



Office of the City Manager

18

CONSENT CALENDAR
October 28, 2025

To: Honorable Mayor and Members of the City Council

From: Paul Buddenhagen, City Manager

Submitted by: Jennifer Louis, Chief of Police, Police Department

Subject: Authorization to Encrypt Berkeley Police Department Primary Radio Channels

RECOMMENDATION

Adopt a Resolution rescinding the City Council's existing policy (established in September of 2021) that limits the Police Department's use of encrypted public safety radio transmissions to Special Response Team operations, special patrol and investigative operations, prolonged critical incidents, execution of search warrants, or transmissions of Criminal Justice Information (CJI) and Personally Identifiable Information (PII) pursuant to California Department of Justice (DOJ) Bulletin 20-09-CJIS and authorize the encryption of all primary Berkeley Police Department (BPD) radio channels.

SUMMARY

This report requests Council approval to rescind the 2021 directive keeping most BPD radio channels unencrypted and to authorize encryption of all primary dispatch channels. The action will align Berkeley with every other Alameda and Contra Costa County agency that will transition to encryption in October 2025, ensure compliance with California DOJ and federal CJIS security requirements, protect community privacy, and address well-documented officer safety and operational integrity concerns.

FISCAL IMPACTS OF RECOMMENDATION

The City has already procured Motorola radios with built-in encryption capability. No additional costs are anticipated and, if necessary, any training or administrative costs associated with the transition will be absorbed within the Police Department's existing operating budget.

CURRENT SITUATION AND ITS EFFECTS

The Berkeley Police Department's primary and secondary dispatch channels currently remain unencrypted and therefore accessible in real time via scanner applications and internet streaming services. In recent months and over the last several years, BPD officers and detectives have documented multiple incidents where suspects actively monitored unencrypted radio traffic while committing crimes, most often in coordinated

overnight commercial burglaries involving multiple suspects. Intelligence shared through regional partnerships confirms that this is widespread, organized, and in some cases involves armed offenders.

Local examples include arrests in which suspects were stopped while listening to BPD's primary channel on a mobile device, recovery of phones from suspects that were actively broadcasting BPD channels, and investigative video showing lookouts using hand-to-ear signals consistent with monitoring radio traffic and alerting accomplices immediately prior to officer arrival. These behaviors demonstrate that suspects use scanner apps and similar tools to evade capture, to organize sideshows and other mass gatherings, and to track officer movements in real time.

The officer safety implications are substantial. When suspects have advance notice of officer presence or activity in an area, it not only enables their evasion of arrest; it can create a tactical disadvantage for responding personnel and increases the risk of a violent encounter. Advance knowledge of officer locations, response times, and tactics allows offenders to avoid detection, to reposition or withdraw, to prepare aggressive responses, or to set up ambushes if a confrontation ensues. The risk is greatest during low-staffing periods (typically overnight hours), when reporting parties and on-scene witnesses are often exposed and fewer officers are available to provide backup. The overall result is reduced operational effectiveness, higher risk of officer injury or death, compromised evidence recovery, increased danger to victims and witnesses, and diminished morale and confidence among public safety personnel.

Utilizing unencrypted radio channels also undermines regional operational and compliance benefits. The East Bay Regional Communications System Authority (EBRCSA) scheduled Contra Costa agencies to encrypt their communications on October 7, 2025, and Alameda County agencies on October 9, 2025. On October 7, Contra Costa agencies completed the encryption of their communications. Due to a need to correct a minor patching issue, the Alameda County agencies encryption is now scheduled for October 15, 2025. However, because the Berkeley Police Department cannot implement encryption without a change to Council policy, any Berkeley transition will occur after the rest of Alameda County. Without Council approval, Berkeley would be the only agency in the two-county system to continue broadcasting primary dispatch traffic unencrypted. That status not only concentrates criminal attention on Berkeley's open channels but also exposes the City to heightened liability as the City would be choosing not to meet statewide privacy and security expectations at a time when all of the other regional law enforcement partners did so.

