Series	Effective Date	Review Date	Directive Number
200 Operations	TBD	*Three Years*	**203.15**
Chapter 202 - Limits on Authority			
Reviewing Office Commanding Officer (Major Crimes); Legal Advisor; Technical Support			☒ **New Directive** ☐ **Revised** Revisions are in *italics*
References *Michigan Law Enforcement Accreditation Commission 1.8.1, 1.8.2*			

CELL-SITE SIMULATOR

203.15 - 1 PURPOSE

The purpose of this policy is to establish guidelines and procedures governing the use of the Department's Cell-Site Simulator that will ensure public confidence in the Department's commitment to constitutional policing.

203.15 - 2 POLICY

The Cell-Site Simulator (CSS) is an investigative tool designed to identify and locate specific mobile devices by emulating a cellular tower signal. While this technology provides essential support to critical investigations, its use requires oversight, accountability, and strict adherence to legal and privacy standards.

Members are authorized to use the Department's cell site simulator to locate or identify mobile devices only to further investigations into violent crimes, crimes involving the possession or use of firearms or other dangerous weapons, complex investigations, or the recovery of missing persons. Only members trained in the operation of the CSS may operate the technology. Use of this technology must always comport with all relevant laws and regulations, including—

1. The Fourth Amendment of the Constitution of the United States (most notably, the Fourth Amendment).
2. The Constitution of the Michigan Constitution, Article I, Section 11.
3. The Electronic Communication Privacy Act (ECPA).
4. The DOJ Policy Guidance on Use of Cell-Site Simulator Technology.
5. MCL 780.651 *et seq* (governing search warrants).

The Department is committed to minimizing data collection to protect the privacy of non-targeted devices.

The commanding officer of Major Crimes shall serve as the designated, executive point of contact and will be responsible for implementing this policy and for promoting compliance with its provisions. Any member that uses the Cell-Site Simulator in violation of this policy will be subject to discipline, up to and including termination.

203.15 - 3 DEFINITIONS

As used in this directive, the following terms are defined as follows:

203.15 - 3.1 Authorized Operator
A sworn DPD member who has completed approved Cell-Site Simulator training and is certified to deploy the device under supervisory direction.

203.15 - 3.2 Cell-Site Simulator (CSS)
A device that functions by transmitting signals to cellular devices in the vicinity, causing devices to identify themselves by their unique identifiers. The CSS enables officers to locate a targeted mobile device by measuring signal strength and direction.

203.15 - 3.3 Data Custodian
The DPD member or designated IT personnel responsible for the secure storage, handling, and deletion of data generated during CSS operations.

203.15 - 3.4 Exigent Circumstances
Situations where immediate action is required to prevent loss of life, serious bodily harm, or the destruction of evidence.

203.15 - 3.5 International Mobile Subscriber Identity (IMSI)
A unique number assigned to a cellular subscriber used to identify the user on a mobile network.

203.15 - 3.6 Minimization
The process of configuring or operating the CSS to limit the collection, retention, and dissemination of data only to that necessary to achieve the authorized investigative purpose.

203.15 - 3.7 Non-Target Data
Data relating to cellular devices other than the target device, collected incidentally during authorized use.

203.15 - 3.8 Supervisory Officer
A ranking officer (sergeant or above) of the Headquarters Surveillance Unit or Homicide Unit responsible for authorizing, overseeing, and documenting CSS operations.

203.15 - 3.9 Target Device
The specific mobile device identified in the search warrant or court order that the CSS is authorized to locate or identify.

203.15 - 4 PROCEDURES

203.15 - 4.1 Authorized Use

The CSS may only be used to further an investigation into one of the following:

1. Murder or its attempt.
2. Assaults with intent to commit great bodily harm.
3. Any felonious assault that involves the use of a weapon.
4. Felony weapons offenses.
5. Fugitive apprehension.
6. Complex investigations (human trafficking, organized crime, crimes involving conspiracies, etc.).
7. Criminal sexual conduct.
8. Kidnapping.
9. Recovery of missing or lost individuals.

The Department often works closely with its State and Local law enforcement partners and provides technological assistance under a variety of circumstances. This policy applies to all instances in which The Department utilizes the Cell-Site Simulator in support of other Federal agencies and/or State and Local law enforcement agencies. Prior authorization must be approved by a Deputy Chief or above**.**

203.15 - 4.2 Judicial Authorization

Absent exigent circumstances, the CSS may only be used pursuant to a valid search warrant or court order that specifies—

1. The target phone number or unique device identifier.
2. The purpose of the operation.
3. The duration of authorized use.
4. Minimization requirements and data handling procedures.

The application or affidavit to support the issuance of a court order or search warrant should include the following:

a. The technique to be employed.
b. The investigator's 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.
c. The fact 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.
d. That the target cellular device and other cellular devices in the search area might experience a temporary disruption of service from the service provider.
e. How the Department will address deletion of data not associated with the target device and that no investigative use of any non-target data absent further order of the court will be used.

203.15 - 4.3 Exigent Circumstances

The CSS may be used without a search warrant or court order only where exigent circumstances, as that term is defined in this directive, exist. Such use must be approved by a ranking member of the Homicide Unit.

In the event the CSS is deployed under exigent circumstances, a warrant or retroactive judicial order must be sought and submitted within 48 hours of deployment.

