



City of Palo Alto City Council Staff Report

(ID # 14168)

Meeting Date: 4/4/2022

Title: Receive the Police Department's Annual Report and Discuss and Accept the Staff Update on Radio Encryption as a Follow-up from the Policy and Services Committee Recommendation on February 8, 2022

From: City Manager

Lead Department: Police

Recommended Motion

Staff recommends that the City Council receive the Police Department's Annual Report and discuss and accept the staff update on radio encryption (Attachment A) as a follow-up from the Policy and Services Committee Recommendation on February 8, 2022.

Executive Summary

The Palo Alto Police Department (PAPD) typically shares accomplishments on an annual basis through a published report which the department presents at a study session with the City Council. This year's 2021 Annual Report is similar in content as past updates. It also provides information on radio encryption based on a follow-up request from the Policy and Services Committee discussion on February 8, 2022 for City Council to be updated on this matter.

Background

The Department strives to provide a published annual report to the City Council and public as done in [2018](#) and [2019](#). [The 2019 report](#) was published and presented in a [Study Session on February 24, 2020](#). Since the shelter-in-place and subsequent changes to the Department, the next report for the calendar year 2020 was presented as a [staff report](#) at the [April 5, 2021 City Council Meeting](#). This study session [presented](#) work done regarding police reform including:

- City Council and Ad Hoc Meetings to work in a public forum on police reform measures including policy changes
- [Message of inclusion and hope](#) June 1, 2020
- Added a [Race and Equity page](#) on the City website
- Added an [Accountability page](#) on the [Police Department website](#)
- Live-streamed 3 educational videos on Zoom on PAPD's [Use of Force Policy](#), [Laws of Arrest and Search and Seizure](#), and [Accountability in PAPD](#)
- Listened and participated in online community roundtables and Q&A sessions on [July 1, 2020](#) and [July 29, 2020](#)

- Collaboration with Stanford’s Social Psychological Answers to Real-World Questions (SPARQ) program.

This year’s annual report is similar to the last report which focuses on major department updates and is not presented in the published format (like the 2019 report) due to COVID and competing priorities.

As additional background, at the [annual retreat on February 5, 2022](#), the City Council selected “crime” as one of five city sub-categories of priorities under the [“Community Health and Safety” priority](#) (the other sub-set priorities were mental health, air quality, noise, and sense of belonging). Community members have expressed concern about a perceived rise in crime, with a handful of high-profile incidents during 2021 focusing attention on Palo Alto and safety, which will be addressed as part of the City Council’s annual workplan consideration scheduled for April 4, 2022.

Discussion

The following report provides a summary of 2021 initiatives, statistical trends, and accomplishments. It also provides a report on radio encryption as reviewed and recommended by the Policy and Services Committee. The initial Committee direction was to hold a study session to “discuss police radio encryption, and how best to allow the public and the media to be rapidly informed for calls to service.”

The [FY 2022 Adopted Operating Budget](#) lists the most recent initiatives adopted by the Department (beginning on PDF page 357) to include:

- Continued partnership with stakeholders on race and equity initiatives [Status: In process]
- Purchase an updated Computer Aided Dispatch (CAD) system [Status: Pending - Council action forthcoming]
- Implement Racial and Identity Profiling Act (RIPA) [Status: In process – data collection has begun. First state [RIPA Board report](#) with Palo Alto data will be published April 2023]
- Implement the Psychiatric Emergency Response Team (PERT) [Status: Deployed]
- Focus on hiring critical positions including police officer and public safety dispatch positions [Status: In process]

In 2021, the Department had a net 125.33 FTE full-time positions (149 FTE less 23.67 FTE frozen positions). The net result was 80.0 FTE sworn positions, and a net 45.33 FTE non-sworn positions, along with 1.08 hourly FTE’s that include a net 5 reserve police officers. The Department is divided into three divisions: Field Services, including Patrol squads, Mental Health Intervention and Patrol Community Service Officers; Technical Services, including Communications/Dispatch Center and Records; and Investigative Services, including the Detective Bureau, Evidence/Property staff, Animal Services, and Community Service Officer Parking Enforcement. The Police Department typically responds to more than 50,000 calls for service annually, though calls have been lower during the pandemic. The Department Dispatch Center call volume is the fourth busiest in Santa Clara County (behind Santa Clara County, City

of San Jose and City of Santa Clara). Call volume is driven by the multi-disciplinary nature of Palo Alto's dispatch center which supports Palo Alto police and fire, Stanford Campus, Palo Alto Animal Services, and Palo Alto Utilities calls.

In summary, the Police Department was able to implement several important initiatives during 2021:

- Started the new Psychiatric Emergency Response Team (PERT)
- [Implemented a records management system](#) featuring electronic field reporting that improves staff efficiency and allows for implementation of the Racial and Identity Profiling Act (RIPA)
- Launched a new [Police Calls for Service Interactive Map](#)
- Continued focus on public communications and awareness including continuing responsiveness to inquiries from media partners
- Unveiled a [redesigned website](#) that is easier to navigate and that contains updated, refreshed information
- Collaborated with the Independent Police Auditor (IPA) to implement an expanded scope of services.

Additional details on these efforts and more are listed below:

Crime Statistics

While crime trends tend to be cyclical, overall, Palo Alto continues to have a very low rate of violent crime per capita (violent crime defined as homicides, rapes, robberies and assaults). Most classifications of crime cases are the same as or less than previous years. It should be noted that the ten-year trend has been increasing, consistent with national statistics.

The 24-hour dispatch center processed 137,642 total calls (which include all calls to police, fire, EMS, public works, utilities, animal control, and others) in calendar year 2021. A total of 38,346 were emergency calls placed to 9-1-1 or the cell phone emergency line; 99.44% of the 9-1-1 calls were answered within 10 seconds. The following represents calendar year activity (not fiscal year).

Work Activity	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Police Calls for Service	62,783	65,861	59,773	58,243	52,366	54,926	55,798	51,417	44,654	38,189
Offense Reports	5,607	5,764	6,058	6,729	5,534	5,938	5,715	5,611	4,665	4,588
Collisions Reports	1,001	1,173	1,108	1,025	969	952	993	836	446	523
Crimes										
Homicide	-	-	1	1	1	-	-	1	1	-
Rape	5	4	4	13	10	11	6	10	12	5
Robbery ¹	26	30	26	26	28	39	30	46	39	41
Assault	23	21	24	27	35	40	38	29	30	29
Burglary ²	332	242	273	212	221	215	234	179	243	179
Larceny-Theft ³	1,048	1,179	975	1,407	1,161	1,477	1,197	1,724	1,571	1,356
Stolen Vehicle	48	69	68	87	65	92	83	83	112	98
Arson	12	10	3	5	8	6	9	8	22	30
Totals	1,494	1,555	1,374	1,778	1,529	1,880	1,597	2,080	2,030	1,738

¹ Robbery is defined as the felonious taking of personal property in the possession of another, from his person or immediate presence, and against his will.

² This category includes commercial and residential burglaries, but not auto burglaries

³ This category comprises thefts, which include auto burglaries

Notable Incidents in 2021

To review public safety incidents in 2021, visit the Police Department's website and read the news releases at www.cityofpaloalto.org/PAPDnews.

Here are some highlights of the effective work that Police Department personnel performed in 2021:

- [Attempted murder arrest](#). Officers arrested a suspect who randomly attacked a juvenile female victim on a downtown Palo Alto street, stabbing her with a knife.
- [Organized retail crime arrests](#). Officers arrested two suspects immediately following a late-night commercial burglary attempt in downtown Palo Alto, where a group of 30 to 40 suspects in 20 cars arrived to commit the crime but were deterred by a prompt call from a security guard and a quick response by officers.
- [Arrest for shooting BB gun onto a school campus](#). Officers arrested a man who shot an elementary-school age child who was playing at recess with a BB gun fired from his own backyard.
- [Armed juvenile suspect arrested after robbery](#). Officers arrested a juvenile suspect and recovered a loaded firearm and drugs on him after he threatened and robbed a man who was walking his dog.
- [Armed robbery suspect arrested](#). Officers worked collaboratively with other law enforcement agencies to charge the suspect who committed an armed robbery at Baskin Robbins within two days of the crime, after he had committed other robberies in other cities.
- [Sexual assault suspect arrested](#). Officers arrested a suspect in a violent sexual assault that occurred in a downtown parking lot.
- [Robbery suspect arrested](#). Officer arrested a suspect after he beat and robbed an elderly man at the downtown train station.
- Hate crime arrests. Officers made unrelated arrests in two separate violent attacks on random victims that were apparently motivated by hate. Refer to news releases about those arrests [here](#) and [here](#).

