law enforcement investigation may be ongoing. Each Secret Service case file contained a single investigative record. Of the [redacted] Secret Service CSS operations, we selected a non-generalizable sample of [redacted] investigative records to avoid potentially ongoing investigations. [redacted] of the case files selected were misclassified and did not involve deployment of the CSS, therefore the analysis considered [redacted] investigative cases. [redacted] of the CSS uses were identified as being used to support Secret Service operations; however, the CSS were used to support other Federal, state, and local law enforcement. Secret Service did not indicate that the [redacted] cases were open or active and provided the requested records.

Of the [redacted] ICE HSI CSS case files, we selected a non-generalizable sample of [redacted] cases. ICE HSI field offices used different methods for documenting investigations using a CSS in its case files. Some field offices used a single case file to document each investigation. Other field offices used a single case file to document multiple investigations using a CSS. Although ICE HSI case files did not differentiate between ICE HSI operations and ICE HSI CSS support of other Federal, state, or local law enforcement, they did indicate if the cases were closed. The [redacted] ICE HSI case files selected for review consisted of [redacted] investigations using a CSS. We compared the investigative documentation to the Pen Register Statute and CSS policy requirements to determine if:

- warrants or court orders were obtained or applied for, as appropriate;
- warrants or the associated applications and supporting affidavits contained recommended disclosures;
- supervisory approval was obtained prior to CSS use;
- required training was completed by CSS users; and
- components maintained a record for data deletion.

In addition, to ensure compliance with Federal and DHS privacy requirements for privacy sensitive technology such as the CSS devices, we analyzed the requirements and applied them to approved Secret Service and ICE HSI privacy documents.

In planning and performing our audit, we identified the internal control components and underlying internal control principles significant to our audit objective. Specifically, we assessed the design, implementation, and operating effectiveness of the following controls related to Secret Service and ICE HSI CSS operations: the control environment, risk assessment, control activities, and monitoring. We identified internal control deficiencies that could affect Secret Service and ICE HSI compliance with Federal laws and CSS policies.

We assessed the reliability of the information we received pertaining to the Secret Service and ICE HSI CSS use. Specifically, we:

- observed demonstrations of the CSS device by the Secret Service and ICE HSI, as well as a demonstration of ICE's case management system;
- analyzed the CSS investigation case files including reports of investigations and warrant and court order documents;
- conducted multiple interviews and communicated with the components to ensure we had adequate information to clarify and corroborate the evidence; and

- verified analysis with the component officials to ensure our findings were accurate.

We referred CSS use without a warrant or court order that did not comply with the Pen Register Statute to our Office of Investigations. Based on the procedures performed, we determined the data was sufficiently reliable for purposes of the audit.

We conducted this performance audit between December 2020 and June 2022 pursuant to the *Inspector General Act of 1978*, *as amended*, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

# Appendix B
# Component Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

January 11, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.01.11 12:44:20 -05'00'

SUBJECT: Management Response to Draft Report: "Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators" (Project No. 21-008-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's recognition that the Department policy on the use of cell-site simulators (CSS)[1] incorporates internal controls and accountability requirements, and includes steps to ensure compliance with Constitutional protections afforded by the Fourth Amendment. DHS remains committed to the use of CSS in furtherance of criminal investigations consistent with the requirements and protections of the Constitution. This includes investigations related to narcotics and weapons smuggling, human rights violations, gang activity, money laundering, counterfeiting, cybercrime, and other illicit activities.

Both the United States Secret Service and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) will continue to use surveillance technologies consistent with the U.S. Constitution and federal law in support of DHS's highest priority, which is to protect the American people from threats to their security as articulated in the "DHS Strategic Plan for Fiscal Years 2022-2024."[2]

[1] Policy Directive 047-02, "Department Policy Regarding the Use of Cell-Site Simulator Technology," dated October 19, 2015
[2] https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf

The draft report contained six recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Enclosure

## Enclosure: Management Response to Recommendations Contained in 21-008-AUD-DHS

OIG recommended the Secret Service Office of Investigations Assistant Director:

**Recommendation 1**: Develop and implement internal controls to ensure compliance with 18 U.S.C. 3121, et seq., "Pen Registers and Trap and Trace Devices," [Pen Register Statute] particularly when assisting other Federal, state, and local law enforcement agencies.