This initiative is a Strategic Plan Priority Project, advancing our goal to create a resilient, safe, connected, and prepared city.

BACKGROUND

BPD is a member of the East Bay Regional Communications System Authority, a shared radio system designed to provide interoperable communications for police, fire, and other responders across Alameda and Contra Costa Counties. On October 12, 2020, the California Department of Justice issued Information Bulletin 20-09-CJIS, which requires the protection of Criminal Justice Information (CJI) and Personally Identifiable Information (PII) transmitted over radio systems and directs agencies to use encryption consistent with the FBI CJIS Security Policy. Agencies unable to encrypt immediately were directed to adopt restrictive interim workarounds and submit compliance plans with the understanding that full encryption would be implemented over time.

In September 2021, Council considered encryption as part of approving the City's Motorola radio contract. At that time, the County was not yet prepared to implement systemwide encryption and Council adopted a written policy that, except for Special Response Team operations and transmissions of CJI or PII pursuant to DOJ Bulletin 20-09-CJIS, most public safety radio transmissions remain unencrypted and accessible to the media and public through scanners or similar technology. The City's Motorola system was procured with encryption capability and the Council's action recognized encryption would eventually become necessary.

EBRCSA has since finalized a systemwide transition to AES 256-bit encryption for October of this year. Without Council approval to move forward with encryption, Berkeley will be the only agency in either county whose main dispatch radio communications remain publicly accessible in real time.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

There are no identifiable environmental sustainability or climate impacts associated with this action.

RATIONALE FOR RECOMMENDATION

Operating unencrypted radio channels is inconsistent with DOJ directives and exposes individuals, officers, and the City to significant risk. This is due to the operational reality that responding to and investigating calls for service regularly requires transmitting names, dates of birth, driver's license numbers, warrant information, addresses, or mental health information. As neighboring cities and counties move to protect CJI and PII, Berkeley risks being out of step with privacy standards and regulatory expectations. More critically, continuing to broadcast sensitive information without encryption creates tangible vulnerabilities that criminals exploit to avoid capture, to harm officers or community members, and to jeopardize ongoing investigations and prosecutions. While interim workarounds such as encrypted secondary channels and mobile data terminals have been used, those measures are operationally inefficient and unsustainable given staffing constraints in sworn and dispatch personnel. Continued reliance on these

workarounds increases the likelihood of delayed or incomplete information, reduced situational awareness, and heightened safety risks. To maintain transparency and media access, the Berkeley Fire Department's radio channels will remain unencrypted, ensuring continued public awareness of major incidents such as fires, collisions, and other critical events that often involve joint police and fire responses. This is possible as the fire channels do not typically include PII or police tactics.

Encrypting BPD's primary radio channels will protect officer safety and operational integrity by preventing suspects from anticipating or countering police response, and by eliminating the tactical advantage criminals currently gain from open access to dispatch communications. Encryption will safeguard community privacy by ensuring that PII and CJI are not publicly broadcast and will bring Berkeley into compliance with DOJ Bulletin 20-09-CJIS and the FBI CJIS Security Policy. Aligning with the regional transition reduces liability risk for the City and mitigates the incentive for offenders to disproportionately target Berkeley because it remains the last window into real-time police operations in the East Bay.

Full encryption also addresses staffing realities. Because the dedicated encrypted channel cannot always be staffed with allocated resources, BPD has experienced delayed or incomplete communications when relying on alternate channels. Implementing full encryption will eliminate these inefficiencies and ensure that both officers and dispatchers operate with complete and accurate information in real time, improving safety and mission effectiveness.

