



1 North San Antonio Road
Los Altos, California 94022-3087

MEMORANDUM

DATE: January 19, 2021
TO: Los Altos City Council
FROM: Andy Galea, Chief of Police
SUBJECT: ENCRYPTION OF POLICE RADIOS


The Los Altos Police Department is authorized by the California Department of Justice (CA DOJ) to access CLETS, which stands for the California Law Enforcement Telecommunications System. This is a computer network that provides law enforcement and criminal justice agencies with access to a variety of databases that contain data such as a person's identification information, criminal history, criminal record, and driving record information. One way that officers access CLETS is by using our police radio system called SVRIA (Silicon Valley Regional Interoperability Authority). This is the shared digital radio system that every police and fire department use in Santa Clara County. An example of how the police department uses this system would be when an officer makes a traffic stop and needs to verify that the driver has a valid license and is not wanted. To accomplish this, the officer provides personally identifiable information (PII), most often from a driver's license, over the radio to the emergency communication dispatchers so they can verify this information in the system (CLETS). Currently the main radio channel is not encrypted and anyone with a commercial scanner or a smartphone scanning app can listen and take down this information.

In October of 2020, the California Department of Justice notified every police department in the State of a policy update that mandates the transmission of sensitive personally identifiable information (PII) be encrypted. The Department of Justice memo is attached as a reference. The purpose of the mandate is to protect the privacy and identity of any person whose information is broadcast over a police radio frequency. The encryption requirement is to not only prevent potential identity theft, but also to give privacy to victims of crime. Police Department staff evaluated potential options to avoid the encryption mandate but found no viable options. Using a separate encrypted radio channel to conduct check criminal history poses safety concerns as that would require additional staffing in the communications center to monitor the additional radio channel. We currently do not have the staffing for this to take place.

Currently, all police departments have made the switch to encrypted radio channels with the exception of Milpitas, Mountain View, Santa Clara, and Los Altos. Plans are being made to join the Mountain View Police Department in the switch to an encrypted main channel in March of this year. Every police department will be switched over to an encrypted radio channel this year.

In recent news reports there have been concerns expressed about the encryption of police radios and how this change would limit news media or community members' access to police activity. I certainly understand the concerns expressed by those who would lose access to our main radio channel. The Los Altos Police Department has embraced social media to keep the community up-to-date and provides tools for community members to keep informed about crime and events. We utilize several social platforms such as Twitter, Facebook, Nextdoor, and AlertSCC. We typically utilize Twitter to keep media outlets informed of events or press releases. Media and community members can track crime information in the city at CityProtect.com. Most media inquiries received by the police department are from information obtained from CityProtect.com. In addition to the City of Los Altos Public Information Officer Sonia Lee, the police department administration or on duty supervisors are available to provide information to the media 24/7.

The Los Altos Police Department is prepared to communicate the transition to an encrypted main radio channel weeks in advance of the change.

<p>California Department of Justice CALIFORNIA JUSTICE INFORMATION SERVICES DIVISION Joe Dominic, Chief</p>		<h1>INFORMATION BULLETIN</h1>	
<p><i>Subject:</i> Confidentiality of Information from the California Law Enforcement Telecommunications System (CLETS)</p>	<p><i>No.</i> 20-09-CJIS</p> <p><i>Date:</i> 10-12-2020</p>	<p><i>Contact for information:</i> CLETS Administration Section CAS@doj.ca.gov (916) 210-4240</p>	

TO: ALL CLETS SUBSCRIBING AGENCIES

Law enforcement and criminal justice agencies authorized by the California Department of Justice (CA DOJ) to access the CLETS must adhere to the requirements detailed in the CLETS Policies, Practices and Procedures (PPP) and in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy to ensure the confidentiality and integrity of the data therein.¹ More specifically, and as detailed further below, access to certain Criminal Justice Information (CJI) and Personally Identifiable Information (PII) must be limited to authorized personnel; and the transmission of such information must be encrypted. Although generally applicable, the information in this bulletin is particularly relevant to the radio transmission of protected data.

Allowable “access” to CJI and PII, derived from CLETS, is described in CLETS PPP section 1.6.4:

Only authorized law enforcement, criminal justice personnel or their lawfully authorized designees may use a CLETS terminal or have access to information derived from CLETS. Any information from the CLETS is confidential and for official use only. Access is defined as the ability to hear or view any information provided through the CLETS.

The FBI and the CA DOJ establish policies and procedures related to the usage and protection of CJI that govern the usage of the CLETS. The policies define CJI, classify them as restricted or unrestricted, and limit the amount and types of information that can be broadcast over unencrypted radio channels in order to protect sensitive CJI and PII.

Generally, PII is information that can be used to distinguish or trace an individual’s identity, such as an individual’s first name, or first initial, and last name in combination with any one or more specific data elements (see FBI CJIS Security Policy section 4.3.). Data elements include Social Security number, passport number, military identification (ID) number and other unique ID numbers issued on a government document. The most common data elements encountered during field operations include a driver license number or ID number.

The transmission of sensitive CJI and PII must be encrypted pursuant to the FBI CJIS Security Policy sections 5.10 and 5.13; and access may only be provided to authorized individuals as defined under the CLETS PPP and the FBI CJIS Security Policy.

¹ For reference, please refer to the CLETS PPP at <https://oag.ca.gov/sites/default/files/clets-ppp%2012-2019.pdf> and the FBI CJIS Security Policy at https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view. See also Government Code section 15150 et seq. and California Code of Regulations, title 11, section 703.

Compliance with these requirements can be achieved using any of the following:

- Encryption of radio traffic pursuant to FBI CJIS Security Policy sections 5.10.1.2, 5.10.1.2.1, and 5.13.1. This will provide the ability to securely broadcast all CJI (both restricted and unrestricted information) and all combinations of PII.
- Establish policy to restrict dissemination of specific information that would provide for the protection of restricted CJI database information and combinations of name and other data elements that meet the definition of PII. This will provide for the protection of CJI and PII while allowing for radio traffic with the information necessary to provide public safety.

If your agency is not currently in compliance with the requirements outlined herein, please submit an implementation plan to the CA DOJ, CLETS Administration Section, no later than December 31, 2020. The plan must be on agency letterhead and signed by the Agency Head (e.g., Sheriff, Chief); include a detailed description of how radio communications will be brought into compliance (e.g., encryption), or how the risks will be mitigated through policy if unable to implement the required technology; and must include the projected timeline as to when the issue will be resolved.

For questions about this bulletin, contact the CLETS Administration Section at CAS@doj.ca.gov or (916) 210-4240.

Sincerely,



JOE DOMINIC, Chief
California Justice Information Services Division

For XAVIER BECERRA
Attorney General