**Response:** Concur. To ensure compliance with 18 U.S.C. 3121, the Secret Service Office of Investigations has begun implementing internal controls, which will require CSS operators to document the legal process followed when conducting CSS investigations. Once complete, the Secret Service Office of Investigations will communicate these new controls via a training session for all active personnel. Further, the Office of Investigations, in partnership with the Secret Service Office of Chief Counsel, will continue to provide training to current and new operators on statutory and policy requirements, to include when assisting other law enforcement agencies. Current and future CSS operators will also be instructed to articulate these requirements to the federal and SLTT law enforcement agencies that request CSS assistance. Estimated Completion Date (ECD): June 30, 2023.

**Recommendation 2**: Develop and implement internal controls to ensure cell-site simulator users differentiate between cell-site simulator-policy defined exigent circumstances and 18 U.S.C. 3125-defined emergency situations to comply with 18 U.S.C. 3121, et seq., "Pen Registers and Trap and Trace Devices."

**Response:** Concur. The Secret Service Office of Investigations has already begun implementing controls to require operators to distinguish between exigent circumstances (as recognized by the Fourth Amendment of the Constitution) and emergency situations (as recognized by the Pen Register Statute). Specifically, operators will first determine whether a recognized exigency exists, then separately determine if an emergency situation exists, as well. Depending on the operator's determination, the application will indicate what type of legal process is likely required. Once these internal controls are complete, the Secret Service Office of Investigations will also communicate these updates via a training session for all active personnel, and the updates will be incorporated into all future training courses and procedures. In addition, the Office of Investigations, in partnership with the Office of Chief Counsel, will continue to provide training to current and new operators on statute and policy requirements, to include differentiating between emergency situations and exigent circumstances. ECD: June 30, 2023.

OIG recommended the ICE Cyber and Operational Technology Assistant Director:

**Recommendation 3**: Develop and implement internal controls to ensure compliance with 18 U.S.C. 3121, et seq., "Pen Registers and Trap and Trace Devices," particularly when assisting other Federal, state, and local law enforcement agencies.

**Response:** Concur. To ensure compliance with 18 U.S.C. 3121, ICE HSI will update its CSS policy to clarify the requirements when assisting other Federal and SLTT law enforcement agencies. The policy will be updated to include language on complying with requirements when other entities, such as local law enforcement, are responsible for obtaining the required CSS judicial authorizations. ECD: June 30, 2023.

**Recommendation 4**: Develop and implement internal controls to ensure CSS users differentiate between CSS policy-defined exigent situations and 18 U.S.C. 3125-defined emergency circumstances to comply with 18 U.S.C. 3121, et seq., "Pen Registers and Trap and Trace Devices."

**Response:** Concur. ICE HSI will update its "Use of Cell-Site Simulator Technology," policy, dated August 31, 2017, to differentiate between exigent circumstances and emergency situations, including the respective legal processes that must be followed for compliance and use of CSS. Specifically, the policy will clarify that, during an exigent circumstance, ICE will obtain a court order pursuant to 18 U.S.C. 3121. During an emergency situation, with due diligence, if a court order authorizing such use cannot be obtained beforehand and the facts meet the definition of "emergency;" then, a Pen Register order will be obtained within 48 hours of installation or beginning of install. ECD: June 30, 2023.

**Recommendation 5**: Develop and implement internal controls to ensure CSS data deletion is accurately documented in the Incident Case Management system.

**Response:** Concur. As the OIG noted in the draft report, ICE HSI has addressed the supervisory approval requirement during the course of the audit with an update to its reporting system to ensure CSS approvals are properly documented. However, HSI will also revise its policy to add language ensuring CSS data deletion is accurately documented in its case management system. The policy update will also remind, and guide, users through this policy requirement. ECD: June 30, 2023.

**Recommendation 6**: Develop and implement internal controls to ensure privacy compliance documentation is completed and approved before developing or procuring information technology that collects, maintains, or disseminates information in identifiable form.

**Response:** Concur. DHS Privacy Office approved the ICE HSI Surveillance Technologies Privacy Impact Assessment (PIA) on January 24, 2022. If ICE HSI seeks to use any technology outlined in this PIA for a new purpose, it will confer with the ICE Office of the Principal Legal Advisor for legal advice and guidance to ensure adherence to federal statutes. If the technologies are updated or further developed for any purposes not contemplated by the ICE CSS PIA, then HSI will coordinate with the DHS and ICE Privacy Offices to update the PIA, as appropriate. We request that the OIG consider this recommendation resolved and closed, as implemented.