Beyond operational and legal benefits, encryption ensures officer safety and proactively reduces preventable risks. At the same time, encryption does not eliminate transparency. BPD will continue and expand its existing public information practices, including publication of crime and use-of-force data on the BPD Transparency Hub, timely notifications to City Council regarding significant incidents, social media updates through established City channels (Twitter/X, Facebook, Instagram, and Nixle), media briefings and access facilitated by the Public Information Officer, and continued access to records through the California Public Records Act.

Given the legal, operational, and public-safety imperatives described above, rescinding the Council's 2021 policy and authorizing full encryption of primary radio channels in coordination with the EBRCSA transition in October of 2025, is recommended. While an extended period of community engagement and education would have been preferable, the urgency of DOJ compliance and the immediate risks posed by ongoing unencrypted broadcasts justify near-term action. If approved, BPD will implement a public outreach plan during the transition that includes a description of the changes for the public, media notifications, and opportunities for community feedback.

Authorization to Encrypt Berkeley Police Department
Primary Radio Channels

CONSENT CALENDAR
October 28, 2025

ALTERNATIVE ACTIONS CONSIDERED

One alternative is to maintain the current policy and continue using interim workarounds such as encrypted secondary channels and mobile data computers. This approach was rejected because it is operationally inefficient, burdens personnel, does not fully meet DOJ/CJIS expectations, and leaves the City exposed to increased risk. A second alternative is to delay implementation of encryption; this was rejected because it would leave Berkeley as the sole unencrypted agency in the region, concentrate criminal attention on our open channels, and increase potential liability and safety risks.

CONTACT PERSON

Jennifer Louis, Chief of Police, Police Department, (510) 981-5700

Attachments:

1: Resolution

Exhibit A: EBRCSA Memo Regarding Encryption

Exhibit B: 9-28-2021 Supplemental 3 Agenda Material

RESOLUTION NO. ##,###-N.S.

RESCINDING THE CITY COUNCIL'S POLICY REGARDING UNENCRYPTED PUBLIC SAFETY RADIO CHANNELS AND AUTHORIZING THE ENCRYPTION OF BERKELEY POLICE DEPARTMENT PRIMARY RADIO CHANNELS

WHEREAS, the California Department of Justice issued Information Bulletin 20-09-CJIS (October 12, 2020) requiring encryption of all Criminal Justice Information (CJI) and Personally Identifiable Information (PII) transmitted over radio systems, consistent with the FBI CJIS Security Policy; and

WHEREAS, in September 2021 the City Council adopted a policy that most City public safety radio transmissions remain unencrypted, except for Special Response Team operations and transmissions of CJI/PII; and

WHEREAS, the Berkeley Police Department has documented numerous incidents in which suspects used unencrypted radio traffic to coordinate crimes, evade capture, and endanger officers and community members; and

WHEREAS, advance notice of officer presence or activity creates a tactical disadvantage and increases the risk of violent confrontation or ambush; and

WHEREAS, failure to encrypt would leave Berkeley the only unencrypted agency in Alameda and Contra Costa Counties, creating a unique public safety risk, undermining regional consistency, and exposing the City to liability; and

WHEREAS, the East Bay Regional Communications System Authority (EBRCSA) has scheduled encryption for Contra Costa agencies on October 7, 2025, and Alameda County agencies, including Berkeley, on October 15, 2025, which is the earliest date BPD could transition; however, actual implementation will occur as soon as practicable following Council authorization and administrative preparation.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the policy adopted on September 28, 2021, of transmitting unencrypted information on primary channels is hereby rescinded.

BE IT FURTHER RESOLVED that the Council authorizes the City Manager to approve the encryption of all primary Berkeley Police Department radio channels, to be implemented promptly after Council approval and required administrative steps are completed.

East Bay Regional Communications System Authority (EBRCSA)

Radio Encryption Transition: Timeline and Frequently Asked Questions (FAQ)

Subject: Transition to AES 256-bit Encryption for Radio Communications

Effective Dates: September 3 & 4, 2025

The East Bay Regional Communications System Authority (EBRCSA) is transitioning primary radio talk groups to AES 256-bit encryption. This change is being made to comply with state and federal mandates regarding the protection of sensitive information and to enhance safety.