Managing Current Budget and Staff Limitations

The [FY 2022 Adopted Operating Budget](#) lists details adopted by City Council (beginning on PDF page 357).

Authorized Positions											
by Division	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Administration	6.33	6.00	8.00	7.40	7.40	8.40	9.40	9.40	9.52	9.52	7.30
Field Services	66.30	71.80	68.80	66.80	68.80	61.80	73.55	73.55	73.55	73.55	64.15
Investigations	50.69	43.86	44.18	45.18	45.18	51.18	38.43	38.43	31.75	32.23	24.78
Technical	37.87	36.67	37.13	37.00	37.00	37.00	37.00	37.00	37.00	37.00	29.12
Total	161.19	158.33	158.11	156.38	158.38	158.38	158.38	158.38	151.82	152.30	125.35

Budget (in thousands)

Revenue	\$ 4,691	\$ 4,203	\$ 4,541	\$ 4,245	\$ 4,324	\$ 4,188	\$ 4,409	\$ 4,524	\$ 4,352	\$ 4,200	\$ 4,016
Staff Cost	\$ 26,599	\$ 27,149	\$ 28,091	\$ 29,314	\$ 31,810	\$ 32,029	\$ 35,293	\$ 36,134	\$ 38,814	\$ 35,229	\$ 37,461
Other Cost	\$ 5,319	\$ 5,183	\$ 4,482	\$ 4,762	\$ 5,049	\$ 6,108	\$ 7,040	\$ 6,214	\$ 5,852	\$ 5,147	\$ 5,654
Total Expenses	\$ 31,918	\$ 32,332	\$ 32,573	\$ 34,076	\$ 36,859	\$ 38,137	\$ 42,333	\$ 42,348	\$ 44,666	\$ 40,376	\$ 43,115

Since the [reduction of positions](#) (net 25.89 FTE) within the Police Department, initiated in FY 2021, City Council has restored, restarted or provided temporary resources for the Department to continue to focus on its main priorities focused on public safety and notably at the [February 7, 2022 City Council meeting](#), the City Council approved the Department to “hire-ahead” five (5) police officer candidates in anticipation of attrition.

Police and Diversity

The Department and City Management recognize the topic of Police and Diversity is important; the following work underway is just a sampling of the work underway at this time:

- The Independent Police Auditor (IPA), OIR Group, will [conduct a performance review of the Police hiring practices](#) and report back to the City Council
- The Department will work with the City Manager’s Office to engage an outside contractor to process RIPA data and report an analysis of the data to the City Council
- Staff continues to work on the demographic data dashboard which includes information on the racial and gender identities of all staff citywide including the Police Department

The Department has been actively recruiting for a broad applicant pool and continues to have success hiring staff with diverse backgrounds. Currently, as one form of highlighting the diverse backgrounds, the Department has 32 police staff who are cumulatively bilingual in 11 languages beyond English (Spanish, German, Korean, Russian, Mandarin, Urdu, Tagalog, Portuguese, Cantonese, Vietnamese, and Farsi). This is just one way the Department can better engage with the community.

Lastly, the City Manager, in the [listening sessions](#) on recruiting for the next Chief of Police, has heard many members of the community shared an interest in the new Police Chief keeping these topics of diversity, equity, and inclusion as a priority in the operations of the Department.

Independent Police Auditor (IPA) Revised Scope of Work

The IPA is an independent, third-party [contractor](#) who conducts secondary reviews of the Department’s investigations regarding police contacts, complaints and personnel. Historically, the IPA has reviewed three categories of Police Department investigations: (a) complaints from members of the public, (b) Department-initiated internal affairs investigations, and (c) all TASER deployments, regardless of whether a complaint was filed. At [City Council’s direction](#) the IPA’s scope of services was expanded in 2021 and now includes reviews of all of the following uses of force reports: where a baton, chemical agent, TASER, less-lethal projectile, canine, or firearm is used, and all cases where the subject’s injuries necessitate any treatment beyond minor

medical treatment in the field. The expanded scope of services also now includes review of internal complaints against sworn officers regarding misconduct related to harassment, discrimination, or retaliation. In addition, the IPA now attends and confers with City Council two times per year, following publication of the [IPA's report](#). The IPA can perform one audit of process each year – the most recent being an audit of police hiring practices.

[State law](#) requires all police agencies to receive and investigate complaints made by the public against police officers. However, having independent review of police investigations is a choice made by the City of Palo Alto in 2006 and is not required by law. While large agencies like the City of San Jose work with an independent police auditor, it is rare for smaller cities to retain a police auditor or contract for services. The IPA reviews police investigations for objectivity, thoroughness, and appropriateness of disposition, and can also make recommendations to the Police Chief regarding further investigation, processes, and dispositions. At the conclusion of the review, the IPA shares a public report with the City Council. As required by state law, the reports do not name or identify uniformed officers. It should be noted, members of the public have considerable discretion under the Brown Act when speaking in public comment and may name individual officers or speculate about particular Department personnel, however, members of the public should understand the IPA, City staff and Council Members, and Boards and Commission members cannot respond to requests from the public for information about individual officers in accordance with state law.

All reports dating back to the inception of the IPA in 2006 are viewable on the [Police Department's website](#).

Police Use of Force Annual Report

The City joined jurisdictions across the country in re-evaluating its approach to police accountability in the aftermath of the George Floyd murder and subsequent movement for change. As part of that, the City now publishes an annual report on uses of force (UOF) in conjunction with the February Independent Police Auditor (IPA) report. In the annual UOF report released by the Police Department on [February 14, 2022](#) (page 299), there are details on the types of physical force used since the last update. From November 16, 2020, until the end of 2021, PAPD officers used force requiring a “Supervisor’s Report on Use of Force” a total of 16 times. During this same period, Palo Alto Police Officers responded to 42,405 calls for service; this equates to officers using force on 0.03 percent of dispatched calls. See the full December 2020-December 2021 UOF report released by the Police Department [here](#).

Launch of Psychiatric Emergency Response Team & Other Mental Health Intervention Options

In November 2021, in conjunction with the Santa Clara County Behavioral Health Services Department, the Police Department launched a Psychiatric Emergency Response Team (PERT). PERT consists of a police officer partnered with a license mental health clinician, combining the unique resources available from each profession to provide the highest possible level of service to someone in mental health crisis before the situation worsens or requires hospitalization. PERT is tasked with responding to calls for service involving people in acute mental health crisis

and getting them the help they need in the most comprehensive and compassionate way possible. PERT is an important element in furthering the City's Race and Equity priorities by reinforcing Palo Alto's commitment to supplementing law enforcement response options.

Palo Alto is the second law enforcement agency and first city in the County to launch a PERT team; earlier in 2021, the Santa Clara County Sheriff's Office became the first and is currently fielding two PERT teams. Future teams are planned in other cities and Palo Alto will have to wait for access to a second County clinician.

PERT also serves as the Police Department's regular main point of contact for long-term and ongoing concerns with the City's unhoused population. PERT also conducts follow-up visits on past clients as necessary and accepts referrals from other Police Department employees who encounter someone who may benefit from the services of the team. PERT self-responds to appropriate calls throughout their shift and can also be summoned by a police supervisor to any scene where their expertise would be of benefit. The team operates in an unmarked police car, with the assigned officer wearing a plainclothes-style uniform to be distinct from a regular patrol officer.

In the first full four months of the team's operation, the team handled 99 calls for service, conducted 68 follow-up visits on past clients, offered resources to 87 additional people, placed 20 people on involuntary psychiatric evaluations, facilitated 6 voluntary psychiatric evaluations, and diverted 22 people from what likely would have been psychiatric hospitalizations. The team has not had to make a single criminal arrest, and has not used any form of force at any time. The Police Department and the Santa Clara County Behavioral Health Services Department will be conducting robust analysis of all PERT statistics as the team's operation continues.

The City successfully advocated to be included in [Santa Clara County's new Community Mobile Response Program](#) — known as the Trusted Response Urgent Support Team (TRUST) — which is a non-law enforcement response resource for lower-level mental health crises. The program seeks to de-escalate crisis situations and divert individuals away from hospital emergency rooms or jail, and toward alternative means such as counseling, a sobering center, a respite program or mediation through a crisis stabilization unit. This program continues to be developed by the County. Palo Alto staff stays in contact with the County staff about the implementation. In addition to the PERT program and the TRUST program, the County is also adding an additional Mobile Crisis Response Team (MCRT) in north county. New staffing, expected to start this summer, will serve north county and west foothill areas, which include Los Gatos, Monte Sereno, Palo Alto, Los Altos, Los Altos Hills, Mountain View, Cupertino, Saratoga and portions of San Jose.