## Appendix C
## *Department Policy Regarding the Use of Cell-Site Simulator Technology*, Policy Directive 047-02, October 19, 2015

*Deputy Secretary*
**U.S. Department of Homeland Security**
Washington, DC 20528

Homeland Security

October 19, 2015

POLICY DIRECTIVE 047-02

MEMORANDUM FOR: Sarah Saldaña
Assistant Secretary
U.S. Immigration and Customs Enforcement

Joseph Clancy
Director
United States Secret Service

R. Gil Kerlikowske
Commissioner
U.S. Customs and Border Protection

Admiral Paul F. Zukunft
Commandant
United States Coast Guard

Peter Neffenger
Administrator
Transportation Security Administration

L. Eric Patterson
Director
Federal Protective Service

FROM: Alejandro N. Mayorkas
Deputy Secretary

SUBJECT: **Department Policy Regarding the Use of Cell-Site Simulator Technology**

Cell-site simulators are invaluable law enforcement tools that locate or identify mobile devices during active criminal investigations. They allow law enforcement to locate both subjects of an investigation and their victims. This policy is being issued in light of the Department of Justice's recent legal analysis of the use of the valuable cell-site simulator technology.

www.dhs.gov

As with any law enforcement capability, the Department of Homeland Security ("DHS" or the "Department") must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data. As technology evolves, DHS must continue to assess its tools to ensure that practice and applicable policies reflect the Department's law enforcement and national security missions, as well as the Department's commitments to accord respect for individuals' privacy and civil liberties.

By this memorandum, I am directing immediate implementation of a DHS-wide policy on the use of cell-site simulator technology. This policy provides guidance and establishes common principles for the use of cell-site simulators across DHS. This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. Affected DHS Components may issue additional specific guidance consistent with this policy.

**BACKGROUND**

Law enforcement agents can use cell-site simulators to help locate cellular devices the unique identifiers of which are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity. This technology is one tool among many traditional law enforcement techniques and is deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

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

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

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is, however, limited. Cell-site simulators provide only the relative signal strength and general direction of the subject cellular device; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department's law enforcement Components must be configured as pen registers and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the device itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the device. Moreover, cell-site simulators used by the Department's law enforcement Components do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

**MANAGEMENT CONTROLS & ACCOUNTABILITY**

Department personnel require training and practice to properly operate cell-site simulators. Determinations regarding the appropriate use of this capability always should be informed by technological proficiency and experienced assessments of the suitability of the equipment for any given operation. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. Each Component that uses cell-site simulators shall develop operational policy or procedures to govern the use of this technology consistent with this policy. When developing operational policy or procedures to govern the use of this technology consistent with Department policy, Components will coordinate with the DHS Office of the General Counsel, the Office of Policy, the Privacy Office, and the Office for Civil Rights and Civil Liberties.

2. Department personnel must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their Component to use the technology and whose training has been administered by a qualified Component expert.

3. Within 30 days from the date of this policy, DHS law enforcement Components that use cell-site simulators shall designate an executive-level point of contact at the Component's headquarters office. The point of contact will be responsible for the implementation of this policy and for promoting compliance with its provisions, within his or her area of responsibility.

4. Prior to deployment of the technology, use of a cell-site simulator by the Component must be approved by a first-level supervisor. Any emergency use

of a cell-site simulator must be approved by an appropriate second-level supervisor. Any use of a cell-site simulator on an aircraft must be approved either by a Special Agent in Charge or the executive-level point of contact for the area of responsibility, as described in paragraph 3 of this section.

5. Each Component that uses cell-site simulators shall identify training protocols (including training on privacy and civil liberties) and protocols identifying which officials will have approval authority.

**LEGAL PROCESS & COURT ORDERS**

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

As a practical matter, because agents or operators, in consultation with prosecutors, will need to seek authority pursuant to Rule 41 and the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit also must reflect the information noted in the immediately following section of this policy ("Applications for Use of Cell Site Simulators").

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

*Exigent Circumstances under the Fourth Amendment*

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

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

*Exceptional Circumstances*

There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. For example, potential uses of the technology in furtherance of protective duties pursuant to 18 U.S.C. § 3056 and 18 U.S.C. § 3056A. In these limited circumstances, agents must first obtain approval from executive-level personnel at the Component's headquarters and the relevant U.S. Attorney, who coordinates approval within the Department of Justice.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, et seq., which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition, if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required (see provisions in *Exigent Circumstances under the Fourth Amendment*, directly above).

