CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: ALL DEPARTMENT PERSONNEL

FROM: Edgardo Garcia
Chief of Police

SUBJECT: **DUTY MANUAL ADDITION: L 4206 - USE OF CELLULAR COMMUNICATION INTERCEPTION TECHNOLOGY**

DATE: June 29th, 2016

Memo 2016-029

BACKGROUND

On January 1, 2016, Senate Bill 741 went into effect. SB 741 created California Government Code (CGC) section 53166. CGC 53166 requires law enforcement agencies that operate cellular communications interception technology (CCIT) to maintain reasonable security procedures and practices to protect information gathered through the use of CCIT from unauthorized access, destruction, use, modification, or disclosure. CGC section 53166 also requires agencies to implement a usage and privacy policy to ensure that collection, use, maintenance, sharing, and dissemination of information gathered through the use of CCIT complies with all applicable law and is consistent with individual privacy and civil liberties. The new law requires the usage and privacy policy to be available in writing to the public and to be posted conspicuously on the law enforcement agency's Internet Web site. CCIT is defined as any device that intercepts mobile telephone calling information, including international mobile subscriber identity catchers or other virtual based transceiver stations that masquerade as a cellular station and logs mobile telephone calling information.

As with any law enforcement capability, the San Jose Police Department must use CCIT in a manner that is consistent with the requirements and protections of the United States and California Constitutions, as well as federal and state law, including the Electronic Communications Privacy Act (ECPA), California Penal Code Sections 1546 –1546.4, 18 U.S.C. **§** 2703, 3122, 3123, which were enacted by the Legislature in Senate Bill 178 during the same legislative session as SB 741. The use of CCIT and any information collected through the use of CCIT must comply with the requirements of California Government Code 53166 and the ECPA.

ANALYSIS

In response to the creation of Government Code 53166, the Duty Manual has been updated to include several additions. The Duty Manual additions are reflected below in italics and underlined.

L 4206 ***USE OF CELLULAR COMMUNICATION INTERCEPTION TECHNOLOGY (CCIT)***
Added 06-29-16

San Jose Police Department CCIT Usage and Privacy Policy

Definition:

CCIT (cellular communications interception technology) is defined as any device or technology that intercepts mobile telephone calling information, including international mobile subscriber identity catchers or other virtual based transceiver stations that masquerade as a cellular station and logs mobile telephone calling information.

Authorized Purposes:

CCIT provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort (including the use of "ESN" or "IMSI" registration capture), to locate at-risk people or missing children, or to provide search and rescue support in natural disasters and emergencies, CCIT fulfills critical operational needs. All uses of CCIT will be in compliance with state and federal law. CCIT is but one tool among many traditional law enforcement strategies and will only be employed in cases in which the technology is best suited to achieve specific public safety goals. This technology will only be utilized when authorized by a search warrant that has been reviewed through the judicial process and is signed by a judicial officer (Penal Code Section 1546.1(b)(1)), (d)),(18 U.S.C. § 2703,3122,3123) or by specific consent of the authorized possessor of the mobile phone or with the specific consent of the owner of the mobile phone, only when the mobile phone has been reported as lost or stolen (Penal Code Section 1546.1(c)(3) and (4). All search warrants written for the authorized use of CCIT equipment maintained by the Covert Response Unit (CRU) must be reviewed and authorized by the CRU Commander or his designee.

The San Jose Police Department may use CCIT in the wake of a natural disaster or other emergency involving danger of death or serious bodily injury to any person, where the ability to locate a victim's cell phone can assist first responders in narrowing the area of a search, or locate victims and render aid in the shortest possible time frame (Penal Code Section 1546.1(c)(5)). In emergency circumstances involving a danger of death or serious bodily injury where the Department needs access to electronic information without delay, a search warrant shall be obtained within 48 hours of the use of CCIT (Penal Code Section 1546.1(c)(5) and (h)), (18 U.S.C. § 2703,3122,3123).

The Department may also use CCIT without a warrant if the Department, in good faith, believes the device to be lost, stolen, or abandoned, provided the Department shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

Authorized Employees:

CCIT may only be utilized by personnel who have received CCIT-specific training. All Department personnel who utilize CCIT shall be trained by the manufacturers of the CCIT or an authorized trainer within the Department. Authorized employees must attend refresher training as deemed necessary by the manufacturer. Department personnel, who access, maintain, disseminate, or

audit CCIT data and information shall be familiar with, and ensure compliance with this policy and the Electronic Communications Privacy Act (ECPA), California Penal Code Sections 1546-1546.4.

Security Procedures:

*CCIT is a restricted use asset. Physical safeguards include that when not in use, San Jose Police Department's CCIT devices and technology are secured in a locked facility. Technical safeguards shall include that all CCIT access information is password protected. The password shall be unique to the CCIT and shall not be distributed to unauthorized users. Information gathered by CCIT shall also be password protected and only accessible by Department members trained by the manufacturer in the use of CCIT. Operational safeguards include that the use of any CCIT devices or technology shall require pre-approval by a Command Officer or Covert Response Unit Sergeant and that each request that results in an approved use is supported by a search warrant or an applicable exemption under the ECPA. When making any application for a search warrant, Department members shall disclose appropriately and accurately the underlying purpose and activities for which the order or authorization is sought and shall otherwise comply with the search warrant requirements of the ECPA, (18 U.S.C. **§** 2703,3122,3123), Penal Code Sections 1546.1and 1546.2, and the search warrant requirements of Part 2, Title 12, Chapter 3, Penal Code Sections 1523-1542.5.*