Launch of New Records Management System and Data Collection

In December 2021, the Department launched an updated internal records management system (RMS). This robust system allows personnel to complete their reports electronically, reducing paper waste and increasing staff efficiency. Officers are now able to complete their reports

digitally, in their patrol cars or the police station, and submit them to supervisors electronically for review and to our Records Unit for data entry. This replaces the previous paper-based process. The launch of this new system was a major endeavor requiring multiple days of training for all staff, and promises to provide benefits for years to come. The RMS database also provides an interface for officers to comply with the provisions of [RIPA](#).

RMS was designed to comply with the Racial and Identity Profiling Act (RIPA) – AB953. This state law requires state law enforcement agencies to collect and report on 16 different data elements on every police contact (including perceived race) and the reason for the contact. Since January 2022, the data is collected and reported to California Department of Justice (DOJ) at the end of every shift per policy. Annually, the data is compiled by a separate board, the [RIPA Board](#), and reported to the public. Agencies the size of PAPD will be added to the report published in or around April of 2023. Palo Alto data will be reported with all law enforcement agencies in the state so the Department plans to provide City Council with a summary report of Palo Alto specific data. By the end of January 2022, PAPD had submitted approximately 353 stop data records. This is a very important step in helping the City of Palo Alto to collect accurate racial identity data for Police contacts with members of the public.

Option for Public to File Police Reports Online Continues for First Full Year

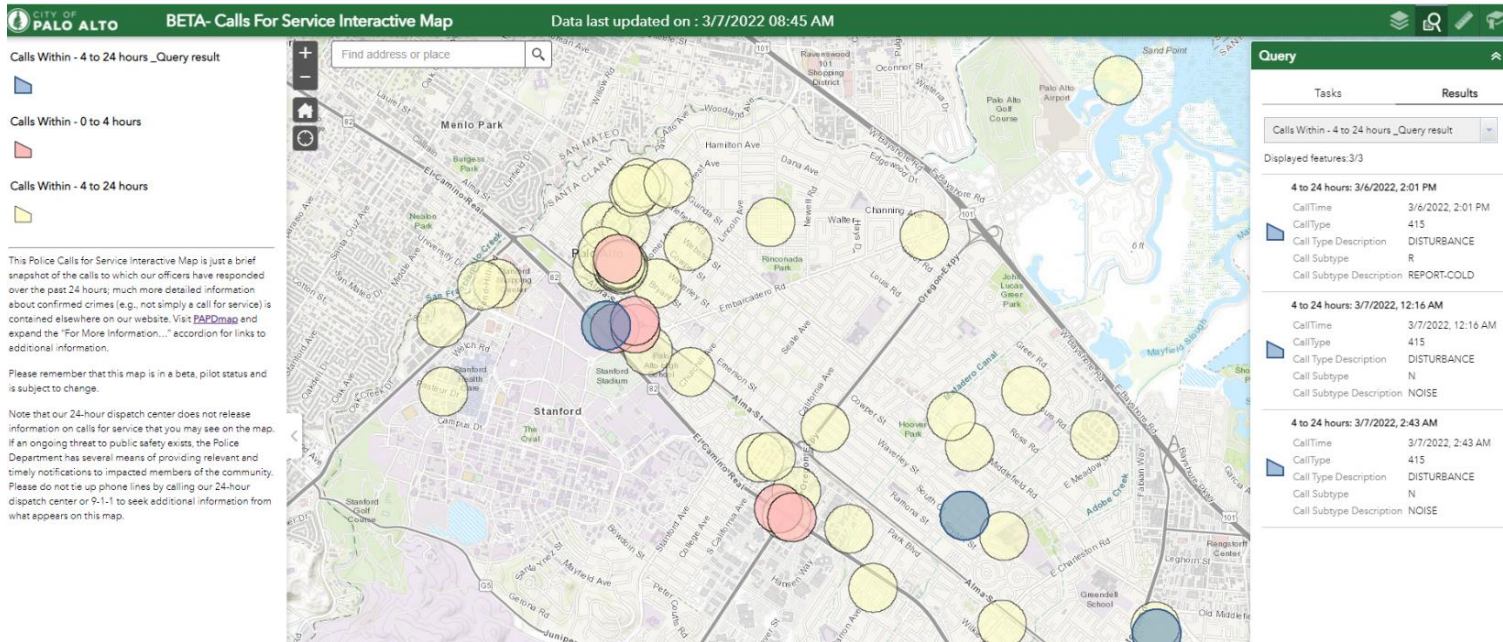
In December 2020, the Police Department launched a new online reporting tool, giving the public the ability to file their own online police reports for a wide array of minor crimes and non-injury traffic collisions. The tool has been extremely well-received by the public and has been widely used during 2021: the system received 1,340 reports filed online, increasing convenience for the public and saving approximately 2,010 hours of officer time. This creates efficiencies for officers and Community Service Officers to respond to more urgent calls for service. For access to the online reporting tool, visit www.cityofpaloalto.org/onlinereports.

Launch of Police Calls-for-Service Interactive Map

The Department launched a new online interactive map, providing a near real-time snapshot of the types and locations of calls for service to which Palo Alto police officers have responded over the past 24 hours. The map offers enhanced community awareness on police calls for service while protecting personal identifying information and was developed as an alternative after the California Department of Justice required encryption of police radio transmissions containing personally identifiable information and protected criminal justice information (See Attachment A for further information).

The Police Calls for Service Interactive Map, available for viewing now at www.cityofpaloalto.org/PAPDmap, draws data directly from the Department’s Computer-Aided Dispatch (CAD) system. It shows the general locations of calls for service from the community, and displays the time the call was received, the call type, and a subtype if applicable. The calls are displayed once the incident is closed to provide the most accurate information and remain visible for 24 hours. The vast majority of the Department’s calls for service are closed within an hour. The exact geographic location of the call is not provided to ensure the confidentiality of possible crime victims.

The new interactive map was a concept discussed last year and since that time, City staff have



been developing the online prototype. The pilot platform offers a new online look at calls for service that builds on the Police Department’s key priorities including increasing public information, building community awareness and furthering the community’s understanding about public safety services in Palo Alto.

While several municipal police departments in the Bay Area provide some level of police call data online, the Palo Alto Police Calls for Service Interactive Map offers more call details at near real-time than these other online platforms.

Continued Handling of Media Inquiries While Managing Constrained Resources

The Department conducted an internal review of its responsiveness to media inquiries. After monitoring the process and activity for several months, the examination revealed that for the vast majority of media inquiries, reporters receive a response the same day, often within 90 minutes. By way of recent example, in February 2022, the Police Department received 33 separate inquiries from the media. Over 90% of those (30) received a response from a Public Information Officer the same day; for the remaining three, the inquiries received a response the following day. The longest response time to any inquiry in February was about 18 hours.

One-third, or 33% (11 of 33), of the total inquiries received a response within 30 minutes, and 64% (21 of 33) received a response within 90 minutes. In 82% of the inquiries (27 of 33), the Public Information Officer sent a response via e-mail to the reporter; in the remaining 18% of the inquiries (6 of 33), they called the reporter on the phone.

The Police Department offers an online [Media Request Form](#) or [Public Information Portal](#) that includes the [Police Report Log](#) - published every weekday. Local press organizations are aware they have access to designated police personnel who can respond to press inquiries every day of the week, as outlined by Chief Jonsen in a [May 21, 2021 post](#):

"...three things occurred to cause us to transition to a new temporary operating procedure for handling media inquiries: the elimination of the Public Affairs Manager position; a renewed commitment to have our sergeants in the field actively supervising our field personnel (not in the police station, reviewing reports to distill the legally-releasable information); and a necessity to have our officers in the field responding to calls and conducting patrols due to reduced staffing levels. As a result, we re-assigned public information duties to our two patrol Watch Commanders, police lieutenants who have command responsibility over our patrol division.

New Expedited Web Form Process Deployed

We appreciate the media's flexibility in using a web form to submit their initial request. This helps us immediately route the information to those charged with responding, so they can research the inquiry and respond to the reporter. Our Watch Commanders strive to answer the inquiry as soon as they can, and the responses most often occur within 24 hours (and frequently within a handful of hours). This is the same timing as before our staffing reductions. Of course, responses are quicker on a police incident where there is a danger to public safety, or on a case where we have proactively distributed a news release. The web form allows us to keep track of the inquiries to ensure they are handled properly and in a timely way. Reporters who have follow-up questions are welcome to continue the conversation with the Watch Commander who responds to their inquiry, to ensure that all of their questions are appropriately addressed, and they have the information they need to complete their story."