[1] In non-federal cases, the case agent or operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.
[2] Knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).

## APPLICATIONS FOR USE OF CELL-SITE SIMULATORS

In all circumstances, candor to the court is of paramount importance. When making any application to a court, DHS law enforcement personnel must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement personnel must consult with the prosecutors[3] in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.[4]

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

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

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

---

[3] While this provision typically will implicate notification to Assistant U.S. Attorneys, it also extends to state and local prosecutors when such personnel are engaged in operations involving cell-site simulators.

[4] Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (e.g., tradecraft, capabilities, limitations or specifications). Sample applications containing such technical information are available from the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice's Criminal Division. To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS and consult with appropriate agency counsel for compliance with DHS policies.

## DATA COLLECTION & DISPOSAL

DHS is committed to ensuring that law enforcement practices concerning the collection or retention[5] of data are lawful and respect the important privacy interests of individuals. As part of this commitment, DHS's law enforcement Components operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence,[6] the Department's use of cell-site simulators shall include the following practices:

1. Immediately following the completion of a mission, an operator of a cell-site simulator must delete all data.[7]

2. When the equipment is used to locate a target, data must be deleted as soon as the target is located.

3. When the equipment is used to identify a target, data must be deleted as soon as the target is identified, and no less than once every 30 days.

4. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

5. Components shall implement an auditing program to ensure that the data is deleted in the manner described above. To the extent feasible, this auditing program will include hardware and software controls, for example through an equipment sign-in process that will include operator badge number and an affirmative acknowledgement by the operator that he or she has the proper legal authority to collect and view data.

---

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

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

[7] A typical mission may last anywhere from less than one day and up to several days.

## STATE AND LOCAL PARTNERS

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

## TRAINING AND COORDINATION, AND ONGOING MANAGEMENT

Each DHS law enforcement Component shall provide this policy, and training as appropriate, to all relevant employees. Periodic review of this policy and training shall be the responsibility of each Component, based upon guidance from DHS oversight offices, with respect to the way the equipment is being used (e.g., significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). Any significant changes in technology or Component information collection, maintenance, use, or retention protocols may also trigger oversight responsibilities, and be reviewed before being implemented accordingly.[8]

Each field office shall report to its Component headquarters annual records reflecting the total number of times a cell-site simulator is deployed in the jurisdiction; the number of deployments at the request of other agencies, including state or local law enforcement; and the number of times the technology is deployed in emergency circumstances.[9]

Moreover, it is vital that all appropriate Department attorneys familiarize themselves with the contents of this policy, so that their court filings and disclosures are appropriate and consistent.

## IMPROPER USE OF CELL-SITE SIMULATORS

Accountability is an essential element in maintaining the integrity of our Federal law enforcement agencies. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the appropriate Component office that handles such allegations.

[8] For example, a significant change in technology could trigger the need for an updated or new privacy impact assessment.
[9] Records reflecting the number of times the cell-site simulators were used may also be required for ongoing oversight by the DHS oversight offices.

## SCOPE OF THIS POLICY

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

# Appendix D
## *18 U.S.C. Chapter 206: Pen Registers and Trap and Trace Devices*

**18 USC Ch. 206: PEN REGISTERS AND TRAP AND TRACE DEVICES**

**From Title 18—CRIMES AND CRIMINAL PROCEDURE**
PART II—CRIMINAL PROCEDURE

**CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES**



**EDITORIAL NOTES**

**AMENDMENTS**

**1988**—Pub. L. 100–690, title VII, §§7068, 7092(c), Nov. 18, 1988, 102 Stat. 4405, 4411, substituted "trap and trace" for "trap or trace" in item 3123, added item 3125, and redesignated former items 3125 and 3126 as 3126 and 3127, respectively.

### §3121. General prohibition on pen register and trap and trace device use; exception

(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

(c) LIMITATION.—A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(d) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

(Added Pub. L. 99–508, title III, §301(a), Oct. 21, 1986, 100 Stat. 1868; amended Pub. L. 103–414, title II, §207(b), Oct. 25, 1994, 108 Stat. 4292; Pub. L. 107–56, title II, §216(a), Oct. 26, 2001, 115 Stat. 288; Pub. L. 115–141, div. V, §104(3)(A), Mar. 23, 2018, 132 Stat. 1217.)

