Homeland Security Investigations
Office of the Executive Associate Director

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536

MEMORANDUM FOR: Assistant Directors
Deputy Assistant Directors
Special Agents in Charge
Attachés

FROM: Katrina W. Berger
Executive Associate Director
Homeland Security Investigations
09/01/2023

SUBJECT: Use of Cell-Site Simulator Technology

Cell-site simulators (CSSs) 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 victims of ongoing criminal activity. Homeland Security Investigations (HSI) Special Agents (SAs) and Technical Enforcement Officers (TEOs) may use CSSs in accordance with the Department of Homeland Security (DHS) Policy Directive 047-02, "Department Policy Regarding the Use of Cell-Site Simulator Technology," dated October 19, 2015, or as updated, and this HSI policy memorandum.

As with any law enforcement capability, HSI must use CSSs in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment and applicable statutory authorities, (b) (7)(E) [redacted] Moreover, any information resulting from the use of CSSs must be handled in a way that is consistent with applicable statutes, regulations, and policies that guide HSI data collection, retention, and disclosure.

This policy memorandum provides guidance for the use of CSSs by HSI SAs and TEOs. This policy applies solely to the use of CSS technology in the United States and its Commonwealths, Territories, and Possessions, and only in furtherance of criminal investigations. CSSs may not be used in the enforcement of civil violations where the civil violation is the only identified violation.

Background

HSI SAs and TEOs may use CSSs to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an

unknown device, by collecting limited signaling information from devices in the simulator user's vicinity.

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

A CSS 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 CSS initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the CSS 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 CSS 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, CSSs acquire the identifying information from cellular devices. CSSs 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. (b) (7)(E)

(b) (7)(E)

Management Controls and Accountability

The following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1) The HSI Assistant Director (AD), Cyber and Operational Technology (COT), will be responsible for the implementation of this policy and for ensuring compliance with its provisions within HSI. The AD, COT, will also serve as the ICE executive level point of contact.

2) Prior to the court order application for the deployment of this technology, the use of a CSS must be approved by a first-level supervisor. Any exigent or emergency use of a CSS must also be approved by an appropriate second-level supervisor prior to its use. If the circumstances permit, these approvals should be granted in writing (an

email fulfills this requirement). When circumstances do not permit, approval should be documented in writing at the soonest practicable moment.

3) All users of CSSs are required to attend training before using the equipment, which is required to include annual training on both privacy and civil liberties. The Unit Chief of the HSI Title III/Linguistics Unit is responsible for the development and coordination of the initial and advanced training requirements for the use of CSSs.

Legal Process and Court Orders

The use of CSSs is permitted only as authorized by law and policy. While HSI SAs and TEOs have, in the past, appropriately obtained authorization to use a CSS by seeking an order (b) (7)(E) as a matter of policy, HSI SAs and TEOs 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.

HSI SAs and TEOs will need to seek authority pursuant to Rule 41 (b) (7)(E) (b) (7)(E) depending on the rules in their jurisdiction, prior to using a CSS. They must therefore consult with the Assistant United States Attorney (AUSA) or the appropriate state or local prosecutor, depending on the jurisdiction in which the CSS is being utilized, to either (1) obtain a warrant that contains all information required to be included (b) (7)(E) , or (2) seek a warrant (b) (7)(E) The search warrant affidavit must also reflect the information noted below under "Applications for Use of Cell Site Simulators." In addition to consulting with the appropriate prosecuting attorney, HSI SAs and TEOs shall coordinate with their local Office of the Principal Legal Advisor (OPLA) prior to beginning the legal process or, in the case of exigent circumstances, as soon as practicable thereafter.

There are three circumstances in which this policy does not require a warrant prior to the use of a CSS:

1) Exigent Circumstances Under the Fourth Amendment

Exigent circumstances is an exception to the Fourth Amendment warrant requirement, but CSSs 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 CSS still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.,* which ordinarily requires judicial authorization before use of the CSS, based on the government's certification that the information sought is relevant to an ongoing criminal investigation.