Sharing Critical Alerts with the Community

Implemented Department of Justice Requirements Related to Personally Identifiable Information (PII)

Staff is prepared to discuss aspects of radio encryption with the City Council on April 4, 2022 including ways that the Department ensure the public and media have real time information about the Department's calls for service. **Attachment A** provides more details about this topic for City Council discussion and consideration.

In summary, in early 2021, the [Palo Alto Police Department](#) encrypted its radio transmissions to comply with a mandate from the [California Department of Justice](#) that requires all California law enforcement agencies to protect personally identifiable information. The Palo Alto Police Department was not the first law enforcement agency in Santa Clara County to comply with this

state mandate, and since that time, every law enforcement agency in Santa Clara County is using encryption.

The California Department of Justice mandate is designed to protect the privacy of the people with whom law enforcement officers may come into contact. Personally identifiable information includes such things like names, driver license numbers, and social security numbers. The DOJ policy also mandates protection for Criminal Justice Information, which is confidential information contained in federal and state criminal justice databases. When broadcast on an open and unencrypted radio frequency, PII and CJI can be accessed and used for any purpose by anyone using a commercially-available radio scanner. Using an encrypted radio frequency to broadcast this information safeguards that information. The Department of Justice bulletin describing these mandates, can be viewed [here](#).

As noted earlier, the Police Department continues to respond to press inquiries for public information; produce [a police report log](#) every business day; distribute [news releases](#); post information on the City's website like [crime statistics](#), [monthly activity reports](#), [Policy Manual](#); and, manage many [social media platforms](#) to ensure the public is aware of police activities and ways to stay safe.

Popular Web Links in 2021

[2022 Operating Budget](#)

[2021 City Council Study Session on PAPD](#)

[Police Public Information Portal including News Releases](#)

[Psychiatric Emergency Response Team \(PERT\)](#)

[Hate Crimes and Incidents](#)

[Police Accountability](#)

[PAPD Policy Manual](#)

[PAPD Contacts](#)

[2019 PAPD Annual Report](#)

Resource Impact

The Department used over 100 hours of staff time to create this report and accompanying attachments. No other resources are being requested at this time.

Stakeholder Engagement

For Attachment A, staff communicated with the California Department of Justice, SVRIA, regional and statewide agencies, Palo Alto Police Officers Association, State Senator Becker's office, and the City Attorney's Office while receiving feedback from community and media partners.

Environmental Review

The recommended action is not considered a Project as defined by the California Environmental Quality Act.

Attachments

Along with the PAPD Annual Report, the Department is taking this opportunity to discuss Radio Encryption. Attachments A and B provide context for that conversation.

Attachments:

- **Attachment16.a:** Attachment A: Background on Palo Alto Police Radio Encryption
- **Attachment16.b:** Attachment B: DOJ CJIS Notification

Report on Radio Encryption

Executive Summary

The following report provides details to the encryption of Palo Alto Police Department's radios and the complexity on this topic. Department discussions with DOJ confirmed that agencies that had the technical capability and infrastructure in place to transmit [Personally Identifying Information](#) (PII) and [Criminal Justice Information](#) (CJI) radio transmissions over encrypted channels must do so, to protect confidential information. In response to the DOJ mandate released in October 2020 (Attachment B), and, along with the Silicon Valley Regional Interoperability Authority partners (all police agencies in Santa Clara County), the City updated the law enforcement radio channel to an encrypted frequency to conduct law enforcement operations in January 2021.

Based on the continued conversations with local law enforcement agencies, regional partners and the State DOJ, it is staff's conclusion that there are no other feasible options available at this time to implement "unencrypted" radio transmissions. It should be noted that this issue is fluid and even as early as last week, state lawmakers have introduced legislation that could change the legal requirements on this issue. At this time, however, to help inform the City Council on this complex issue, staff does not recommend changes to the operational decision to encrypt radios, as there are other options to providing public information in near-real time.

In addition, the potential impacts of not abiding by the State mandate include:

- Risk losing law enforcement database ([California Law Enforcement Telecommunications System](#), or CLETS) access, which is the database all law enforcement agencies use to support investigations and ensure the safety of local communities
- Risk of jeopardizing the City's regional partnership with Mountain View and Los Altos (who share the Records Management System with Palo Alto)
- Financial risk of having to move to the City's own radio network outside the Silicon Valley Regional Interoperability Authority, which all Santa Clara County law enforcement agencies participate in
- Staffing impacts and risks associated with operational and financial efficiencies lost by reverting back to unencrypted radio channel, affecting 9-1-1 dispatchers and police officers

Background

The Policy and Services Committee (P&S) met on [February 8, 2022 to receive an update on Race and Equity work since September 2021 and the Committee discussed staff's update](#). An outcome of that meeting included four recommendations to City Council from the Committee and one of them was item D: Request the City Manager and Mayor schedule a study session to discuss police radio encryption, and how best to allow the public and the media to be rapidly informed for calls to service.

The item before the City Council on April 4, 2022 regular City Council meeting is the Police Department's annual report with an update on encryption and the City Manager set the discussion as an action item to enable the City Council to take action should it wish to do so.

Report on Radio Encryption

The table below summarizes the timeline for the State and the City of Palo Alto related to Police Radio encryption. This is useful context for the additional information about encryption included within this attachment.

Encryption Timeline

Date	Action
June 2018	Palo Alto moved from analog radio to a P25 digital radio system
October 2020	The CA Department of Justice (DOJ) sent notice to all law enforcement agencies re: data confidentiality. DOJ instructed agencies to submit implementation plan
December 2020	Palo Alto responded to DOJ notice as required
January 2021	SVRIA agencies (including PA) began encrypting police radios
January 2021	Staff began work on alternatives to police radio encryption
March 2021	Palo Alto sent DOJ a request for permission to temporarily reverse encryption of police channels
July 2021	DOJ responded via letter to Palo Alto – request denied
February 2022	New Calls for Service Interactive Map went live
March 2022	Staff met with Senator Becker staff to discuss Becker’s proposed legislation (Senate Bill 1000) on police radio encryption

Further Information on Encryption

The following information provides details on radio encryption to assist the City Council discussion on this topic.

Introduction

The California Department of Justice (DOJ), the primary law enforcement agency in the state, is directed by the State Attorney General (AG) who receives their authority from [Constitution of California](#), Article V, Section 13. On October 12, 2020, the agency sent notice (Attachment B) to all law enforcement agencies that access the California Law Enforcement Telecommunications Systems (CLETS – defined later) instructing that agencies *“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.”*

Further, the bulletin instructed agencies to prevent access to sensitive information by unauthorized persons including discontinuing the practice of broadcasting certain personal information over publicly accessible channels. Per the notice, *“Personal Identifying Information (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...such as Social Security number, passport number, military identification number and other unique ID numbers issued on a government document.”*

Report on Radio Encryption

The bulletin refers to established State of California [rules and policy](#) about unauthorized access to personal information through the database directly stating:

1.6.4 Confidentiality of Information from the CLETS

*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.*

It is required that each employee/volunteer/private contractor sign an Employee/Volunteer Statement form...prior to operating or having access to CLETS terminals, equipment or information. This form addresses confidentiality, release and misuse of information from the CLETS.

- A. *Information from the CLETS is on a “right-to-know” and “need-to-know” basis.*
- B. *Authorized personnel shall not inquire into their own record or have someone inquire for them.*
- C. *Accessing and/or releasing information from the CLETS for non-law enforcement purposes is prohibited, unless otherwise mandated, and is subject to administrative action and/or criminal prosecution.*
- D. *Pursuant to the PPP § 1.10.1D, all investigations of misuse must be reported to the CA DOJ on the CLETS Misuse Investigation Reporting form...including investigations where misuse was not found.*

The DOJ notice stated that compliance is additive to the requirements of the [FBI CJIS security policies](#). The notice states the policies can be met by either broadcasting PII and CJ information over encrypted radio channels or for agencies to establish policies that restrict the dissemination of PII and CJ information over the radio “if unable to implement the required technology.” Department discussions with DOJ confirmed that agencies that had the technical capability and infrastructure in place to transmit PII and CJ radio transmissions over encrypted channels must do so, to protect confidential information. Agencies that did not have a radio system in place that could be encrypted were being given the option of temporary policy modifications to comply with the mandate, as confirmed by a [transcript](#) of the [AG’s committee](#) that oversees the CLETS system.

Regional Partnerships and Radio Encryption

Additionally, the Department is a member of the Silicon Valley Regional Interoperability Authority ([SVRIA](#)), which provides access to the regional radio network titled Silicon Valley Regional Communication System (SVRCS). In June 2018, the Department moved the City radio operations from an analog radio system to a P25 digital radio system in accordance with [Council action](#). Digital systems such as SVRCS have a number of advantages over analog systems including inter-agency communication, stability, operator identification and encryption – all

Report on Radio Encryption

initiatives that came out of the 9/11 disaster. Not all agencies in the state have converted to digital, but all agencies in Santa Clara County have converted to digital. In response to the DOJ mandate the City updated the law enforcement radio channel to an encrypted frequency to conduct law enforcement operations in January 2021.