**EDITORIAL NOTES**

**REFERENCES IN TEXT**

The Foreign Intelligence Surveillance Act of 1978, referred to in subsec. (a), is Pub. L. 95–511, Oct. 25, 1978, 92 Stat. 1783, which is classified principally to chapter 36 (§1801 et seq.) of Title 50, War and National

Defense. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of Title 50 and Tables.

### AMENDMENTS

**2018**—Subsec. (a). Pub. L. 115–141 inserted before period at end "or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523".

**2001**—Subsec. (c). Pub. L. 107–56 inserted "or trap and trace device" after "pen register" and ", routing, addressing," after "dialing" and substituted "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications" for "call processing".

**1994**—Subsecs. (c), (d). Pub. L. 103–414 added subsec. (c) and redesignated former subsec. (c) as (d).

#### STATUTORY NOTES AND RELATED SUBSIDIARIES

### EFFECTIVE DATE

Pub. L. 99–508, title III, §302, Oct. 21, 1986, 100 Stat. 1872, provided that:

"(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title [enacting this chapter and section 1367 of this title] shall take effect ninety days after the date of the enactment of this Act [Oct. 21, 1986] and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

"(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any pen register or trap and trace device order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

"(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

"(2) the date two years after the date of the enactment of this Act [Oct. 21, 1986]."

## §3122. Application for an order for a pen register or a trap and trace device

(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

(Added Pub. L. 99–508, title III, §301(a), Oct. 21, 1986, 100 Stat. 1869.)

#### STATUTORY NOTES AND RELATED SUBSIDIARIES

### EFFECTIVE DATE

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 302 of Pub. L. 99–508, set out as a note under section 3121 of this title.

## §3123. Issuance of an order for a pen register or a trap and trace device

(a) IN GENERAL.—

(1) ATTORNEY FOR THE GOVERNMENT.—Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the

United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify—

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) CONTENTS OF ORDER.—An order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER OR A TRAP AND TRACE DEVICE.—An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that—

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

(Added Pub. L. 99–508, title III, §301(a), Oct. 21, 1986, 100 Stat. 1869; amended Pub. L. 107–56, title II, §216(b), Oct. 26, 2001, 115 Stat. 288.)

**EDITORIAL NOTES**

**AMENDMENTS**

**2001**—Subsec. (a). Pub. L. 107–56, §216(b)(1), reenacted heading without change and amended text generally. Prior to amendment, text read as follows: "Upon an application made under section 3122 of this

title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."

Subsec. (b)(1)(A). Pub. L. 107–56, §216(b)(2)(A), inserted "or other facility" after "telephone line" and "or applied" before semicolon at end.

Subsec. (b)(1)(C). Pub. L. 107–56, §216(b)(2)(B), added subpar. (C) and struck out former subpar (C) which read as follows: "the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and".

Subsec. (d)(2). Pub. L. 107–56, §216(b)(3), inserted "or other facility" after "leasing the line" and substituted "or applied, or who is obligated by the order" for ", or who has been ordered by the court".

#### Statutory Notes and Related Subsidiaries

#### Effective Date

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 302 of Pub. L. 99–508, set out as a note under section 3121 of this title.

### §3124. Assistance in installation and use of a pen register or a trap and trace device

(a) Pen Registers.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) Trap and Trace Device.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation.—A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(d) No Cause of Action Against a Provider Disclosing Information Under This Chapter.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter, request pursuant to section 3125 of this title, or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(e) Defense.—A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, a statutory authorization, or a good faith determination that the conduct complained of was permitted by an order from a foreign government that is subject to executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523, is a complete defense against any civil or criminal action brought under this chapter or any other law.

(f) Communications Assistance Enforcement Orders.—Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(Added Pub. L. 99–508, title III, §301(a), Oct. 21, 1986, 100 Stat. 1870; amended Pub. L. 100–690, title VII, §§7040, 7092(b), (d), Nov. 18, 1988, 102 Stat. 4399, 4411; Pub. L. 101–647, title XXXV, §3575, Nov. 29, 1990, 104 Stat. 4929; Pub. L. 103–414, title II, §201(b)(2), Oct. 25, 1994, 108 Stat. 4290; Pub. L. 107–56, title II, §216(c)(5), (6), Oct. 26, 2001, 115 Stat. 290; Pub. L. 115–141, div. V, §104(3)(B), Mar. 23, 2018, 132 Stat. 1217.)