203.15 - 4.4 Prohibited Uses:

The CSS shall not be used for any of the following:

1. Personal, civil, administrative, or non-criminal matters.
2. Surveillance based on political, racial, religious, or personal associations or beliefs.
3. Tracking or identifying devices without lawful authority.
4. Monitoring individuals engaged in lawful demonstrations or protected First Amendment activities without judicial authorization or exigent circumstances coupled with an offense that meets one of the authorized use cases set forth above.

203.15 - 4.5 Deployment Authorization

All operations must be authorized by a supervising officer of the investigative unit as well as the operating unit of Headquarter Surveillance or Homicide Unit. Prior to deployment, operators and supervisors must review the warrant, mission objectives, minimization procedures.

203.15 - 4.6 Minimization

The CSS shall be configured to collect only the data needed to locate the target device. Non-target data shall be automatically deleted or rendered inaccessible at the earliest feasible time, no later than 24 hours after collection.

Furthermore, ALL data must be deleted at the completion of an operation, when the target cellular device is located, or within 30 days of collection, whichever is sooner. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

The commanding officer of Major Crimes shall implement an auditing protocol to ensure that data is deleted as required by this policy.

203.15 - 4.7 CSS Deployment Log

All operations shall be recorded in the CSS deployment. This log shall include a record of the assigned personnel, the date and time of the mission, and the case number corresponding to the investigation.

203.15 - 4.8 Post-Operation Documentation
Upon completion of each operation, the operator shall prepare a CSS Usage Report that includes—

1. The case number and offense type.
2. The date and time of the deployment of the CSS.
3. The supervisory authorization and warrant information.
4. Results and follow-up action.

All post-operation documentation shall be submitted to the unit supervisor within 24 hours of the conclusion of the operation.

203.15 - 4.9 Supervision and Oversight
Supervisors shall review all CSS requests, deployments, and reports for completeness and adherence to this policy. A summary of all CSS deployments, including any policy violations, shall be submitted to the Deputy Chief of Police.

203.15 - 4.10 Confidentiality
All CSS information and documentation shall be maintained as confidential investigative material. Requests for release of information must be reviewed by the Legal Advisor and approved by the commanding officer of Major Crimes. Trained members with working knowledge of the CSS shall sign a non-disclosure agreement covering the technical capabilities, frequencies, or operational methods to unauthorized individuals.

203.15 - 4.11 Questions Regarding Legal Sufficiency
The Department's Legal Advisor or the Wayne County Prosecutor's Office shall be consulted on all questions regarding legal sufficiency.

202.2 - 5 DATA SECURITY, HANDLING, AND RETENTION

203.15 - 5.1 Data Storage [MLEAC 1.8.2 a]
CSS-generated software and reports shall be stored on secure DPD servers, managed by the Technical Support Unit, and safeguarded in accordance with DPD data security standards.

203.15 - 5.2 Access Control [MLEAC1.8.1 a, 1.8.2 b, d]
Access is restricted to authorized personnel only. Audit logs shall track data access and modifications.

203.15 - 5.3 Retention and Destruction [MLEAC 1.8.1 f]
Target data shall be retained only as long as necessary for the ongoing investigation or as requested within a search warrant. Non-target data shall be permanently deleted immediately upon identification. The unit supervisor shall certify data deletion within seven business days.

203.15 - 5.4 Disclosure
CSS-related data shall not be shared with outside entities except by court order, subpoena, or as required by law.

203.15 - 5.5 Technology, Security, and Maintenance [MLEAC 1.8.1 d]
The Headquarters Surveillance Unit shall ensure all firmware, encryption, and software are up to date. All software updates shall be applied through Detroit Police Technical Support with approval by the Commanding Officer of Major Crimes.

Unauthorized modifications or tampering with CSS equipment is strictly prohibited and will subject the member to disciplinary action and / or criminal prosecution. Any malfunctions or suspected compromise shall be reported immediately to the Commanding Officer of Major Crimes.

203.15 - 6 TRAINING REQUIREMENTS
Only trained and certified personnel shall operate or assist in CSS deployments. Training shall include, at a minimum, the following:

1. Legal parameters and warrant procedures.
2. Technical operation and data security.
3. Privacy and civil rights considerations.
4. Documentation and evidence handling.

Annual refresher training shall be mandatory.

203.15 - 7 ACCOUNTABILITY AND DISCIPLINE
203.15 - 7.1 Misuse or Unauthorized Access
Any member found to have used or authorized the use of the CSS without proper judicial authorization or outside the scope of this policy shall be subject to disciplinary action, including termination.

203.15 - 7.2 Negligence or Failure to Report
Failure to maintain accurate records, delete data, or report misuse shall result in disciplinary actions in accordance with the Department's disciplinary protocols.

203.15 - 7.3 Intentional Abuse
Intentional use of CSS technology for personal gain, surveillance of protected activity, or violation of constitutional rights shall result in immediate suspension pending investigation, and referral for criminal prosecution.

203.15 - 7.4 Supervisor Accountability
Supervisors who fail to provide adequate oversight or knowingly authorize non-compliant deployments shall be held equally accountable.

203.15 - 7.5 Corrective Action

Minor procedural violations may result in retraining or counseling. Major violations, misuse, or constitutional breaches will result in termination and potential legal action.

203.15 - 7.6 Notification to Internal Affairs

Internal Affairs shall be notified of all violations of this policy and shall have the discretion of assuming any investigation.

Related Procedures:

- 202.2 Search and Seizure
- 202.3 Search Warrants and Execution
- 203.6 Surveillance

Related Forms:

- PEN Registry Trap & Trace Search Warrant