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.

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.