Staff Efficiencies Related to Radio Encryption

Two-way radio systems are used to communicate with dispatchers or other police officers efficiently and safely while doing work with their hands or allowing their hands to be free to respond to an immediate threat. Other means to communicate exist, such as cell-phone or in-car computers, but these methods do not always provide a safe opportunity to be used in police work.

In circumstances where an officer is required to manipulate a device not attached to their body or go inside their police vehicle to use the computer, it can take the officer's attention away from a subject and also require the dispatcher to have to answer another phone call (increasing the call volume into the communications center). Both issues are mitigated by the use of a radio and significantly reduce the officer safety concerns associated with using a phone or in-car computer. Radios not only require minimal hand manipulation, but also allow for a police officer to keep their eyes on their work or on a subject so that they can remain focused on sensitive or dangerous work or imminent threats while communicating and problem solving.

Further Communications with DOJ

On March 8, 2021, as a result of stakeholder feedback, the Department sent a letter to DOJ requesting permission to revert law enforcement radio operations back to an unencrypted channel through the end of 2021, to allow for time to explore alternative options. (Attachment B). On July 2, 2021, DOJ Chief Joe Dominic responded to the request in writing informing the Department it cannot revert to the previous practice of broadcasting PII over a publicly accessible radio channel (Attachment B). Further, Department communications with DOJ confirmed that willfully disregarding the CJIS policies could result in the Chief of Police being called before the [CLETS Advisory Committee](#), the AG's committee overseeing CLETS. CLETS is the state administered computer network that gives authorized agencies access to multiple state and federal databases containing information on criminal records, criminal justice status (persons or vehicles with warrants), missing persons, protective orders, restraining orders, driver's license and vehicle/vessel information, stolen property, stolen vehicles, firearms registration, and other restricted databases. DOJ stated, depending on the Chief's testimony and other evidence, the CLETS Advisory Committee could recommend that the Attorney General deny Palo Alto access to CLETS. To add another layer of complexity, Palo Alto derives its CLETS access through the City of Mountain View, for now, but possibly through Santa Clara County in the future, subject to agreement. Police departments must enter and retrieve information in CLETS to conduct daily operations. There is no other alternative to this system (besides not having the information). After discussing the risks to the City related to this issue, staff has complied with the DOJ notice.

Report on Radio Encryption

Review of other law enforcement agencies response to DOJ

The San Francisco Police Department, in December 2021, transitioned all law enforcement radio communication to a digital radio network using fully encrypted channels. Staff understands that prior to their decision to encrypt, the department examined alternatives that placed additional responsibilities on dispatchers; this was ultimately not pursued. The California Highway Patrol (CHP) law enforcement operations are operating on a VHF low band analog radio system that is not capable of encryption. CHP has modified its radio transmission policies to comply with the Department of Justice policies and procedures to the extent possible with the technological constraints of its analog radio system. This option is not available to the City of Palo Alto. In March 2021, the Palo Alto Police Department asked the Department of Justice to allow the department to move law enforcement radio communications back to an unencrypted channel and DOJ denied the request. Staff has invited DOJ and CHP representatives to participate in the Council's discussion of this matter, and will advise if representatives will attend.

Staff Work on Alternative Methods: New Beta Interactive Map Released & Other Methods for Real-time Calls for Service Information

After complying with the DOJ notice, Police Department staff looked into alternative methods for providing the public greater awareness and visibility on police activity (real-time calls-for-service information or CFS) besides over the radio frequencies. The Department's actions included engaging technology companies and making inquiries to other law enforcement agencies. A technology company providing a platform for fire department CFS was unwilling to pursue staff's request to do the same for law enforcement. Department staff also contacted multiple law enforcement agencies throughout the state to inquire how they were complying with the DOJ mandate. This outreach included agencies using digital, encrypted radio channels and low-band unencrypted radio channels. The Department also utilized a statewide law enforcement discussion board to inquire how other law enforcement agencies were providing visibility on police activity in light of DOJ's directive. Sustainable solutions were not identified. Along with this track of activity, City staff was exploring the possibility of making a custom solution.

To meet stakeholders' desire to receive more information about the calls-for-service (CFS) the police respond to in real-time, the City moved forward with a portal to display CFS on an [interactive map](#). CFS, for police, include all requests for police assistance from the public based on the reporting party's initial need or concern, regardless of final disposition or categorization of the CFS (example: initial CFS could be a residential intruder alarm notification but the police investigation revealed it was a false alarm). The development of this interactive display was a months-long collaboration involving the Police Department, City Manager's Office, City Attorney, Information Technology Department, Human Resources Department, and the Palo Alto Police Officers Association. The creation of the platform was completed by City IT staff, working within the limitations of the City's antiquated Computer Aided Dispatch (CAD) system. (Note: CAD modernization is an upcoming item for City Council to consider soon). The parameters of the interactive map adapted to community member privacy concerns as well as police officer-safety concerns. The result of this process was a display map that gives near real-time information on police response to CFS with consideration for PII/CJI privacy requirements

Report on Radio Encryption

and officer safety concerns. Few law enforcement agencies display this type of information in real-time, often opting to share information in a [“press log,”](#) often 24-48 hours after the CFS.

Other Discussions Ongoing

Further, City staff, including Police staff, met with a representative of State Senator Josh Becker’s office to discuss radio encryption and provide input on potential legislation that would address making radio communications accessible to the public. Senate Bill (SB) 1000 is Senator Becker’s recently-introduced bill on public access to police radio transmissions. Staff is reviewing the bill. In the coming weeks, the Legislative Analyst will prepare an analysis of the bill and its impacts, and stakeholder comments will be received.

As noted, the subject of encryption throughout California is still fluid. The City of Palo Alto, and particularly the Police Department, is committed to protecting the privacy of all those the Department interacts with including suspects, drivers, passengers, witnesses, and victims while staying up to date on methods for informing media partners and the public in real-time.

Specific Questions Answered

What information is broadcast on a police radio channel?

Public Safety Answering Points (PSAPs) are another name for dispatch centers. PSAP’s receive their authority to operate and policies from the [State](#). The City of Palo Alto PSAP serves emergency and non-emergency requests for service (CFS) for Palo Alto Police, Palo Alto Fire, Palo Alto Public Works and Utilities, Stanford DPS Police, and Animal Control and serves as a back-up PSAP to Mountain View and Los Altos.

For emergencies requiring a police response, the Dispatcher receives requests for service through a number of methods including email, text, voice (landline and cellular), and radio. For phone requests, which comprise of an estimated 95% of service requests, the Dispatcher listens to caller information, enters the initial service request into the Computer Aided Dispatch (CAD) database. For emergencies or other public safety needs, police and/or fire operators are dispatched. “Dispatched,” in the case of police CFS, refers to transmitting the call-for-service over the police radio channel to assigned police units. The information broadcast gives the exact location of the request (if possible), the reported circumstances of the event, possible officer safety concerns, and specific call information, such as subject descriptions, victim actions/injures, and other important information the officer needs to respond to the call. The CAD database sends some of this information to the responding officer’s in-car computer. During in-progress calls (calls that have a higher sense of urgency), updated information continues to be broadcast to responding officers. Further, officers communicate with Dispatchers and other officers, including other agencies, using the radio. At any time during dispatched calls, when time is of the essence, PII/CJI information of involved parties may be broadcast when known or relevant including criminal record information even before an officer arrives on the scene and contacts an involved person. In FY 2021, Palo Alto had approximately 12,000 of such “in-progress” calls-for-service – 32/day.

Report on Radio Encryption

Once at the scene of the request, field officers will ask Dispatchers, via the radio, to provide information relevant to the incident including personal information related to detainees, suspects, victims, injured parties, witnesses or their property and vehicles and their drivers. Dispatchers and officers will communicate back and forth during the duration of the call. Other officers, while not directly in the conversation, can hear the exchange of information and provide assistance as needed – something not achievable via telephone or SMS text. Because of the rapidly unfolding, unpredictable and dangerous nature of police work, once an officer is away from their vehicle and engaged with a subject(s), their ability to obtain critical information, including PII/CJI, is most safely done via the radio. Other means of receiving this information can put the officer and the public at risk.

The tactical positioning of officers is also arranged and broadcast over the police radio. Field supervisors direct officers to certain locations as necessary for the emergency. Other tactical information, such as type and manner of response, the creation of tactical response teams, and direction on weapon deployment may also be coordinated over the police radio. There may be times when it is in the public's best interest not to have this information broadcasted, such as during active shooter calls or crimes involving a criminal with more sophistication.

