SENATE COMMITTEE ON APPROPRIATIONS
Senator Anthony Portantino, Chair
2021 - 2022 Regular Session

SB 1000 (Becker) - Law enforcement agencies: radio communications

Version: March 16, 2022
Urgency: No
Hearing Date: May 9, 2022
Policy Vote: PUB. S. 4 - 1
Mandate: Yes
Consultant: Matthew Fleming

Bill Summary: SB 1000 requires each law enforcement agency to ensure that radio communications are accessible to the public by January 1, 2023, with specified exemptions.

Fiscal Impact: Unknown, potentially reimbursable costs in the millions for local law enforcement agencies to comply with the requirements of this bill. (General Fund).

Background: The right to transparency in government is a cornerstone of California's democracy, enshrined in its constitution and implemented by various statutes and regulations. One of these statutes, the California Public Records Act (CPRA), enacted in 1968, recognizes that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."

Implemented in the 1970's, the California Law Enforcement Telecommunications System (CLETS) is a data interchange network administered by the California Department of Justice (DOJ). CLETS provides law enforcement and criminal justice agencies access to databases maintained by state and federal agencies, and allows for the exchange of administrative messages to agencies within California, other states, and Canada. Its primary function is to provide law enforcement with individuals' criminal and driving records, often in real time as officers conduct investigations and respond to calls in the field. In October 2020, the DOJ division charged with administering CLETS issued a memo directing law enforcement agencies to take steps to restrict access to Criminal Justice Information (CJI) and Personally Identifiable Information (PII). According to the memo, agencies were permitted to comply with its directives via the following methods:

- Encryption Approach: Encryption of radio traffic pursuant to FBI Criminal Justice Information Service Security Policy. This will provide the ability to securely broadcast all CJI (both restricted and unrestricted information) and all combinations of PII.

- Hybrid Approach: 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.

In response to the DOJ's memo, several law enforcement agencies began to adopt the department's first suggested approach and fully encrypt their radio communications. Most notably, law enforcement agencies in San Jose, San Francisco, Palo Alto, San Diego, Mountain View and Tracy have opted for full encryption over adopting a policy

that restricts the dissemination of CJI and PII while allowing some public access to radio channels. Many of these agencies faced criticism from the journalists, the public, and local leaders advocating for greater transparency. In Palo Alto, for instance, the police department issued a memo asserting that because of the dangerous nature of police work, officers' ability to obtain critical information, including PII and CJI, is most safely done via radio communication. The memo went on to conclude that "other means of receiving this information can put the officer and the public at risk," and thus, "there are no other feasible options at this time to implement 'unencrypted' radio transmissions." As of April 4, 2022, radio communications for roughly 120 law enforcement agencies across California are fully encrypted, allowing no public access.

Proposed Law:

- Requires each law enforcement agency, as defined, to ensure that all radio communications, as defined, are accessible to the public by January 1, 2023.

- Specifies that a law enforcement agency may comply with the public access requirement in any manner that provides reasonable public access to radio communications including, without limitation, any of the following means:

    - Use of unencrypted radio communications on a radio frequency that is able to be monitored by commonly available radio scanning equipment.

    - Use of unencrypted radio communications on a radio frequency that is able to be monitored by commonly available radio scanning equipment.

    - Upon request and for a reasonable fee, providing access to encrypted communications to any interested person.

- Specifies that the public access requirement does not apply to any encrypted radio channel that is used exclusively for the exchange or dissemination of confidential information or to any encrypted radio channel that is used for tactical operations, undercover operations, or other communications that would unreasonably jeopardize public safety or the safety of officers if made public.

- Requires each law enforcement agency to enact policies that prevent or substantially minimize criminal justice information or personally identifiable information directly obtained through CLETS from being broadcast in a manner that is accessible to the public.

- Specifies that a law enforcement agency may comply with this confidentiality requirement in any manner that safeguards confidential CLETS information, including, without limitation, any of the following means:

    - The use of an encrypted channel for the exchange or dissemination of confidential information
    - Transmission of confidential information to a mobile data terminal, tablet, or other text display device.

  - Communication of confidential information via telephone or other private device-to-device communication.

- Specifies that the confidentiality requirement does not apply to confidential information that has previously been made public through a bulletin, alert or other means or to the broadcast of confidential information that is immediately necessary for the safety of the public or the safety of officers under circumstances where compliance would otherwise be unreasonable.

- Requires each law enforcement agency to adopt a written policy implementing its provisions no later than January 1, 2023.

Staff Comments: The California Constitution requires the state to reimburse local agencies for certain costs mandated by the state. This bill would require local law enforcement agencies to communicate most information on non-encrypted radio channels. Staff notes that there are approximately 120 law enforcement agencies in California who have opted to fully encrypt their radio communications in response to the DOJ memo that was distributed in 2020. In order to comply with the requirements of this bill, each of those agencies will have to switch over from using fully encrypted communications to the hybrid approach described above, in which encrypted channels are only used to communicate specific types of sensitive information. Reimbursable costs could include necessary training/retraining of officers in those agencies on which information can or must be communicated on a public channel as opposed to an encrypted one. In addition, local law enforcement agencies will need to create and implement the policies required by this bill.

-- END --