Privacy and Civil Liberties:

The San Jose Police Department is committed to ensuring that law enforcement practices concerning the use of CCIT are lawful, and appropriately respects the important privacy interests of individuals. CCIT may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution. All use of CCIT shall meet the requirements set forth in California Government Code 53166 and the ECPA. Any public records requests for information obtained by CCIT must be in accordance with California Public Records Act (CPRA), and San Jose Police Department Duty Manual section C 2201 - City Policy and Resources for Responding to Public Record Act Requests. Records of police investigations are generally exempt from public disclosure under Government Code Section 6254(f). Moreover, police records of information collected using CCIT will generally be considered official information acquired in confidence by authorized personnel which is privileged from disclosure under California Evidence Code Section 1040 and therefore exempt from public disclosure pursuant to Government Code Section 6254(k). Affidavits and applications in support of search warrants for information collected using CCIT are judicial records and are subject to disclosure by the Superior Court that issues the warrant, California Penal Code Section 1534(a). To the extent that electronic information accessed or obtained through the execution of a search warrant is recorded, the record may be considered to be a judicial record, Penal Code Section 1536. California Rules of Court, Rule 2.400(a) states that unless otherwise provide by court rules or ordered by the court, court records can only be inspected by the public in the office of the court. Judicial records are not subject to the California Public Records Act, Government Code Section 6252(f).

Training and Accountability Provisions:

Accountability is an essential element in maintaining the integrity of the use of CCIT by the San Jose Police Department. Every law enforcement agency and/or officer requesting use of CCIT, shall be provided with a copy of this Policy and specialized training in its use. Such agencies shall also provide copies of this Policy and training, as appropriate, to all relevant employees who may be involved in the use of this technology. Periodic review of this Policy and training shall be the responsibility of the Deputy Chief of the Bureau of Investigations or his/her designee with respect to the way the equipment is being used or the data is being collected (e.g., significant advances in technological capabilities, type of data collected, or the manner in which it is collected). Department members will familiarize themselves with this Policy and comply with all orders concerning the use of this technology. Moreover, as the law in this area evolves, this Policy will be amended to reflect the current state of the law. It is vital that all authorized users of CCIT familiarize themselves with the contents of this Policy and the full content of the ECPA (PC 1546-1546.5),(18 U.S.C. § 2703,3122,3123), so that their administration of CCIT, and their court filings and representations are accurate and consistent with both the intent and scope of this Policy.

Monitoring Use:

The monitoring of the use of CCIT devices or technology will be the responsibility of the Deputy Chief of the Bureau of Investigations or his/her designee. Compliance checks with this usage and policy will be completed every fiscal quarter in conjunction with Program Manager Reports.

Information Sharing:

The San Jose Police Department often works closely with its Federal, State and Local law enforcement partners and provides technological and investigative assistance under a variety of circumstances. This policy applies to all instances in which the San Jose Police Department uses CCIT in support of other Federal, State or Local law enforcement agencies. The San Jose Police Department may share CCIT with other law enforcement agency partners that comply with all applicable state and federal laws, including the Electronic Communications Privacy Act, the California Government Code, and the California Public Records Act, regarding the uses and restrictions from sharing information, including the purposes of, processes for, and limitations from sharing information.

Information Retention and Dissemination:

The San Jose Police Department will operate CCIT 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 CCIT. The San Jose Police Department will not collect, retain or disseminate any data except as authorized by this Policy and by law. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence, the San Jose Police Department's use of CCIT shall include the following operational practices:

1. *Any data collected through the use of a CCIT device or technology that is not considered official evidence shall not be recorded or stored.*

2. *When the equipment is used following a disaster, or in a search and rescue context, all data must be deleted as soon as the person or persons in need of assistance have been located and in any event no less than once every (10) days.*

3. *The San Jose Police Department shall implement an audit program to ensure that the data is deleted in the manner described above. This audit shall take place not less than once every six (6) months. The audit program will be administered by the Deputy Chief of the Bureau of Investigations or his/her designee.*

4. *In cases where the information gathered by CCIT is considered evidence, the information shall be recorded and retained in the investigative case file and retained in compliance with the City of San Jose Records Retention Schedule located in City Policy Manual Section 6.1.5, which can be viewed at: http://www.sanjoseca.gov/DocumentCenter/View/11820.*

5. *Any data or information obtained through the use of CCIT shall be considered Sensitive Controlled Information (SCI). Any records of SCI that are created shall only be accessed in conjunction with the need to know and right to know the data or information being sought, in accordance with San Jose Police Department Duty Manual Section C 2003.1and in accordance with the other requirements of Duty Manual Chapter C 2000, including Section 2008.1, Recording Release of SCI.*

ORDER

CCIT significantly enhances the San Jose Police Department's efforts to achieve its public safety and law enforcement objectives. As with other capabilities, the San Jose Police Department must use this technology in a manner that is consistent with the Constitution and all other legal authorities. This policy provides additional principles and guidance to ensure that the San Jose Police Department utilizes CCIT in an effective and appropriate manner consistent with authorizing law. Effective immediately, Department members shall abide by this Policy and this Policy shall be implemented and made available to the public in writing and posted on the San Jose Police Department Internet page, www.sjpd.org.

Edgardo Garcia
Chief of Police

EG:SL:JB