What was the effect of encryption?

Before January 5, 2021, Palo Alto's law enforcement communication channels were available for the public to listen to, through personally-owned radios or radio frequency scanners. By complying with the DOJ CJIS mandate of only authorized persons being able to listen to personal information transmissions, the public and media were no longer able to hear Palo Alto Police radio transmissions. The mandate resulted in the protection of community members' PII/CJI, medical/injury information (HIPAA), and sensitive CFS information. Media outlets and community members who wish to monitor police activity have been impacted by not having police radio transmissions open for monitoring. However, earlier this year, the City has launched a beta system sharing near-term details on calls for service online. Staff continue to make adjustments to the system to support additional public information about calls for service.

How can the media stay informed on real time incidents?

Local media stakeholders communicated they rely on the scanner radio traffic to monitor police activity and respond to crime scenes to gather information for reporting on events. While the interactive CFS map display is one way the police department has provided the media with information about police activity, the department also provides additional sources of information including [press releases](#), [social media](#) (including [Nixle](#)), and the [daily PAPD Police log](#). [AlertSCC](#) is another method of receiving real-time information. The department respects and takes seriously the public's desire to be informed about daily police operations and strives to provide information in manner that is timely and reaches the biggest audience.

Report on Radio Encryption


The Police Department has been examining its responsiveness to media inquiries for several months now. That examination reveals that for the vast majority of media inquiries, reporters receive a response the same day, often within 90 minutes. This is actually an improved response time over the way media inquiries were handled with the Public Affairs Manager and on-duty field personnel.

By way of recent example, in February 2022, the Police Department received 33 separate inquiries from the media. 91% of those (30) received a response from a Public Information Officer the same day; for the remaining three, the inquiries received a response the following day. The longest response time to any inquiry in February was about 18 hours. 33% (11 of 33) of the total inquiries received a response within 30 minutes, and 64% (21 of 33) received a response within 90 minutes. In 82% of the inquiries (27 of 33), the Public Information Officer sent a response via e-mail to the reporter; in the remaining 18% of the inquiries (6 of 33), they called the reporter on the phone.

Based on all the information provided within this report, staff does not recommend any changes to the Palo Alto police radio encryption. Alternatives that could be considered further, but that do not appear actionable at this time, include:

- Adding dispatcher personnel dedicated to the handling of PII communications or alternatively to broadcasting filtered reports of ongoing calls for service. At this time, the City of Palo Alto is challenged to fill and maintain dispatch staffing at authorized levels. Staff does not believe that the addition of positions to specifically address radio encryption would be a viable option given operational and financial constraints.
- City support of SB 1000. As this legislation was just recently introduced, staff recommends deferral of a City position until the state's Legislative Analyst publishes its evaluation. At this time, it is not clear what additional tools may be provided by state legislation to address the requirements established by DOJ for CLETS access.
- Restoration of non-sworn personnel to handle media inquiries could be considered. As described in this report, the Police Department has been able to establish a high level of responsiveness to media requests. The addition of non-sworn personnel in other functions such as responding to public requests for records would be recommended as a higher budgetary priority.

Xavier Becerra, Attorney General

<p>California Department of Justice CALIFORNIA JUSTICE INFORMATION SERVICES DIVISION Joe Dominic, Chief</p> 	<h1>INFORMATION BULLETIN</h1>	
<p><i>Subject:</i></p> <p>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></p> <p>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.

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 CJJ (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 CJJ database information and combinations of name and other data elements that meet the definition of PII. This will provide for the protection of CJJ 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



POLICE DEPARTMENT
275 Forest Avenue
Palo Alto, CA 94301
650.329.2406

12/10/2020

CLETS Administration Section
California Department of Justice
916-210-4240/CAS@doj.ca.gov

Palo Alto Police Department
275 Forest Ave.
Palo Alto, CA 94301

December 10, 2020

CLETS Administration Section,

Pursuant to CAL DOJ Information Bulletin 20-09-CJIS, dated October 12, 2020, the Palo Alto Police Department is responding to your inquiry on the confidentiality of information from the California Law Enforcement Telecommunications System (CLETS).

The Palo Alto Police Department Public Safety Answering Point (PSAP) provides law enforcement communications for the Palo Alto Police Department and the Stanford Department of Public Safety. Our department utilizes a P25 Phase II TDMA digital radio system administered by the Silicon Valley Regional Interoperability Authority (SVRIA), a Joint Powers Authority. Our primary law enforcement channel is currently NOT encrypted.

To comply with the directive of CLETS PPP section 1.6.4 and FBI CJIS Security Policy sections 5.10.1.2, 5.10.1.2.1, and 5.13.1, the Palo Alto PSAP will change our law enforcement communications channel to one that is encrypted. This switch to an encrypted digital radio channel will occur on January 5, 2021, to allow time to communicate with all departments affected by the change. We will, upon radio frequency reprogramming, encrypt our primary law enforcement channel to have fully encrypted channels for all of our operations.

Please contact Technical Services Division Captain April Wagner at april.wagner@cityofpaloalto.org if you have any questions. Thank you for your consideration.

Respectfully,

DocuSigned by:
Chief Robert Jonsen
774FACF6E4B94A5

Palo Alto Police Department



POLICE DEPARTMENT
275 Forest Avenue
Palo Alto, CA 94301
650.329.2406

3/8/2021

Chief Joe Dominic

March 8, 2021

California Justice Information Services Division

California Department of Justice

Chief Robert Jonsen

Palo Alto Police Department

275 Forest Ave. Palo Alto, CA 94301

Robert.jonsen@cityofpaloalto.org

Chief Dominic,

In October 2020, the City of Palo Alto and the Palo Alto Police Department received DOJ letter, 20-09 CJIS, inquiring if agencies were compliant with CJIS security policies and asking for a plan to become compliant concerning not broadcasting PII information over non-encrypted channels. Due to our investment in digital radio infrastructure, on January 5, 2021, the City of Palo Alto and the Palo Alto Police Department moved our digital primary law enforcement radio channel to an encrypted channel to comply with state and federal regulations. This was the department's only feasible timely option and the transition was successful with us coming into compliance.

The City of Palo Alto is requesting guidance on if we can revert our primary law enforcement radio channel back to a non-encrypted channel, while alternative options are explored, to allow for greater transparency with the public. This will result in PII information being broadcast on a non-encrypted channel. The City of Palo Alto would remain on a publicly accessible channel until December 31, 2021, unless a viable alternative has been identified before that date. Any changes in this status would be immediately communicated to DOJ.

We respectfully ask for your guidance and recommendation to this request in writing. Thank you.

Regards,

Chief Robert Jonsen, Palo Alto Police Department

Robert.jonsen@cityofpaloalto.org

ROB BONTA
Attorney General

State of California
DEPARTMENT OF JUSTICE



P.O. Box 903387
Sacramento, CA 94203
Telephone: (916) 210-5000
Joe.Dominic@doj.ca.gov

July 2, 2021

Robert Jonsen, Chief
Palo Alto Police Department
275 Forest Avenue
Palo Alto, CA 94301

Via email: Robert.Jonsen@cityofpaloalto.org

Re: Radio Encryption

Dear Chief Jonsen:

Thank you for your letter dated March 8, 2021, regarding encrypting your digital primary law enforcement radio channel to comply with state and federal regulations. First and foremost, I want to apologize for the delay in responding to your request. Your letter requested guidance regarding reverting your primary law enforcement radio channel back to a non-encrypted channel, while exploring alternative options to allow for greater transparency to the public. Your letter also indicated that if it was reverted, Personal Identifying Information (PII) would be broadcast on a non-encrypted channel.

Your request was presented to the Department of Justice's legal team, which after careful review, concluded that the City of Palo Alto is required to comply with state and federal rules on the encryption of Criminal Justice Information (CJI) and PII, as provided in Information Bulletin 20-09-CJIS (attached herein for reference). The City of Palo Alto cannot revert back to their previous system and broadcast PII on a non-encrypted channel that can be accessed by unauthorized individuals.

If you would like to discuss this further, please do not hesitate to contact us.

Sincerely,

A handwritten signature in black ink, appearing to read "Joe Dominic", with a long horizontal flourish extending to the right.

JOE DOMINIC, Chief/CIO
California Justice Information Services Division

For ROB BONTA
Attorney General



SUPPLEMENTAL REPORT – ITEM 16

MEETING DATE: **APRIL 4, 2022**

TO: **HONORABLE COUNCIL MEMBERS**

FROM: **ROBERT JONSEN, CHIEF OF POLICE**

SUBJECT: **AGENDA ITEM NUMBER 16 - Receive the Police Department’s Annual Report and Discuss and Accept the Staff Update on Radio Encryption as a Follow-up from the Policy and Services Committee Recommendation on February 8, 2022**

Below is a letter received from Silicon Valley Regional Interoperability Authority (SVRIA) regarding police radio operations in Santa Clara County for context.



