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

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