Transition Schedule:

- **Alameda County Agencies:** September 3, 2025, from 0330 to 0530 hours.
- **Contra Costa County Agencies:** September 4, 2025, from 0330 to 0530 hours.

A final list of affected agencies is found at the end of this memo

Operational Support During Transition: A radio technician will be available in the communications center during the transition period to assist with the resetting of radio consoles and to address any questions from staff.

Preparation for Personnel: To ensure a smooth transition, all personnel working during these hours are strongly encouraged to familiarize themselves with the location of the encrypted zones on their radios before September 3 or 4. Simulating the process will help ensure operational readiness.

Frequently Asked Questions (FAQ) for Community and Media Engagement

The following information is provided to assist Chiefs and other personnel in responding to inquiries from the public and media.

1. Why are law enforcement agencies moving to radio encryption? This transition is a critical step to ensure compliance with legal and security requirements. Specifically, it addresses:

- **State Mandates:** The California Department of Justice (DOJ) requires the protection of Criminal Justice Information (CJI) and Personal Identifying Information (PII) during transmission.
- **Federal Standards:** The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy mandates encryption for the transmission of sensitive data.

- **Officer Safety:** Encrypting primary radio channels prevents individuals with malicious intent from monitoring police activities, including tactical information and officer locations, thereby reducing the risk to officers during dynamic situations.

2. The CA DOJ memo requiring the protection of PII and CJI was issued in 2020. Why is this transition happening now? Since the 2020 DOJ memo, many agencies have implemented interim solutions to protect PII and CJI, such as using back-up channels or in-car computers for data exchange. Some agencies also began using encrypted secondary channels for primary traffic. EBRCSA has worked to develop and implement a system-wide encryption solution to ensure consistent and comprehensive compliance for member agencies.

3. How common is radio encryption among other law enforcement agencies in California? While a precise count is not available, it is EBRCSA's understanding that most law enforcement agencies in California have already transitioned to or utilize encrypted radio channels for their primary communications, including most Bay Area law enforcement agencies.

4. Are there alternatives to encryption for protecting PII and CJI? While other solutions exist, they do not fully meet the rigorous standards set by the DOJ and FBI, are cost prohibitive to continue long-term or could compromise peace officer safety. The DOJ memo explicitly states that "the transmission of such information must be encrypted."

5. How will the media and public learn about in-progress events? Each department will manage such communications based on their specific needs, potentially through social media updates and encouraging all media to contact department dispatch or public information officers for official information.

6. Will the EBRCSA issue a press release about this change? No. EBRCSA is only providing the technical infrastructure for the transition. Public communication needs vary significantly among member agencies, so the EBRCSA will defer all media inquiries to the individual departments for comment.

7. How have other agencies handled public and media communications regarding encryption? For examples of how other agencies have managed this process, please review the following resources:

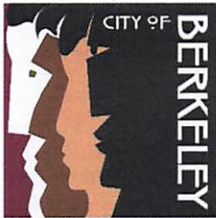
- City of Los Altos: <https://www.losaltosca.gov/404/Radio-Encryption>
- City of Santa Clara Police Department: <https://www.santaclaraca.gov/our-city/departments-g-z/police-department/community/news/police-radio-system>

Table 1: Alameda County, September 3

Agency	Technician Assigned	Time Block
ACSO	Jethro	0330
Oakland	Justice	0330
Livermore	Patricia	0330
Piedmont	J.J.	0330
San Leandro	John	0330
Pleasanton	Phil	0400
Alameda	Robert	0400
Albany	Matt	0400
Emeryville	Brandon	0400
UC Berkeley	Randy	0400
Berkeley	J.J.	0445
Fremont	John	0445
Hayward	Justice	0445
Newark	Patricia	0445
Oakland Housing Authority	Jethro	0445