Silicon Valley Regional Interoperability Authority

DATE: March 31, 2021

TO: Bob Jonsen, City of Palo Alto Police Chief

FROM: Eric Nickel, SVRIA Executive Director

SUBJECT: **SVRIA and Encryption Background and Analysis**

EXECUTIVE SUMMARY

Since 2001, the City of Palo Alto (Palo Alto) has been a member of a countywide organization dedicated to facilitating interoperable voice and data communications for public safety and public service providers within Santa Clara County known as Silicon Valley Regional Interoperability Authority (SVRIA). Palo Alto joined SVRIA shortly after the September 11, 2001 terrorist attacks highlighted the need for shared, regional and interoperable radio communications between public safety officials from local, state and federal agencies.

SVRIA is comprised of the County of Santa Clara; the Cities of Campbell, Cupertino, Gilroy, Los Altos, Milpitas, Monte Sereno, Morgan Hill, Mountain View, Palo Alto, Santa Clara, San Jose, Saratoga, and Sunnyvale; the Town of Los Gatos; the South Santa Clara County Fire District; San Jose State University, Foothill/DeAnza College District, San Jose/Evergreen College District, West Valley/Mission College District; the Santa Clara Valley Water District, and the Valley Transportation Authority (VTA).

SVRIA operates the Silicon Valley Regional Communications System (SVRCS). In calendar year 2021, the SVRCS broadcast 23.5 million transmissions from 11,365 mobile and portable radios and authorized connections to 7,830 mutual aid operators representing federal, state and local public safety agencies through regional interoperable talkgroups.

In February 2010 and again in November 2016, Palo Alto agreed to and signed the Joint Powers Authority (JPA) agreement that established the SVRIA. Palo Alto contributed to the radio system design, selection of the primary vendor, and implementation of the radio network. Today, Palo Alto staff and a councilmember share in the overall policy establishment, decision-making and operations. The current SVRIA Executive Director served as the Palo Alto Fire Chief from November 2012 to January 2019.

Encryption was always planned for and specifically requested in the radio system design and Request for Proposal (RFP) issued in November 2011. On October 12, 2020, the California Department of Justice (DOJ) issued a memo that prohibited sharing of personally identifiable information (PII) over unsecured radio networks. The DOJ identified two methods to comply with the mandate, encrypt radio communications or establish policies to not communicate PII over open and unsecured radio channels.

SVRIA BACKGROUND

Legal Basis: The legal basis for SVRIA can be found in its JPA Agreement. As a result of the September 11, 2001 terrorist attacks, Palo Alto entered a Joint Funding Agreement for the purposes of joint contracting and purchasing powers to design and implement an interoperable communications, radio and data network. As the possibilities of regional and interoperable communication grew along with tens of millions of dollars in state and federal grant funding, on February 16, 2010, SVRIA officially formed, and Palo Alto agreed to and signed the JPA agreement. When the Valley Transit Authority (VTA) joined in November 2016, the Board and staff revised the JPA, and Palo Alto signed the restated agreement.

The goal of the JPA is to facilitate interoperable voice communications for the public safety and public service providers within Santa Clara County, allowing first responders, police, fire, emergency medical services, public works, utilities, and transportation officials to talk to one another on one platform during emergency incidents and non-emergency events.

The purpose of the Authority is to enhance and improve communications, data sharing and other technological systems, tools and processes for protection of the public and public safety and to facilitate related local and regional cooperative efforts.

Pursuant to Section 6509 of the Joint Exercise of Powers Act, the Authority has designated a general law city as the Member for determination of the restrictions upon the Authority in exercising the common powers under this Agreement and the City of Cupertino serves as the source of legal authority for SVRIA.

Article 3.5 of the JPA notes that unless expressly provided by the JPA Agreement, the Authority does not intend to subject itself to the internal policies or ordinances of any Member. The JPA follows all relevant laws, rules and mandates.

Board of Directors Representation: SVRIA is governed by an 11 member Board of Directors who represent the signatories of the JPA. The Board follows the Brown Act and meets bi-monthly to conduct business and establish policy. Its meeting schedule, agendas and approved minutes are available online at www.svria.org.

Palo Alto shares a Board of Directors seat with Mountain View and Los Altos. The Board seat is jointly held for a maximum of a three-year term by an appointed councilmember representing one of the three cities. The Mayors of each city with the assistance of the City Managers, collaborate to determine the Director and Alternate rotation. The table below lists the representation and attendance at Board meetings dating to January 2013.

Board Meeting Date	Director	Attendance
12/4/2013	Los Altos (Vice Chair)	Present
4/24/2014	Los Altos (Vice Chair)	Present
6/26/2014	Los Altos	Absent
10/23/2014	Los Altos (Vice Chair)	Present
1/22/2015	Los Altos (Vice Chair)	Present
3/26/2015	Los Altos (Board Chair)	Present
4/13/2015	Los Altos (Board Chair)	Present
5/8/2015	Los Altos (Board Chair)	Present

5/28/2015	Los Altos (Board Chair)	Present
9/27/2015	Los Altos (Board Chair)	Present
11/19/2015	Los Altos (Board Chair)	Present
12/9/2015	Los Altos (Board Chair)	Present
2/25/2016	Los Altos (Board Chair)	Present
3/24/2016	Los Altos	Absent
5/26/2016	Los Altos (Board Chair)	Present
9/22/2016	Vacant	
11/17/2016	Vacant	
1/26/2017	Vacant	
3/23/2017	Vacant	
5/25/2017	Vacant	
9/28/2017	Palo Alto	Absent
1/25/2018	Palo Alto	Absent
3/22/2018	Palo Alto	Absent
5/24/2018	Palo Alto	Absent
7/26/2018	Palo Alto	Absent
9/27/2018	Palo Alto	Absent
11/29/2018	Palo Alto	Absent
1/24/2019	Vacant	
3/28/2019	Los Altos	Present
5/23/2019	Los Altos	Present
9/26/2019	Los Altos	Present
1/23/2020	Los Altos	Present
3/26/2020	Los Altos	Present
6/3/2020	Los Altos	Present
9/24/2020	Los Altos	Present
10/22/2020	Los Altos	Present
11/19/2020	Los Altos	Present
1/28/2021	Los Altos	Present
3/25/2021	Los Altos (Palo Alto Alternate also present)	Present
5/27/2021	Los Altos (Palo Alto Alternate also present)	Present
7/22/2021	Los Altos (Palo Alto Alternate also present)	Present
9/23/2021	Los Altos (Palo Alto Alternate also present)	Present
11/18/2021	Los Altos (Palo Alto Alternate also present)	Present
1/27/2022	Palo Alto	Present
3/24/2022	Palo Alto	Present

It is important to note that the City of Mountain View was being represented through an appointment by the Santa Clara Cities Association which has a designated seat as required and established in the JPA.

When a councilmember who is appointed by the Cities Association is from a city that shares another Director seat, the shared Director seat must be filled by the other agencies.

In addition to setting policy for the JPA, the Board of Directors approves contracts and receives system updates from the Executive Director and staff. Encryption updates are shared regularly at the Board of Directors Meetings.

Radio System Procurement History: SVRIA undertook a lawful vendor solicitation, selection, and procurement process.

The RFP was derived from a document prepared in 2009 by the consulting firm BearingPoint which was revised by Federal Engineering as part of a regional RFP preparation effort undertaken by the Bay Area Urban Area Security Initiative (BA UASI). The revised RFP was further refined in 2011 by Forrest Telecom Engineering, consulting to SVRIA.

Radio encryption was specifically identified as a requirement from vendors in the RFP.

A 12 member RFP team was established, representing seven cities, the County and SVRIA. The team included staff from law enforcement, dispatch and communications. The Palo Alto Police Department's Technical Services Director was a key member of the RFP team.

The RFP was issued on November 4, 2011. Four vendors, Motorola, Harris, Cassidian and Tait, attended a pre-proposal conference on November 18, 2011. Subsequently, Tait withdrew from consideration and Cassidian later advised they would not submit a proposal.

Final presentations by the two proposers – Motorola and Harris – were made on March 26, 2012. Following those presentations, the RFP team utilized a consensus approach to proposal evaluation rather than a structured points-based approach. Both proposals were considered equally qualified, products were deemed satisfactory and neither proposer took any disqualifying exceptions to the RFP.