2) Exigent Circumstances Under Emergency (b) (7)(E)

In addition, in the subset of exigent situations where circumstances necessitate emergency (b) (7)(E) 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 supervisory approval to use a pen register before using a CSS.[1] 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 AUSA in the local U.S. Attorney's Office, who will coordinate approval within the Department of Justice (DOJ).[2] (b) (7)(E)

3) Training and Function Testing

All HSI SAs and TEOs who operate CSS equipment must have attended formal training provided by the equipment vendor and any other training determined necessary by the AD, COT. These operators are required to take an annual refresher course on the requirements of this policy, including training on privacy and civil liberties, which will be furnished by the HSI Technical Operations Unit.

During practical training scenarios, HSI personnel are permitted to target specified government- or vendor-provided equipment intended for use in training purposes. Non-approved devices and civilian devices will not be used as targets during training scenarios.

[1] This is in accordance with HSI Handbook 14-04, Technical Operations Handbook, dated July 21, 2014, or as updated.
[2] 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.

(b) (7)(E)

As part of the pre-deployment of CSS equipment, HSI operators should verify that the equipment is in proper working condition and confirm that the equipment has been cleared of all previous operational data, if it pertains to an unrelated mission, prior to deploying the equipment.

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, HSI SAs and TEOs must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. HSI SAs and TEOs must consult with the AUSA or appropriate prosecuting attorney in advance of using a CSS, and applications for the use of a CSS must include sufficient information to ensure that the courts are aware that the technology may be used.[4]

(b) (7)(E)

[4] Courts in certain jurisdictions may require additional technical information regarding the CSS'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 DOJ's Criminal Division. To ensure that courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, SAs, TEOs, or the prosecuting attorney must contact CCIPS, as well as consult with the local OPLA office for compliance with DHS policies.
[5] Despite any disruption in service, cell phones being disrupted will still be able to conduct emergency calls, e.g., 911.

(b) (7)(E)

Data Collection, Recordkeeping, and Disposal

HSI is committed to ensuring that law enforcement practices concerning the collection or retention[6] of data are authorized and respect the privacy interests of individuals. As part of this commitment, HSI will operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a CSS. Consistent with applicable law, regulation, and policy, including any duty to preserve exculpatory evidence,[7] HSI's use of CSSs shall include the following practices:

1) Immediately following the completion of a mission, an operator of a CSS must delete all data.[8]

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) Each deployment of a CSS will be documented in a Report of Investigation (ROI) by the CSS-trained operator. The ROI will be stored in the relevant investigative case file and retained in accordance with the applicable Federal records schedule.

[6] 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.
[7] It is not likely, given the limited type of data that CSSs collect (as discussed above), that exculpatory evidence would be obtained by a CSS in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent that investigators know or have reason to believe that information is exculpatory or impeaching, they have a duty to memorialize that information.
[8] A typical mission may last anywhere from less than one day to several days.

State and Local Partners

HSI often works closely with its state and local law enforcement partners and provides technological assistance under a variety of circumstances. In all cases, U.S. law enforcement must conduct authorized missions in a manner that respects the rights of individuals. This policy applies to all instances in which HSI uses CSSs in support of other Federal agencies and/or state and local law enforcement agencies. HSI must ensure that any requesting law enforcement agency will provide a copy of the appropriate legal documents authorizing the use of a CSS device to HSI before conducting the CSS mission unless the mission is deemed exigent under emergency circumstances. If a case is deemed "exigent" under emergency circumstances, appropriate legal documentation must be provided to HSI within a reasonable amount of time at the conclusion of the case.

Coordination and Ongoing Management

Each Special Agent in Charge office shall ensure proper documentation of CSS deployments into a CSS ROI by the trained CSS operator. In these ROIs, confirmation that the equipment had been cleared of any previous operational data must also be included. The ROI must be completed by the CSS-trained operator of the CSS.

Improper Use of Cell-Site Simulators

Accountability is an essential element in maintaining the integrity of HSI. CSSs are only used in furtherance of criminal investigations and are not to be used for the enforcement of civil violations where the civil violation is the only identified violation. HSI CSSs are to be operated only by properly trained HSI employees. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the Joint Intake Center and/or the ICE Office of Professional Responsibility.

No Private Right

This HSI policy memorandum 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.

Superseded Document
HSI memorandum, "Use of Cell-Site Simulator Technology," dated August 31, 2017.