Table 2: Contra Costa County, September 4

Agency	Technician Assigned	Time Block
Contra Costa SO	Robert	0330
Concord	Phil	0330
San Ramon	Matt	0330
Antioch	Jethro	0400
EBRPD	John	0400
Pinole	J.J.	0400
Richmond	Brandon	0400
Brentwood	Phil	0400
Martinez	Justice	0445
Pleasant Hill	Robert	0445
Walnut Creek	Matt	0445



Kate Harrison
Councilmember District 4

SUPPLEMENTAL 3 AGENDA MATERIAL

Meeting Date: September 28, 2021

Item Number: 18

Item Description: Lease Agreement with Motorola Solutions for Public Safety Radios

Supplemental/Revision Submitted By: Councilmember Harrison

“Good of the City” Analysis:

The analysis below must demonstrate how accepting this supplement/revision is for the “good of the City” and outweighs the lack of time for citizen review or evaluation by the Council.

Councilmember Harrison’s office was provided with the City’s current unwritten policy with respect to encrypted public safety radio transmissions on September 28, 2021 after the deadline for submitting Supplemental 1 or 2 material.

The City’s current policy is to only use encrypted public safety radio transmissions during tactical operations.

Given that the Lease Agreement with Motorola Solutions for Public Safety Radios includes the procurement of new radios that feature encryption capabilities, which could have significant First Amendment and transparency implications, it is in the public interest to establish a written policy at the Council level codifying current practices and ensuring that the news media and public continue to have access to unencrypted radio transmissions.

The attached motion would establish a written policy that all City public safety radio transmissions unrelated to Special Response Team operations and transmissions related to Criminal Justice Information (CJI) and Personally Identifiable Information (PII) in connection with the California Law Enforcement Telecommunications System (CLETS) and pursuant to California Department of Justice (CA DOJ) Information Bulletin No. 20-09-CJIS, shall be unencrypted and thereby transmittable to the news media and public through scanners or other relevant technology.

Consideration of supplemental or revised agenda material is subject to approval by a two-thirds vote of the City Council. (BMC 2.06.070)

A minimum of **42 copies** must be submitted to the City Clerk for distribution at the Council meeting. This completed cover page must accompany every copy.

Copies of the supplemental/revised agenda material may be delivered to the City Clerk Department by 12:00 p.m. the day of the meeting. Copies that are ready after 12:00 p.m. must be delivered directly to the City Clerk at Council Chambers prior to the start of the meeting.

Supplements or Revisions submitted pursuant to BMC § 2.06.070 may only be revisions of the original report included in the Agenda Packet.

It is the policy of the Berkeley City Council that the City of Berkeley, including the Berkeley Police Department and Berkeley Fire Department, shall only use encrypted public safety radio transmissions during Special Response Team operations or to transmit Criminal Justice Information and Personally Identifiable Information related to the California Law Enforcement Telecommunications System and pursuant to California Department of Justice Information Bulletin No. 20-09-CJIS. In accordance with the First Amendment and in spirit of transparency, all other public safety radio transmissions shall be unencrypted and thereby transmittable to the news media and public through scanners or other relevant technology.

Xavier Becerra, Attorney General

California Department of Justice CALIFORNIA JUSTICE INFORMATION SERVICES DIVISION Joe Dominic, Chief 	INFORMATION BULLETIN	
<i>Subject:</i> Confidentiality of Information from the California Law Enforcement Telecommunications System (CLETS)	<i>No.</i> 20-09-CJIS <i>Date:</i> 10-12-2020	<i>Contact for information:</i> 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.

Information Bulletin
Confidentiality of CLETS Information
Page 2

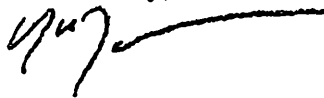
Compliance with these requirements can be achieved using any of the following:

- 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