The vendor selection was based solely on economic factors. Through a combination of discounts and incentives, Motorola's proposal was approximately \$500,000 less than Harris' proposal. Both vendors were advised that Motorola was the selected vendor although contract award would be pending successful negotiations. The contract was awarded to Motorola in September 2012.

ENCRYPTION DISCUSSION

California DOJ mandate compliance: SVRIA does not set encryption policy for its member agencies. As noted in the legal basis section, the Authority will follow all relevant laws, rules and mandates, including DOJ encryption. Further, the Authority does not intend to subject itself to the internal policies or ordinances of any Member.

SVRIA's process for compliance is driven by maintaining regional interoperable radio communications. As stated in SVRIA's mission, regional interoperable radio and data communications is the reason for the Authority's existence. SVRIA exists to support the technical radio communication needs of its members. SVRIA's focus is to ensure that its technology works 24/7/365, and the radios and operators can communicate with one another.

SVRIA supported its law enforcement members in analyzing and reviewing the October 12, 2020, DOJ encryption memo. A subcommittee of staff representing JPA members collaborated on a written response to the State DOJ. The communication with the DOJ required a written plan and deadline to comply. Two letter templates were drafted for law enforcement agencies. One letter was for agencies already in compliance with the DOJ mandate, and a second, more detailed letter, was for those agencies not in compliance as of December 31, 2020. The templates were provided to the police chiefs and County Sheriff.

Currently, all Santa Clara County law enforcement agencies and SVRIA comply with the DOJ memo. All agencies except San Jose Evergreen College have achieved compliance through radio encryption. San Jose Evergreen College complies through policy but is expected to become encrypted by April 30, 2022.

The Authority is not willing to take one member’s non-compliance liability. Legal analysis would need to determine if a hold harmless agreement could be an option. Specifically, as a condition of Palo Alto operating unencrypted on the SVRCS, they would take on the liability for the Authority. This is likely unacceptable to Palo Alto.

It is important to note that all encrypted talkgroups are recorded and logged. The recordings include all communications on the talkgroups including officers in the field and dispatchers. The records are kept by the individual agencies based upon their retention policies and are subject to Public Records Act requests.

Agency Encryption History: Encrypted talkgroups have been used by SVRIA law enforcement agencies since the system was deployed in 2015. In the last two and a half years, all law enforcement agencies in the SVRCS except for San Jose Evergreen College have transitioned their primary dispatch talkgroups to encryption. Six agencies representing the majority of the radios on the system, began encryption before the DOJ memo was released. Morgan Hill and Gilroy began operating on the SVRCS with encryption on their law primary talkgroup. The other agencies began with unencrypted law enforcement primary talkgroups, then transitioned to encrypted.

Agency	Date of Encryption on Law Primary Talkgroup
Morgan Hill Police	September 2019
San Jose Police	March 2020
Gilroy Police	May 2020
Campbell Police	May 2020
Los Gatos Police	June 2020
County Sheriff’s Office	August 2020
California DOJ Encryption Memo	October 12, 2020
Sunnyvale Police	November 2020
Palo Alto Police	January 2021
Los Altos Police	March 2021
Mountain View Police	March 2021
Foothill/DeAnza College Police	March 2021
San Jose State University Police	March 2021
Santa Clara City Police	April 2021
Milpitas Police	July 2021
SVRIA Law Interoperability Talkgroups	August 2021

West Valley/Mission College Police	August 2021
San Jose Evergreen College	April 2022

Staff time and costs to program radios: Radios must be programmed when talkgroups and radios are changed from unencrypted to encrypted. This is costly as each radio takes an average of 30 minutes to reprogram. Approximately half of the 11,365 radios operated by SVRIA agencies are assigned to law enforcement agencies, the staff time alone to reprogram radios is nearly 3000 hours, or approximately one and a half full-time equivalent staff position. Additionally, reprogramming the radio system core and other operating systems would be a minimum of 400 hours. Staff costs are incurred by each agency as well as SVRIA.

There is a careful balance when agencies reprogram their radios as features of the system are inactive and inoperable. Thoughtful coordination between radio programming staff, dispatchers, field operations officials, adjoining agencies, and radio system operators (SVRIA and other regional systems in the Bay Area) must occur.

Encryption Technology and Operational implications: It is important to note that when an encrypted radio and an unencrypted radio are operating on the same talkgroup, all communication is unencrypted, even when the talkgroup is programmed for encryption.

SVRIA utilizes 256 bit Advanced Encryption Standard (AES). This is the industry standard and using this technology is required in order to receive state or federal radio and security grant funding.

In multi-agency incidents, the radios from all the responding agencies are joined, the technical term is patched, into a shared, regional interoperability talkgroup. The patch allows responders from all agencies to seamlessly communicate with one another. If the shared talkgroup is programmed to be encrypted, and an unencrypted radio or talkgroup is patched, the group of patched radios are now unencrypted and can be heard by a digital scanner. This exposes the JPA to non-compliance if PII is transmitted on the shared, regional interoperability talkgroup.

There are options to ensure all radios operating on the regional interoperable talkgroups are operating in compliance with the DOJ directive.

First, in order to ensure that all radios entering the shared interoperable talkgroup patch are encrypted, the responding units would need to switch their radio to an encrypted talkgroup and then be patched. The dispatcher or field officer could do this as they are responding to the multi-agency incident. This option unfortunately adds extra steps to the public safety staff entering dynamic emergency situations. Public safety dispatchers coordinate this shared regional response and patch.

SVRIA’s goal is to minimize public safety officials from having to change talkgroups on their radios during critical incidents. It is unreasonable to expect already short-staffed and over-worked dispatcher centers to take on extra work to switch field radios from unencrypted to encrypted talkgroups, and then coordinate a patch into the encrypted interoperable talkgroup in an emerging and out-of-control incident.

A second option would be to exclude unencrypted radios from being patched into regional interoperable law enforcement talkgroups. As a matter of policy, SVRIA’s Board could limit access to the encrypted regional interoperable talkgroups. Only radios that are programmed for encryption and can

be directly patched, without the intermediate channel change step, into the encrypted regional interoperable talkgroups would be allowed. Encrypted regional talkgroups would be removed from the agency's radios that are unencrypted. Unencrypted radios would not have any regional or interoperable law enforcement talkgroups, and the operators would have limited communication capabilities with other law enforcement officials outside their home agency. This eliminates almost all interoperability, impacts public and officer safety, and regresses to the pre-September 11, 2001 communication condition.

The inability to communicate has been identified in adverse outcomes and line of duty death incidents. Multi-agency communication is the primary reason for regional, interoperable radio systems. I have personal experience of a firefighter line of duty death (Cedar Fire, San Diego County, October 29, 2003) that was partially attributed to the fire crews not knowing they needed to change talkgroups on their radios. The crew missed repeated radio warnings of the wildfire blowing up beneath them. The crew was burnt over and one of my colleagues was killed.

Palo Alto could also lose most interoperable communication access to law enforcement mutual aid radios authorized to operate on the encrypted regional interoperability talkgroups. These mutual aid partners include California Highway Patrol (CHP), California Governor's Office of Emergency Services (CalOES), Federal Bureau of Investigations (FBI), Bureau of Alcohol, Tobacco and Firearms (ATF), United States Marshal's Service, Internal Revenue Service – Criminal Investigations, NASA/Ames Protective Services, and Bay Area Counties regional communications networks including San Mateo and the East Bay systems.

No single agency in Santa Clara County is able to stand alone and handle all of their incidents without mutual aid. Every day across the county, public safety personnel move across local government boundaries to assist neighboring agencies. The lack of cohesion and communication between the unencrypted and encrypted agencies will lead to adverse outcomes, in particular for the agency that is unencrypted and lacks the full functionality of a regional interoperable radio system.

Encryption and Stanford Department of Public Safety (DPS): The Santa Clara County Sheriff provides oversight and operational authority to Stanford DPS through direct supervision of the assigned Captain. The Sheriff's Captain acts at the direction of the Sheriff in policy matters. Palo Alto provides dispatching and communications services to Stanford DPS through a service contract.

If Palo Alto were to transition to an unencrypted primary and the Sheriff required encrypted communications, it sets up a demanding situation for dispatchers, field personnel, and contact compliance.

Operational difficulties include separate dispatch talkgroups, one encrypted, one unencrypted, dispatchers having to move between encrypted and unencrypted talkgroups, officers being on the wrong talkgroup or unable to communicate with one another, and Stanford DPS having access to the encrypted regional interoperable talkgroups and Palo Alto Police not having access.

Contract compliance and administrative challenges include providing enhanced services due to the additional workload of encrypted/unencrypted, documenting communication compliance, and modifying the service contract with Stanford University due to the added workload and costs.