### Editorial Notes

#### References in Text

The Communications Assistance for Law Enforcement Act, referred to in subsec. (f), is title I of Pub. L. 103–414, Oct. 25, 1994, 108 Stat. 4279, which is classified generally to subchapter I (§1001 et seq.) of chapter 9 of Title 47, Telecommunications. For complete classification of this Act to the Code, see Short Title note set out under section 1001 of Title 47 and Tables.

#### Amendments

**2018**—Subsec. (d). Pub. L. 115–141, §104(3)(B)(i), amended subsec. (d) generally. Prior to amendment, text read as follows: "No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title."

Subsec. (e). Pub. L. 115–141, §104(3)(B)(ii), amended subsec. (e) generally. Prior to amendment, text read as follows: "A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law."

**2001**—Subsec. (b). Pub. L. 107–56, §216(c)(6), inserted "or other facility" after "the appropriate line".

Subsec. (d). Pub. L. 107–56, §216(c)(5), struck out "the terms of" before "a court order".

**1994**—Subsec. (f). Pub. L. 103–414 added subsec. (f).

**1990**—Subsec. (b). Pub. L. 101–647 substituted "section 3123(b)" for "subsection 3123(b)".

**1988**—Subsec. (b). Pub. L. 100–690, §§7040, 7092(d), inserted ", pursuant to subsection 3123(b) or section 3125 of this title," after "shall be furnished" and "order" after last reference to "court".

Subsec. (d). Pub. L. 100–690, §7092(b)(1), inserted "or request pursuant to section 3125 of this title" after "this chapter".

Subsec. (e). Pub. L. 100–690, §7092(b)(2), inserted "under this chapter, a request pursuant to section 3125 of this title" after "court order".

### Statutory Notes and Related Subsidiaries

#### Effective Date

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 302 of Pub. L. 99–508, set out as a note under section 3121 of this title.

#### Assistance to Law Enforcement Agencies

Pub. L. 107–56, title II, §222, Oct. 26, 2001, 115 Stat. 292, provided that: "Nothing in this Act [see Short Title of 2001 Amendment note set out under section 1 of this title] shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 [amending this section and sections 3121, 3123, and 3127 of this title] shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities or assistance."

## §3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(1) an emergency situation exists that involves—

(A) immediate danger of death or serious bodily injury to any person;

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(Added Pub. L. 100–690, title VII, §7092(a)(2), Nov. 18, 1988, 102 Stat. 4410; amended Pub. L. 103–322, title XXXIII, §330008(3), Sept. 13, 1994, 108 Stat. 2142; Pub. L. 104–294, title VI, §601(f)(5), Oct. 11, 1996, 110 Stat. 3499; Pub. L. 107–296, title XXII, §2207(i), formerly title II, §225(i), Nov. 25, 2002, 116 Stat. 2158, renumbered §2207(i), Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

### Editorial Notes

#### Prior Provisions

A prior section 3125 was renumbered section 3126 of this title.

#### Amendments

**2002**—Subsec. (a)(1)(C), (D). Pub. L. 107–296 added subpars. (C) and (D).

**1996**—Subsec. (a). Pub. L. 104–294 struck out closing quotation mark at end.

**1994**—Subsec. (a). Pub. L. 103–322, §330008(3)(A), (B), substituted "use;" for "use' " in par. (2) and directed that matter beginning with "may have installed" and ending with "section 3123 of this title" be realigned so that it is flush to the left margin, which was executed to text containing a period after "section 3123 of this title", to reflect the probable intent of Congress.

Subsec. (d). Pub. L. 103–322, §330008(3)(C), substituted "provider of" for "provider for".

### Statutory Notes and Related Subsidiaries

#### Effective Date of 2002 Amendment

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

#### Effective Date

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 302 of Pub. L. 99–508, set out as a note under section 3121 of this title.

## §3126. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning—

(1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(2) the offense specified in the order or application, or extension of an order;

(3) the number of investigations involved;
(4) the number and nature of the facilities affected; and
(5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

(Added Pub. L. 99–508, title III, §301(a), Oct. 21, 1986, 100 Stat. 1871, §3125; renumbered §3126, Pub. L. 100–690, title VII, §7092(a)(1), Nov. 18, 1988, 102 Stat. 4410; amended Pub. L. 106–197, §3, May 2, 2000, 114 Stat. 247.)

### Editorial Notes

#### Prior Provisions

A prior section 3126 was renumbered section 3127 of this title.

#### Amendments

**2000**—Pub. L. 106–197 substituted ", which report shall include information concerning—" and pars. (1) to (5) for period at end.
**1988**—Pub. L. 100–690 renumbered section 3125 of this title as this section.

### Statutory Notes and Related Subsidiaries

#### Effective Date

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 302 of Pub. L. 99–508, set out as a note under section 3121 of this title.

#### Report on Use of DCS 1000 (Carnivore) To Implement Orders Under Section 3123

Pub. L. 107–273, div. A, title III, §305(a), Nov. 2, 2002, 116 Stat. 1782, provided that: "At the same time that the Attorney General submits to Congress the annual reports required by section 3126 of title 18, United States Code, that are respectively next due after the end of each of the fiscal years 2002 and 2003, the Attorney General shall also submit to the Chairmen and ranking minority members of the Committees on the Judiciary of the Senate and of the House of Representatives a report, covering the same respective time period, on the number of orders under section 3123 applied for by law enforcement agencies of the Department of Justice whose implementation involved the use of the DCS 1000 program (or any subsequent version of such program), which report shall include information concerning—

"(1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
"(2) the offense specified in the order or application, or extension of an order;
"(3) the number of investigations involved;
"(4) the number and nature of the facilities affected;
"(5) the identity of the applying investigative or law enforcement agency making the application for an order; and
"(6) the specific persons authorizing the use of the DCS 1000 program (or any subsequent version of such program) in the implementation of such order."

## §3127. Definitions for chapter

As used in this chapter—
(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;
(2) the term "court of competent jurisdiction" means—
(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—
(i) has jurisdiction over the offense being investigated;
(ii) is in or for a district in which the provider of a wire or electronic communication service is located;
(iii) is in or for a district in which a landlord, custodian, or other person subject to subsections (a) or (b) of section 3124 of this title is located; or
(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

(3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

(Added Pub. L. 99–508, title III, §301(a), Oct. 21, 1986, 100 Stat. 1871, §3126; renumbered §3127, Pub. L. 100–690, title VII, §7092(a)(1), Nov. 18, 1988, 102 Stat. 4410; amended Pub. L. 107–56, title II, §216(c)(1)–(4), Oct. 26, 2001, 115 Stat. 290; Pub. L. 111–79, §2(3), Oct. 19, 2009, 123 Stat. 2087.)

### Editorial Notes

#### References in Text

The Federal Rules of Criminal Procedure, referred to in par. (5), are set out in the Appendix to this title.

#### Amendments

**2009**—Par. (2)(A). Pub. L. 111–79 substituted "that—" and cls. (i) to (iv) for "having jurisdiction over the offense being investigated; or".

**2001**—Par. (1). Pub. L. 107–56, §216(c)(4), struck out "and" after " 'electronic communication'," and inserted ", and 'contents' " after " 'electronic communication service' ".

Par. (2)(A). Pub. L. 107–56, §216(c)(1), added subpar. (A) and struck out former subpar. (A) which read as follows: "a district court of the United States (including a magistrate judge of such a court) or a United States Court of Appeals; or".

Par. (3). Pub. L. 107–56, §216(c)(2), substituted "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication" for "electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached" and inserted "or process" after "device" wherever appearing.

Par. (4). Pub. L. 107–56, §216(c)(3), inserted "or process" after "means a device" and substituted "or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;" for "of an instrument or device from which a wire or electronic communication was transmitted;".

**1988**—Pub. L. 100–690 renumbered section 3126 of this title as this section.

### Statutory Notes and Related Subsidiaries

#### Effective Date

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 302 of Pub. L. 99–508, set out as a note under section 3121 of this title.

# Appendix E
# Report Distribution

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Director, United States Secret Service
Assistant Director, Office of Investigations, United States Secret Service
Director, U.S. Immigration and Customs Enforcement
Assistant Director, Cyber and Operational Technology, U.S. Immigration and Customs Enforcement
United States Secret Service Audit Liaison
U.S. Immigration and Customs Enforcement Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

## ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

## OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" box. If you cannot access our website, call our hotline at (800) 323-8603, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305